

II

(Nelegislativní akty)

ROZHODNUTÍ

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

(oznámeno pod číslem C(2016) 4176)

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ⁽¹⁾, a zejména na čl. 25 odst. 6 uvedené směrnice,

po konzultaci s evropským inspektorem ochrany údajů ⁽²⁾,

1. ÚVOD

- (1) Směrnice 95/46/ES stanoví pravidla pro předávání osobních údajů z členských států do třetích zemí, pokud toto předávání spadá do oblasti působnosti uvedené směrnice.
- (2) Z článku 1 a z 2. a 10. bodu odůvodnění směrnice 95/46/ES vyplývá, že předmětem směrnice je nejen zajištění účinné a úplné ochrany základních práv a svobod fyzických osob, zejména základního práva na respektování soukromého života v souvislosti se zpracováním osobních údajů, ale i zajištění vysoké úrovně ochrany těchto základních práv a svobod ⁽³⁾.
- (3) Význam jak základního práva na respektování soukromého života zaručeného článkem 7 Listiny základních práv Evropské unie, tak základního práva na ochranu osobních údajů zaručeného článkem 8 této listiny je vyzdvížen v judikatuře Soudního dvora ⁽⁴⁾.
- (4) Podle čl. 25 odst. 1 směrnice 95/46/ES členské státy stanoví, že k předávání osobních údajů do třetí země může dojít, pouze pokud dotyčná třetí země zajistí odpovídající úroveň ochrany a pokud jsou před předáním dodrženy právní předpisy členského státu přijaté na základě ostatních ustanovení směrnice. Komise může shledat, že třetí země zajišťuje takovou odpovídající úroveň ochrany, na základě vnitrostátních předpisů dotyčné třetí země nebo mezinárodních závazků v oblasti ochrany práv fyzických osob, k nimž se dotyčná země zavázala. V takovém případě, a aniž je dotčeno dodržení vnitrostátních právních předpisů přijatých na základě ostatních ustanovení směrnice, mohou být osobní údaje z členských států předávány bez nutnosti dodatečných záruk.

⁽¹⁾ Úř. věst. L 281, 23.11.1995, s. 31.

⁽²⁾ Viz stanovisko 4/2016 k návrhu rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí, vydané dne 30. května 2016.

⁽³⁾ Věc C-362/14, Maximilian Schrems proti Data Protection Commissioner (dále jen „Schrems“), EU:C:2015:650, bod 39.

⁽⁴⁾ Věc C-553/07, Rijkeboer, EU:C:2009:293, bod 47; spojené věci C-293/12 a C-594/12, Digital Rights Ireland a další, EU:C:2014:238, bod 53; Věc C-131/12, Google Spain a Google, EU:C:2014:317, body 53, 66 a 74.

- (5) Podle čl. 25 odst. 2 směrnice 95/46/ES by úroveň ochrany údajů poskytovaná třetí zemí měla být posouzena s ohledem na všechny okolnosti související s předáním nebo předáváním údajů, mimo jiné s ohledem na právní předpisy, obecné či odvětvové, platné v dotčené třetí zemi.
- (6) V rozhodnutí Komise 2000/520/ES ⁽⁵⁾ bylo shledáno, že pro účely čl. 25 odst. 2 směrnice 95/46/ES poskytují „zásady „bezpečného přístavu“, prováděné v souladu s pokyny uvedenými v tzv. „často kladených otázkách“ vydaných Ministerstvem obchodu USA, odpovídající úroveň ochrany osobních údajů předávaných z Unie organizacím ve Spojených státech.
- (7) Ve sděleních COM(2013) 846 final ⁽⁶⁾ a COM(2013) 847 final ze dne 27. listopadu 2013 ⁽⁷⁾ Komise uvedla, že základní pilíř systému zásad „bezpečného přístavu“ je třeba přezkoumat a posílit v kontextu řady faktorů, mimo jiné exponenciálního nárůstu toku údajů a jejich zásadního významu pro transatlantickou ekonomiku, rychlého nárůstu počtu amerických společností, které přijaly zásady „bezpečného přístavu“, a nových informací o rozsahu a záběru některých amerických zpravodajských programů, které nastolily otázky ohledně úrovně ochrany, jakou „bezpečný přístav“ může zaručit. Kromě toho Komise v systému zásad „bezpečného přístavu“ odhalila řadu slabín a nedostatků.
- (8) Na základě důkazů, mimo jiné informací vyplynulých z práce Kontaktní skupiny EU–USA pro ochranu soukromí ⁽⁸⁾ a informací o amerických zpravodajských programech získaných v rámci *ad-hoc* pracovní skupiny EU–USA ⁽⁹⁾, formulovala Komise 13 doporučení pro přezkum systému zásad „bezpečného přístavu“. Tato doporučení se zaměřila na posílení hmotněprávních zásad ochrany soukromí, zvýšení transparentnosti politik ochrany soukromí amerických autocertifikovaných společností, lepší dohled, monitorování a vymáhání těchto zásad ze strany orgánů USA, dostupnost finančně přijatelných mechanismů řešení sporů a potřebu zajistit, aby výjimka z důvodu národní bezpečnosti stanovená v rozhodnutí 2000/520/ES byla omezena na rozsah striktně nezbytný a přiměřený.
- (9) Rozsudkem ze dne 6. října 2015 ve věci C-362/14, *Maximillian Schrems proti Data Protection Commissioner* ⁽¹⁰⁾, prohlásil Soudní dvůr Evropské unie rozhodnutí 2000/520/ES za neplatné. Aniž by zkoumal obsah zásad „bezpečného přístavu“, soud konstatoval, že Komise v uvedeném rozhodnutí neuvedla, že Spojené státy skutečně „zajišťují“ odpovídající úroveň ochrany na základě svých vnitrostátních předpisů nebo mezinárodních závazků ⁽¹¹⁾.
- (10) V tomto ohledu Soudní dvůr vysvětlil, že přestože výraz „odpovídající úroveň ochrany“ obsažený v čl. 25 odst. 6 směrnice 95/46/ES neznamená stejnou úroveň ochrany, jako je úroveň zajištěná v unijním právním řádu, musí být chápán v tom smyslu, že vyžaduje, aby třetí země zajišťovala takovou úroveň ochrany základních práv a svobod, která je „v zásadě rovnocenná“ ochraně zaručené v rámci Unie směrnicí 95/46/ES vykládanou ve světle Listiny základních práv. I když se prostředky, které tato třetí země využívá v tomto směru k zajištění takovéto úrovně ochrany, mohou lišit od prostředků zavedených v rámci Unie, musí se přesto tyto prostředky v praxi ukázat jako účinné ⁽¹²⁾.
- (11) Soudní dvůr zkritizoval, že rozhodnutí 2000/520/ES neobsahuje dostatečná zjištění ohledně existence pravidel státního charakteru ve Spojených státech, jež mají omezit případné zásahy do základních práv osob, jejichž osobní údaje jsou předávány z Unie do Spojených států, tj. zásahy, jež by státní subjekty této země byly oprávněny činit v případě, že sledují takové legitimní cíle, jako je národní bezpečnost, a ohledně existence účinné právní ochrany před zásahy tohoto druhu ⁽¹³⁾.

⁽⁵⁾ Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států (Úř. věst. L 215, 28.8.2000, s. 7).

⁽⁶⁾ Sdělení Komise Evropskému parlamentu a Radě – Obnovení důvěry v toky údajů mezi EU a USA, COM(2013) 846 final ze dne 27. listopadu 2013.

⁽⁷⁾ Sdělení Komise Evropskému parlamentu a Radě o fungování „bezpečného přístavu“ z pohledu občanů EU a společností usazených v EU, COM(2013) 847 final ze dne 27. listopadu 2013.

⁽⁸⁾ Viz např. Rada Evropské unie, Závěrečná zpráva Kontaktní skupiny EU–USA na vysoké úrovni pro sdílení informací a ochranu soukromí a osobních údajů, dokument 9831/08 ze dne 28. května 2008, k dispozici na této adrese: <http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf>.

⁽⁹⁾ Zpráva o zjištěních spolupředsedů zastupujících EU v *ad-hoc* pracovní skupině EU–USA pro ochranu osobních údajů ze dne 27. listopadu 2013, k dispozici na této adrese: <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>.

⁽¹⁰⁾ Viz poznámka pod čarou 3.

⁽¹¹⁾ *Schrems*, bod 97.

⁽¹²⁾ *Schrems*, body 73–74.

⁽¹³⁾ *Schrems*, body 88–89.

- (12) V roce 2014 Komise zahájila s orgány USA rozhovory, aby prodiskutovala posílení režimu „bezpečného přístavu“ na základě 13 doporučení uvedených ve sdělení COM(2013) 847 final. Po rozsudku Soudního dvora Evropské unie ve věci *Schrems* tyto rozhovory dále zintenzivnily ve snaze dospět k případnému novému rozhodnutí o odpovídající úrovni ochrany, které by vyhovovalo požadavkům článku 25 směrnice 95/46/ES tak, jak je vyložil Soudní dvůr. Výsledkem těchto diskusí jsou dokumenty, které tvoří přílohu tohoto rozhodnutí a které budou zveřejněny také ve Federálním úředním věstníku USA (*U.S. Federal Register*). Zásady ochrany soukromí (příloha II) společně s oficiálními prohlášeními a závazky různých orgánů USA obsaženými v dokumentech v přílohách I a III až VII tvoří „štít EU–USA na ochranu soukromí“.
- (13) Komise provedla pečlivou analýzu práva a praxe USA, jakož i těchto oficiálních prohlášení a závazků. Na základě zjištění rozepsaných ve 136. až 140. bodě odůvodnění Komise došla k závěru, že Spojené státy zajišťují odpovídající úroveň ochrany osobních údajů předávaných v rámci štítu EU–USA na ochranu soukromí z Unie autocertifikovaným organizacím ve Spojených státech.

2. „ŠTÍT EU–USA NA OCHRANU SOUKROMÍ“

- (14) Štít EU–USA na ochranu soukromí je založen na systému autocertifikace, kterým se organizace USA zavazují dodržovat soubor zásad ochrany soukromí – rámcové zásady štítu EU–USA na ochranu soukromí, včetně doplňkových zásad (dále dohromady jen „zásady“) – vydaných Ministerstvem obchodu USA a obsažených v příloze II tohoto rozhodnutí. Použije se jak na správce, tak zpracovatele (zprostředkovatele) s tím, že zpracovatelé musí být smluvně zavázáni 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 ⁽¹⁴⁾.
- (15) Aniž je dotčena povinnost vyhovět vnitrostátním ustanovením přijatým podle směrnice 95/46/ES, má toto rozhodnutí účinek v tom smyslu, že je povoleno předávání údajů od správce nebo zpracovatele v Unii organizacím v USA, které autocertifikovaly přijetí zásad u Ministerstva obchodu a které se zavázaly je dodržovat. Zásady se použijí pouze na zpracování osobních údajů organizací USA potud, pokud zpracování takovými organizacemi nespadá do oblasti působnosti právních předpisů Unie ⁽¹⁵⁾. Štítem na ochranu soukromí není dotčeno uplatňování právních předpisů Unie, jimiž se řídí zpracování osobních údajů v členských státech ⁽¹⁶⁾.

⁽¹⁴⁾ Viz příloha II, oddíl III bod 10 písm. a). V souladu s definicí v oddíle I bodě 8 písm. c) správce v EU určuje účel a prostředky zpracování osobních údajů. Smlouva se zprostředkovatelem musí jasně stanovit, zda je povoleno další předávání (viz oddíl III bod 10 písm. a) podbod ii) podpodbod 2).

⁽¹⁵⁾ To se týká i případů, kdy jsou z Unie předávány údaje o lidských zdrojích v kontextu zaměstnaneckého vztahu. Zásady kladou důraz na „hlavní odpovědnost“ zaměstnavatele v EU (viz příloha II, oddíl III bod 9 písm. d) podbod i), přičemž dále vyjasňují, že tento postup se bude řídit nikoli zásadami, nýbrž pravidly platnými v Unii a/nebo příslušném členském státě. Viz příloha II, oddíl III bod 9 písm. a) podbod i), písm. b) podbod ii), písm. c) podbod i), písm. d) podbod i).

⁽¹⁶⁾ To se týká rovněž zpracování, které probíhá použitím zařízení umístěného v Unii, ale používaného organizací usazenou mimo Unii (viz čl. 4 odst. 1 písm. c) směrnice 95/46/ES). Ode dne 25. května 2018 se obecné nařízení o ochraně údajů bude vztahovat na zpracování osobních údajů i) v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii (i tehdy, probíhá-li zpracování ve Spojených státech), nebo ii) subjektů údajů, kteří se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba; nebo b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie. Viz čl. 3 odst. 1, 2 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) (Úř. věst. L 119, 4.5.2016, s. 1).

- (16) Ochrana poskytovaná osobním údajům štítem na ochranu soukromí se vztahuje na všechny subjekty údajů z EU ⁽¹⁷⁾, jejichž osobní údaje byly předány z Unie organizacím v USA, které autocertifikovaly přijetí zásad u Ministerstva obchodu.
- (17) Zásady jsou použitelné bezprostředně po certifikaci. Jediná výjimka se vztahuje na zásadu odpovědnosti za další předávání v případech, kdy organizace autocertifikující přijetí zásad štítu na ochranu soukromí má obchodní vztahy s třetími stranami z dřívější doby. Poněvadž může jistou dobu trvat, než budou tyto obchodní vztahy uvedeny v soulad s pravidly podle zásady odpovědnosti za další předávání, bude taková organizace povinna uvést je v soulad co nejdříve a v každém případě nejpozději do devíti měsíců od autocertifikace (za předpokladu, že k tomu dojde v prvních dvou měsících ode dne, kdy štít na ochranu soukromí nabyl účinku). Během tohoto přechodného období musí organizace uplatňovat zásadu oznamovací povinnosti a zásadu možnosti volby (a umožnit tak subjektu údajů z EU vyslovit nesouhlas) a v případě, že jsou osobní údaje předávány třetí straně jednající jako zprostředkovatel, musí zajistit, že tato třetí strana poskytuje alespoň stejnou úroveň ochrany požadovanou podle zásad ⁽¹⁸⁾. Tímto přechodným obdobím je přiměřeně a vhodně vyváжено dodržování základního práva na ochranu údajů s legitimní potřebou podniků mít dostatek času na přizpůsobení se novému rámci i v případech, kdy toto závisí také na jejich obchodních vztazích s třetími stranami.
- (18) Tento systém bude spravován a monitorován Ministerstvem obchodu na základě jeho závazků uvedených v prohlášeních ministryně obchodu USA (příloha I tohoto rozhodnutí). Pokud jde o prosazování zásad, Federální obchodní komise (FTC) a Ministerstvo obchodu vydaly prohlášení, která jsou obsažena v příloze IV a V tohoto rozhodnutí.

2.1 Zásady ochrany soukromí

- (19) Součástí autocertifikace v rámci štítu EU–USA na ochranu soukromí je, že se organizace musí zavázat k dodržování zásad ⁽¹⁹⁾.
- (20) Podle *zásady oznamovací povinnosti* jsou organizace povinny subjektům údajů poskytovat informace o řadě klíčových prvků týkajících se zpracování jejich osobních údajů (např. o druhu shromažďovaných údajů, o účelu zpracování, o právu na přístup a volbu, o podmínkách dalšího předávání a o odpovědnosti). Platí další ochranná opatření, zejména požadavek, aby organizace zveřejnily svoji politiku ochrany soukromí (odrážející zásady) a aby poskytl odkazy na web Ministerstva obchodu (s dalšími podrobnostmi o autocertifikaci, právech subjektů údajů a dostupných odvolacích mechanismech), na seznam organizací štítu na ochranu soukromí (uvedený ve 30. bodě odůvodnění) a na web příslušného poskytovatele alternativního řešení sporů.
- (21) Podle *zásady integrity údajů a účelového omezení* musí být osobní údaje omezeny na údaje relevantní k účelu zpracování, spolehlivé z hlediska zamýšleného použití, přesné, úplné a aktuální. Organizace nesmí zpracovávat osobní údaje způsobem, který je neslučitelný s účelem, pro který byly původně shromážděny nebo následně subjektem údajů povoleny. Organizace musí zajistit, aby osobní údaje byly spolehlivé z hlediska zamýšleného použití, přesné, úplné a aktuální.

⁽¹⁷⁾ Toto rozhodnutí má význam pro EHP. Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) rozšiřuje vnitřní trh Evropské unie na tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Dohoda o EHP zahrnuje právní předpisy Unie o ochraně údajů, včetně směrnice 95/46/ES, které jsou začleněny v příloze XI této dohody. Smíšený výbor EHP musí rozhodnout o začlenění tohoto rozhodnutí do Dohody o EHP. Jakmile se toto rozhodnutí použije na Island, Lichtenštejnsko a Norsko, bude se také štít EU–USA na ochranu soukromí vztahovat na tyto tři státy a odkazy na EU v souboru předpisů o štítu na ochranu soukromí budou čteny tak, že zahrnují také Island, Lichtenštejnsko a Norsko.

⁽¹⁸⁾ Viz příloha II, oddíl III bod 6 písm. e).

⁽¹⁹⁾ Pro údaje o lidských zdrojích, které jsou shromažďovány v kontextu zaměstnávání, platí v souladu s doplňkovou zásadou o údajích o lidských zdrojích zvláštní pravidla zajišťující doplňkovou ochranu (viz příloha II, oddíl III bod 9). Zaměstnavatelé by tak například měli vycházet vstříc preferencím zaměstnanců z hlediska ochrany soukromí a omezovat přístup k osobním údajům, anonymizovat některé údaje nebo jim přidělovat kódy či pseudonymy. Nejdůležitější je, že organizace musí v souvislosti s těmito údaji spolupracovat a držet se doporučení orgánů Unie ochranu údajů.

- (22) Pokud je nový (změněný) účel významně odlišný, ale stále slučitelný s původním účelem, dává *zásada možnosti volby* subjektům údajů možnost vyslovit nesouhlas (*opt-out*). *Zásada možnosti volby* nenahrazuje výslovný zákaz neslučitelného zpracování⁽²⁰⁾. Zvláštní pravidla, která obecně umožňují vyslovení nesouhlasu s používáním osobních údajů „kdykoli“, se týkají přímého marketingu⁽²¹⁾. V případě citlivých údajů musí organizace v zásadě obdržet potvrzující výslovný souhlas (tzv. *opt-in*) subjektu údajů.
- (23) Ještě pokud jde o *zásadu integrity údajů a účelového omezení*, lze osobní informace uchovávat v podobě ztotožňující fyzickou osobu nebo umožňující jeho ztotožnění (tedy v podobě osobních údajů) jen potud, pokud tyto informace slouží účelu (účelům), pro který byly původně shromážděny nebo následně povoleny. Tato povinnost organizacím účastnícím se štítu na ochranu soukromí 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: archivace ve veřejném zájmu, žurnalistika, literatura a umění, vědecký a historický výzkum a statistická analýza. Delší uchovávání osobních údajů pro jeden z těchto účelů podléhá ochranným opatřením podle zásad.
- (24) Podle *zásady bezpečnosti* musí organizace vytvářející, uchovávající, používající nebo šířící osobní údaje přijmout „přiměřená a vhodná“ bezpečnostní opatření s přihlédnutím k rizikům spojeným se zpracováním a povahou údajů. Jsou-li údaje zpracovávány externě, musí organizace uzavřít s externím zpracovatelem smlouvu, která zaručí stejnou úroveň ochrany, jakou poskytují zásady, a přijmout opatření k zajištění jejího řádného plnění.
- (25) Podle *zásady práva na přístup*⁽²²⁾ mají subjekty údajů právo na to, aby jim bez nutnosti zdůvodňování a pouze za přiměřený poplatek organizace potvrdila, zda tato organizace zpracovává osobní údaje, které se jich týkají, a aby jim tyto údaje byly v přiměřené lhůtě sděleny. Toto právo lze omezit jen za výjimečných okolností; jakékoli odepření tohoto práva či jeho omezení musí být nezbytné a řádně odůvodněné, přičemž důkazní břemeno toho, že jsou tyto požadavky splněny, leží na organizaci. Subjektům údajů musí být umožněno opravovat, upravovat či vymazávat osobní informace, pokud jsou nepřesné nebo pokud byly zpracovány v rozporu se zásadami. V oblastech, kde společnostmi nejčastěji využívají automatizovaného zpracování osobních údajů pro rozhodování, které má dopad na fyzickou osobu (např. úvěry a půjčky, nabídky hypoték, zaměstnání), poskytuje právo USA konkrétní ochranu proti negativním rozhodnutím⁽²³⁾. 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. Tato pravidla poskytují ochranu v pravděpodobně poměrně omezeném počtu případů, kde by automatizovaná rozhodnutí činila sama organizace účastníci se štítu na ochranu soukromí⁽²⁴⁾. Nicméně vzhledem k rostoucímu využití automatizovaného zpracování (včetně profilování) jakožto základu pro rozhodování, které má dopad na fyzické osoby, v moderní digitální ekonomice, je třeba tuto oblast úzce monitorovat. Za účelem usnadnění tohoto monitorování bylo s orgány USA dohodnuto, že součástí prvního každoročního přezkumu a případně následujících přezkumů bude dialog na téma automatizovaného rozhodování, včetně výměny názorů na podobnosti a rozdílnosti v přístupech EU a USA.

⁽²⁰⁾ To se vztahuje na veškeré předávání údajů v rámci štítu na ochranu soukromí, včetně případů, kdy se tyto přenosy týkají údajů shromážděných v rámci zaměstnaneckého vztahu. Autocertifikovaná organizace USA sice v zásadě může použít údaje o lidských zdrojích pro různé účely nesouvisející 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*. Zákaz uplatňování sankcí ze strany organizace USA vůči zaměstnanci, který uplatňuje svou možnost volby, včetně omezení z hlediska zaměstnaneckých příležitostí, zajistí, že se zaměstnanec navzdory podřízenému vztahu a inherentní závislosti nebude cítit pod nátlakem, a může tak provést opravdu svobodnou volbu.

⁽²¹⁾ Viz příloha II, oddíl III bod 12.

⁽²²⁾ Viz také doplňková zásada „Právo na přístup“ (příloha II, oddíl III bod 8).

⁽²³⁾ Viz např. zákon o rovné příležitosti k získání úvěru (*Equal Credit Opportunity Act*, ECOA, 15 U.S.C. 1691 a násl.), zákon o spravedlivém informování o úvěrové spolehlivosti (*Fair Credit Reporting Act*, FRCA, 15 USC § 1681 a násl.) nebo zákon o spravedlivém bydlení (*Fair Housing Act*, FHA, 42 U.S.C. § 3601 a násl.).

⁽²⁴⁾ V kontextu předávání osobních údajů, které byly shromážděny v EU, bude smluvní vztah s fyzickou osobou (zákazníkem) ve většině případů uzavřen se správcem údajů z EU, který se musí řídit pravidly EU pro ochranu údajů, a tudíž jakékoli rozhodnutí na základě automatizovaného zpracování bude obvykle činit tento správce. Sem patří scénáře, kdy zpracování provádí organizace účastníci se štítu na ochranu soukromí jednající jako zprostředkovatel jménem správce z EU.

- (26) Podle *zásady odvolání, prosazování a odpovědnosti* ⁽²⁵⁾ musí účastníci se organizace poskytnout robustní mechanismy, které zajistí dodržování ostatních zásad, a subjektům údajů, jejichž údaje byly zpracovány nenáležitým způsobem, musí poskytnout možnost odvolání i účinnou nápravu. Jakmile se organizace dobrovolně rozhodla autocertifikovat ⁽²⁶⁾ v rámci štítu EU–USA na ochranu soukromí, její faktické dodržování zásad se stává povinným. Aby organizace mohla v rámci štítu EU–USA na ochranu soukromí získávat i nadále osobní údaje z Unie, musí každý rok recertifikovat svou účast v rámci. Organizace musí také přijmout opatření k ověření ⁽²⁷⁾ toho, zda politika ochrany soukromí, kterou zveřejňují, 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 nebo namátkových kontrol. Kromě toho musí organizace zajistit účinný nápravný mechanismus k vyřizování jakýchkoli stížností (v tomto ohledu viz také 43. bod odůvodnění) a podléhat vyšetřovací a donucovací pravomoci FTC, Ministerstva dopravy nebo jiného pověřeného, zákonem zřízeného orgánu USA, které zajistí dodržování zásad.
- (27) Zvláštní pravidla platí pro tzv. „další předávání“, tj. předávání osobních údajů z organizace třetí straně jednající jako správce nebo zpracovatel neohledně na to, zda je taková třetí strana ve Spojených státech nebo ve třetí zemi mimo Spojené státy (a Unii). Účelem těchto pravidel je zajistit, aby ochrana osobních údajů subjektů údajů z EU nebyla narušena a aby nemohla být obejitá tak, že budou údaje postoupeny třetím stranám. To je zejména významné v komplexnějších zpracovatelských řetězcích, které jsou typické pro dnešní digitální ekonomiku.
- (28) Podle *zásady odpovědnosti za další předávání* ⁽²⁸⁾ může k jakémukoli dalšímu předání dojít pouze i) k omezeným a konkrétním účelům, ii) na základě smlouvy (nebo srovnatelného ujednání v rámci skupiny společností ⁽²⁹⁾) a iii) jen pokud taková smlouva poskytuje stejnou úroveň ochrany, jakou poskytují zásady, což zahrnuje požadavek, že uplatňování zásad lze omezit v rozsahu nezbytném k tomu, aby byl splněn účel národní bezpečnosti, prosazování práva a jiných veřejných zájmů ⁽³⁰⁾. Předchozí je třeba vykládat ve spojení se *zásadou oznamovací povinnosti* a v případě dalšího předání třetí straně–správci ⁽³¹⁾, se *zásadou možnosti volby*, podle níž musí být subjekty informovány (mimo jiné) o druhu/totožnosti jakékoli třetí strany–příjemce, o účelu dalšího předání, jakož i o možnosti volby a mohou vyslovit nesouhlas (*opt-out*), nebo v případě citlivých údajů, musí vyslovit „potvrzující výslovný souhlas“ (*opt-in*) s dalším předáním. Ve světle *zásady integrity údajů a účelového omezení* povinnost poskytnout stejnou úroveň ochrany, jaká je zaručena zásadami, předpokládá, že třetí strana smí zpracovat osobní informace jí předané pro účely, které nejsou neslučitelné s účely, pro které byly původně shromážděny nebo fyzickou osobou následně povoleny.
- (29) Povinnost poskytnout stejnou úroveň ochrany, jakou požadují zásady, se vztahuje na jakékoli a všechny třetí strany, které jsou zapojeny do zpracování takto předávaných údajů neohledně na jejich umístění (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. Ve všech případech musí smlouva s třetí stranou–příjemcem, stanovit, že tento příjemce organizaci účastníci se štítu na ochranu soukromí oznámí, pokud zjistí, že již tuto podmínku nesplňuje. Je-li takové zjištění učiněno, zpracování touto třetí stranou bude ukončeno nebo

⁽²⁵⁾ Viz také doplňková zásada „Řešení sporů a prosazování“ (příloha II, oddíl III bod 11).

⁽²⁶⁾ Viz také doplňková zásada „Autocertifikace“ (příloha II, oddíl III bod 6).

⁽²⁷⁾ Viz také doplňková zásada „Ověřování“ (příloha II, oddíl III bod 7).

⁽²⁸⁾ Viz také doplňková zásada „Povinné smlouvy pro účely dalšího předávání“ (příloha II, oddíl III bod 10).

⁽²⁹⁾ Viz také doplňková zásada „Povinné smlouvy pro účely dalšího předávání“ (příloha II, oddíl III bod 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 „zajist[it] kontinuitu ochrany osobních informací podle zásad“. Navíc to, že autocertifikované organizace USA zůstanou odpovědné za dodržování zásad, bude silným impulsem k použití nástrojů, které jsou v praxi opravdu účinné.

⁽³⁰⁾ Viz příloha II, oddíl I bod 5.

⁽³¹⁾ Fyzické osoby nemají právo vyslovit nesouhlas, jsou-li osobní údaje předány 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.

musí být přijaty jiné přiměřené a vhodné kroky k nápravě této situace ⁽³²⁾. Vzniknou-li problémy s dodržováním zásad v (externím) zpracovatelském řetězci, organizace účastníci se štítu na ochranu soukromí a jednající jako správce osobních údajů bude muset dokázat, že není odpovědná za událost, která vedla ke škodě, nebo v opačném případě nést odpovědnost, jak je uvedeno v *zásadě odvolání, prosazování a odpovědnosti*. V případě dalšího předání třetí straně-zprostředkovateli, platí doplňková ochrana ⁽³³⁾.

2.2 Transparentnost, správa štítu EU–USA na ochranu soukromí a dohled nad ním

- (30) Štít EU–USA na ochranu soukromí stanoví dohled a donucovací mechanismy k ověřování a zajištění dodržování zásad ze strany autocertifikovaných společností z USA a řešení veškerých případů nedodržení. Tyto mechanismy jsou popsány v zásadách (příloha II) a závazcích přijatých Ministerstvem obchodu (příloha I), Federální obchodní komisí (příloha IV) a Ministerstvem dopravy (příloha V).
- (31) Pro zajištění řádného uplatňování štítu EU–USA na ochranu soukromí musí být zúčastněné strany, např. subjekty údajů, vývozci údajů a vnitrostátní orgány pro ochranu údajů, schopny identifikovat organizace, které zásady přijaly. Za tímto účelem se Ministerstvo obchodu zavázalo vést a veřejně zpřístupnit seznam organizací, které autocertifikovaly (samy osvědčily) přijetí zásad a které podléhají pravomoci alespoň jednoho z donucovacích orgánů uvedených v přílohách I a II tohoto rozhodnutí (dále jen „seznam organizací štítu na ochranu soukromí“) ⁽³⁴⁾. Ministerstvo obchodu bude tento seznam aktualizovat na základě každoročních recertifikací organizací a kdykoli některá organizace štít EU–USA na ochranu soukromí opustí nebo z něj bude odstraněna. Ministerstvo rovněž povede a veřejnosti zpřístupní autoritativní evidenci organizací, které byly ze seznamu odstraněny, v každém jednotlivém případě s uvedením důvodu pro toto odstranění. Ministerstvo také poskytne odkaz na seznam případů Federální obchodní komise souvisejících s prosazováním zásad štítu na ochranu soukromí zveřejněný na webu FTC.
- (32) Ministerstvo obchodu seznam organizací štítu na ochranu soukromí i recertifikace veřejně zpřístupní na zvláštním webu. Autocertifikované organizace pak musí poskytnout adresu tohoto webu ministerstva, kde je zveřejněn seznam organizací štítu na ochranu soukromí. Zveřejňuje-li organizace politiku ochrany soukromí online, musí být navíc v této police uveden hypertextový odkaz na web štítu na ochranu soukromí a hypertextový odkaz na web nebo na formulář pro podávání stížností v rámci nezávislého odvolacího mechanismu, který je k dispozici pro prošetřování nevyřešených stížností. Ministerstvo obchodu bude systematicky v kontextu certifikace a recertifikace organizace ověřovat, zda její politika ochrany soukromí splňuje zásady.
- (33) Organizace, které soustavně nedodržují zásady, budou odstraněny ze seznamu organizací a musí vrátit nebo smazat osobní údaje, které obdržely v rámci štítu EU–USA na ochranu soukromí. V jiných případech odstranění, například pokud organizace dobrovolně ukončí účast ve štítu nebo pokud se neregistruje, si organizace může takové údaje ponechat, pokud Ministerstvo obchodu každoročně ujistí o svém závazku řídit se zásadami nebo pokud osobním údajům zajistí odpovídající ochranu jiným povoleným způsobem (např. smlouvou, která plně vyhovuje požadavkům příslušných standardních smluvních doložek schválených Komisí). V tomto případě musí organizace určit kontaktní místo uvnitř organizace pro veškeré otázky související se štítem na ochranu soukromí.
- (34) Ministerstvo obchodu bude monitorovat organizace, které již nejsou členem štítu EU–USA na ochranu soukromí buď proto, že jej dobrovolně opustily, nebo že skončila platnost jejich certifikace, za účelem ověření, zda vrátí, vymažou nebo si ponechají ⁽³⁵⁾ osobní údaje dříve získané v rámci štítu. Pokud si tyto údaje ponechají, jsou

⁽³²⁾ Situace se různí v závislosti na tom, zda je třetí strana správcem, nebo zpracovatelem (zprostředkovatelem). V prvním scénáři musí smlouva s třetí stranou stanovit, že tato třetí strana přestane zpracovávat nebo přijme jiné přiměřené a vhodné kroky k nápravě této situace. Ve druhém scénáři pak tato opatření přijímá organizace účastníci se štítu na ochranu soukromí – tedy ta, která spravuje zpracování a jejímiž pokyny se řídí zprostředkovatel.

⁽³³⁾ V tomto případě musí organizace USA 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) aby na základě oznámení ukončila a napravila nepovolené zpracovávání.

⁽³⁴⁾ Informace o správě seznamu organizací štítu na ochranu soukromí lze nalézt v příloze I a II (oddíl I bod 3, oddíl I bod 4, oddíl III bod 6 písm. d) a oddíl III bod 11 písm. g)).

⁽³⁵⁾ Viz např. příloha II, oddíl I bod 3, oddíl III bod 6 písm. f) a oddíl III bod 11 písm. g) podbod i).

organizace povinny na ně i nadále uplatňovat zásady. V případech, kdy Ministerstvo obchodu odstraní organizace z rámce štítu kvůli soustavnému nedodržování zásad, zajistí, aby tyto organizace musely vrátit nebo vymazat osobní údaje, které v rámci štítu získaly.

- (35) Pokud organizace z jakéhokoli důvodu opustí štít EU–USA na ochranu soukromí, musí odstranit veškerá veřejná prohlášení, která implikují, že se štítu EU–USA na ochranu soukromí nadále účastní nebo že má nárok na výhody z něj plynoucí, a zejména veškeré odkazy na štít EU–USA na ochranu soukromí v politice ochrany soukromí, kterou organizace zveřejňuje. Ministerstvo obchodu bude vyhledávat a řešit nepravdivá tvrzení o účasti v rámci včetně ze strany bývalých členů⁽³⁶⁾. Jakékoli uvedení široké veřejnosti v omyl ohledně přijetí zásad zavádějícími prohlášeními nebo postupy je postižitelné Federální obchodní komisí, Ministerstvem dopravy nebo jiným příslušným donucovacím orgánem USA; uvedení Ministerstva obchodu v omyl je postižitelné podle zákona o nepravdivých tvrzeních (*False Statements Act*, 18 U. S. C. § 1001)⁽³⁷⁾.
- (36) Ministerstvo obchodu bude z moci úřední monitorovat jakákoli nepravdivá tvrzení o účasti ve štítu na ochranu soukromí či podvodné použití certifikační značky štítu a orgány pro ochranu údajů mohou organizace postupovat specializovanému kontaktnímu místu ministerstva ke kontrole. Pokud organizace opustí štít EU–USA na ochranu soukromí, neregistruje se, nebo je odstraněna ze seznamu organizací štítu na ochranu soukromí, bude Ministerstvo obchodu průběžně ověřovat, zda organizace ze své politiky ochrany soukromí, kterou zveřejňuje, odstranila veškeré odkazy na štít na ochranu soukromí, které implikují, že se jej nadále účastní, a pokud s nepravdivými tvrzeními nepřestane, postoupí věc Federální obchodní komisi, Ministerstvu dopravy nebo jinému kompetentnímu úřadu za účelem případného postihu. Ministerstvo obchodu také organizacím, kterým autocertifikace končí nebo které dobrovolně opustily štít EU–USA na ochranu soukromí, rozešle dotazníky za účelem ověření, zda organizace osobní údaje, které obdržela během své účasti ve štítu EU–USA na ochranu soukromí, vrátí, vymaže, nebo zda na ně bude nadále uplatňovat zásady ochrany soukromí, a pokud údaje mají být nadále uchovány, za účelem ověření, kdo uvnitř organizace bude nadále fungovat jako kontaktní místo pro otázky související se štítem na ochranu soukromí.
- (37) Ministerstvo obchodu bude průběžně a z moci úřední prozkoumávat dodržování zásad⁽³⁸⁾ v autocertifikovaných organizacích, mimo jiné zasíláním podrobných dotazníků. Systematické kontroly bude provádět, také kdykoli obdrží konkrétní (nikoli bezdůvodnou) stížnost, pokud organizace na jeho dotazy neodpoví uspokojivě, nebo pokud existují věrohodné důkazy nasvědčující tomu, že organizace pravděpodobně nedodržuje zásady. Ve vhodných případech bude Ministerstvo obchodu prováděcí těchto přezkumů dodržování zásad konzultovat s orgány pro ochranu údajů.

2.3 Nápravné mechanismy, vyřizování stížností a prosazování

- (38) Štít EU–USA na ochranu soukromí prostřednictvím *zásady odvolání, prosazování a odpovědnosti* po organizacích požaduje, aby fyzickým osobám, které byly poškozeny nedodržením zásad, poskytly možnosti odvolání, a tudíž aby subjektům údajů z EU daly možnost podávat stížnosti týkající se nedodržování zásad ze strany autocertifikovaných společností z USA a dosáhnout vyřešení těchto stížností, případně formou rozhodnutí poskytujícího účinnou nápravu.
- (39) V rámci autocertifikace musí organizace vyhovět požadavkům zásady odvolání, prosazování a odpovědnosti, a to zajištěním účinných a snadno dostupných nezávislých odvolacích mechanismů, pomocí kterých lze stížnosti fyzických osob a spory vyšetřit a promptně vyřešit, aniž by fyzické osobě vznikly náklady.
- (40) Organizace si mohou zvolit nezávislé odvolací mechanismy buď v Unii nebo ve Spojených státech. Sem patří možnost dobrovolného závazku ke spolupráci s orgány EU pro ochranu údajů. Tato volba však není možná,

⁽³⁶⁾ Viz příloha I, oddíl „Bude hledat a řešit nepravdivá tvrzení o účasti“.

⁽³⁷⁾ Viz příloha II, oddíl III bod 6 písm. h) a oddíl III bod 11 písm. f).

⁽³⁸⁾ Viz příloha I.

pokud organizace zpracovávají údaje o lidských zdrojích, neboť v tom případě je spolupráce s orgány pro ochranu údajů povinná. K dalším alternativám patří nezávislé alternativní řešení sporů nebo soukromým sektorem vyvinuté *programy na ochranu soukromí*, do kterých jsou začleněny zásady ochrany soukromí. Programy na ochranu soukromí musí obsahovat účinné donucovací mechanismy v souladu s požadavky zásady odvolání, prosazování a odpovědnosti. Organizace jsou povinny napravit veškeré problémy související s neplněním zásad. Musí také uvést, že podléhají vyšetřovací a donucovací pravomoci Federální obchodní komise, Ministerstva dopravy nebo jiného pověřeného, zákonem zřízeného orgánu USA.

- (41) Rámec štítu na ochranu soukromí tedy subjektům údajů poskytuje řadu možností jak uplatnit svá práva, podávat stížnosti týkající se nedodržování zásad ze strany autocertifikovaných společností z USA a dosáhnout vyřešení těchto stížností, případně formou rozhodnutí poskytujícího účinnou nápravu. Fyzické osoby mohou stížnost předložit přímo organizaci, nezávislému subjektu pro řešení sporů označeného organizací, vnitrostátnímu orgánu pro ochranu údajů nebo Federální obchodní komisi.
- (42) V případech, kdy jejich stížnosti nebyly vyřešeny ani jedním z odvolacích či donucovacích mechanismů, mají fyzické osoby také právo využít závazného rozhodčího řízení u panelu štítu na ochranu soukromí (příloha 1 přílohy II 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. Existuje však doporučený logický postup, který je rozveden níže.
- (43) Za prvé, subjekty údajů z EU mohou případy nedodržení zásad řešit přímým kontaktováním *autocertifikované společnosti z USA*. 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), a o nezávislých mechanismech vyřizování stížností.
- (44) Po přijetí stížnosti fyzické osoby buď přímo od ní nebo prostřednictvím Ministerstva obchodu v návaznosti na postoupení orgánem pro ochranu údajů musí organizace subjektu údajů z EU odpovědět do 45 dní. Tato odpověď musí obsahovat posouzení důvodnosti stížnosti a informace o tom, jak bude problém napraven. Organizace jsou taktéž povinny promptně odpovídat na dotazy a jiné žádosti o informace ze strany Ministerstva obchodu nebo orgánu pro ochranu údajů ⁽³⁹⁾ (pokud se organizace zavázala s ním spolupracovat) týkající se jejich přijetí zásad. Organizace musí uchovávat záznamy o provádění svých politik ochrany soukromí a na žádost v souvislosti s vyšetřováním nebo stížností na nedodržování zásad je poskytovat nezávislému odvolacímu orgánu nebo Federální obchodní komisi (nebo jinému orgánu USA příslušnému vyšetřovat nekalé a klamavé praktiky).
- (45) 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, aby šetřil a řešil stížností fyzických osob (nejsou-li zjevně nepodložené nebo bezdůvodné) a zdarma fyzickým osobám poskytoval odpovídající právní ochranu. Sankce a opravné prostředky uložené takovým subjektem musí být natolik přísné, aby bylo zajištěno dodržení zásad ze strany organizací, a měly by organizacím umožňovat obrácení nebo nápravu účinků nedodržování zásad a dále v závislosti na okolnostech by měly zajistit ukončení dalšího zpracovávání dotčených osobních údajů a/nebo jejich výmaz a také sloužit k propagaci zjištění o nedodržení zásad. Nezávislé subjekty pro řešení sporů ustanovené organizací budou povinny na svých veřejných webech uvádět relevantní informace týkající se štítu EU–USA na ochranu soukromí a služby, které v jeho rámci poskytují. Každý rok musí zveřejnit výroční zprávu s uvedením souhrnných statistik ohledně těchto služeb ⁽⁴⁰⁾.

⁽³⁹⁾ Jde o vyřizující orgán pověřený panelem orgánů pro ochranu údajů stanovený v doplňkové zásadě „Úloha orgánů pro ochranu údajů“ (příloha II, oddíl III bod 5).

⁽⁴⁰⁾ Výroční zpráva musí obsahovat: 1) celkový počet stížností v souvislosti se štítem na ochranu soukromí obdržených během vykazovaného roku; 2) druhy obdržených stížností; 3) opatření k zajištění kvality řešení sporů, např. délky zpracování stížností; a 4) výsledky obdržených stížností, zejména počet a druh uložených opravných prostředků nebo sankcí.

- (46) V rámci svého přezkumu dodržování zásad bude Ministerstvo obchodu ověřovat, zda se autocertifikované společnosti z USA skutečně zaregistrovaly u nezávislých odvolacích orgánů, u kterých se dle vlastního tvrzení zaregistrovat měly. Jak organizace, tak odpovědné nezávislé odvolací orgány jsou povinny promptně odpovídat na dotazy a žádosti Ministerstva obchodu o informace týkající se štítu na ochranu soukromí.
- (47) 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 nekalé a klamavé praktiky), nebo příslušnému soudu ⁽⁴¹⁾. 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 nedodržuje zásady často, bude to chápáno jako soustavné nedodržování zásad s tím výsledkem, že Ministerstvo obchodu poté, co nejprve v 30denní lhůtě poskytne organizaci, která nedodržela zásady, možnost vyjádřit se, vyškrtne organizaci ze seznamu ⁽⁴²⁾. Pokud po odstranění ze seznamu organizace nadále tvrdí, že je certifikována v rámci štítu na ochranu soukromí, postoupí Ministerstvo obchodu věc Federální obchodní komisi či jinému donucovacímu orgánu ⁽⁴³⁾.
- (48) Za třetí mohou fyzické osoby podávat stížnosti u vnitrostátního orgánu pro ochranu údajů. Organizace jsou povinny spolupracovat s orgánem pro ochranu údajů na šetření a vyřešení stížnosti, buď pokud se týká zpracování údajů o lidských zdrojích shromážděných v kontextu zaměstnaneckého vztahu, nebo pokud se příslušná organizace dobrovolně podřídila dohledu orgánů pro ochranu údajů. Konkrétně musí organizace odpovídat na dotazy, řídit se doporučeními orgánu pro ochranu údajů, pokud jde mimo jiné o nápravné nebo odškodňující opatření, a předkládat orgánu pro ochranu údajů písemná potvrzení o tom, že příslušný krok byl podniknut.
- (49) Orgány pro ochranu údajů poskytují doporučení prostřednictvím neformálního panelu orgánů pro ochranu údajů vytvořeného na úrovni Unie ⁽⁴⁴⁾, jehož smyslem je přispět k harmonizovanému a koherentnímu přístupu k jednotlivým stížnostem. Doporučení se vydá poté, co byla oběma stranám sporu poskytnuta dostatečná příležitost vyjádřit stanovisko a předložit jakékoli důkazy. Panel vydá doporučení v co nejkratší době v souladu s požadavkem na spravedlivé řízení a obecně do 60 dní po obdržení stížnosti. Jestliže se organizace nepodrobí doporučení do 25 dnů od jeho doručení a zpoždění uspokojivě nevysvětlí, vydá panel 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 právního předpisu). V druhém případě panel informuje Ministerstvo obchodu, které toto odmítnutí organizace podrobit se doporučení orgánu pro ochranu údajů posoudí jako soustavné nedodržování zásad, což povede k odstranění organizace ze seznamu organizací štítu na ochranu soukromí.
- (50) Pokud orgán pro ochranu 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.
- (51) Fyzické osoby mohou stížnosti u orgánů pro ochranu údajů podávat i v případě, kdy panel orgánů pro ochranu údajů nebyl organizací určen jako její subjekt pro řešení sporů. V těchto případech může orgán pro ochranu 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 účastnících se štítu na ochranu soukromí zřídí Ministerstvo obchodu specializované kontaktní místo, které bude fungovat jako styčný bod a které bude orgánům pro ochranu údajů pomáhat s dotazy na dodržování zásad ze strany organizací ⁽⁴⁵⁾. Taktéž Federální obchodní komise se zavázala zřídit zvláštní kontaktní místo ⁽⁴⁶⁾ a poskytovat orgánům pro ochranu údajů pomoc při šetřeních v souladu se zákonem o bezpečném internetu ⁽⁴⁷⁾.

⁽⁴¹⁾ Viz příloha II, oddíl III bod 11 písm. e).

⁽⁴²⁾ Viz příloha II, oddíl III bod 11 písm. g), zejména podbody ii) a iii).

⁽⁴³⁾ Viz příloha I, oddíl „Bude hledat a řešit nepravdivá tvrzení o účasti“.

⁽⁴⁴⁾ Jednací řád neformálního panelu orgánů pro ochranu údajů by měly orgány pro ochranu údajů sestavit podle toho, jak jsou schopny zorganizovat svou činnost a vzájemnou spolupráci.

⁽⁴⁵⁾ Viz příloha I, oddíl „Prohloubí spolupráci s orgány pro ochranu údajů“ a „Usnadní řešení stížností na nedodržování zásad“ a příloha II oddíl II bod 7 písm. e).

⁽⁴⁶⁾ Viz příloha IV, s. 6.

⁽⁴⁷⁾ Tamtéž.

- (52) Za čtvrté, Ministerstvo obchodu se zavázalo přijímat a posuzovat stížnosti na nedodržování zásad ze strany organizace a vynaložit veškeré rozumné úsilí k jejich vyřešení. K tomuto účelu poskytuje Ministerstvo obchodu orgánům pro ochranu údajů zvláštní postupy pro postupování stížností specializovanému kontaktnímu místu, jejich sledování a dořešení se společnostmi. Aby bylo zpracování jednotlivých stížností co nejrychlejší, kontaktní místo jedná ve věcech dodržování zásad v přímé součinnosti s příslušným orgánem pro ochranu údajů a zejména jej během nejvýše 90 dní od postoupení informuje o stavu stížností. Subjekty údajů mohou díky tomu stížnosti na nedodržení zásad ze strany autocertifikovaných společností z USA podávat u svých vnitrostátních orgánů pro ochranu údajů, které pak tyto stížnosti zašlou Ministerstvu obchodu jakožto orgánu USA spravujícímu štít EU–USA na ochranu soukromí. Ministerstvo obchodu se také zavázalo vypracovat v rámci každoročního přezkumu fungování štítu EU–USA na ochranu soukromí zprávu souhrnně analyzující stížnosti, které každý rok obdrží ⁽⁴⁸⁾.
- (53) Pokud Ministerstvo obchodu na základě vlastních ověření z moci úřední, stížností nebo jiných informací dospěje k závěru, že organizace soustavně nedodržuje zásady ochrany soukromí, odstraní takovou organizaci ze seznamu organizací štítu na ochranu soukromí. Odmítnutí podřídit se konečnému rozhodnutí vydanému jakýmkoli samoregulačním subjektem pro otázky ochrany soukromí, nezávislým subjektem pro řešení sporů nebo vládním subjektem, včetně orgánu pro řešení sporů, bude chápáno jako soustavné nedodržování zásad.
- (54) Za páté, organizace účastníci se štítu na ochranu soukromí musí podléhat vyšetřovací a donucovací pravomoci orgánů USA, zejména pak *Federální obchodní komise* ⁽⁴⁹⁾, která účinně zajišťuje dodržování zásad. Federální obchodní komise bude prioritně řešit případy nedodržení zásad ochrany soukromí postoupené nezávislými subjekty pro řešení sporů nebo samoregulačními orgány, Ministerstvem obchodu a orgány pro ochranu údajů (jednajícími z vlastní iniciativy nebo na základě stížnosti) za účelem stanovení, zda byl porušen § 5 zákona o Federální obchodní komisi (*Federal Trade Commission Act*) ⁽⁵⁰⁾. Federální obchodní komise se zavázala vytvořit standardizovaný postup postupování případů, ustanovit kontaktní místo uvnitř komise pro případy postoupené orgány pro ochranu údajů, a sdílet informace o postupovaných případech. Kromě toho bude přijímat přímé stížnosti fyzických osob a z vlastní iniciativy provádět šetření případů souvisejících se štítem na ochranu soukromí, zejména jako součást jejich vlastních širších šetření případů porušení soukromí.
- (55) Federální obchodní komise může prosazovat dodržování zásad správními příkazy (*consent orders*) a bude systematicky monitorovat plnění těchto příkazů. Pokud organizace příkaz neplní, Federální obchodní komise smí takový příkaz postoupit příslušnému soudu, aby v občanskoprávním řízení rozhodl o odpovědnosti a jiných opravných prostředcích, včetně za jakoukoli újmu způsobenou nezákonným jednáním. Federální obchodní komise může případně také přímo požádat federální soud o předběžný nebo trvalý soudní příkaz nebo jiné opravné prostředky. Každý *consent order* vydaný organizací, která se účastní štítu na ochranu soukromí, bude obsahovat ustanovení o podávání zpráv ⁽⁵¹⁾ a organizace budou povinny zveřejnit jakoukoli relevantní, štítu na ochranu soukromí se týkající část každé hodnotící zprávy nebo zprávy o dodržování zásad předložené Federální obchodní komisi. A konečně Federální obchodní komise povede online seznam společností, jimž byl vydán soudní příkaz nebo příkaz správní FTC v případech týkajících se štítu na ochranu soukromí.
- (56) Za šesté, v případě, že žádnou z ostatních dostupných možností nápravy nebyla stížnost fyzické osoby vyřešena, smí subjekt údajů z EU využít závazného rozhodčího řízení u „panelu štítu na ochranu soukromí (*Privacy Shield Panel*)“. Organizace musí fyzické osoby informovat o tom, že za určitých podmínek mají možnost využít závazného rozhodčího řízení, a jsou povinny reagovat, jakmile fyzická osoba tuto možnost využila zasláním oznámení dotčené organizaci ⁽⁵²⁾.

⁽⁴⁸⁾ Viz příloha I, oddíl „Usnadnění řešení stížností na nedodržování zásad“.

⁽⁴⁹⁾ Organizace účastníci se štítu na ochranu soukromí musí veřejně deklarovat závazek dodržovat zásady, veřejně zpřístupnit politiku ochrany soukromí v souladu s těmito zásadami a plně tyto zásady 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.

⁽⁵⁰⁾ Podle jejích vlastních informací nemá Federální obchodní komise pravomoc vykonávat kontroly na místě v oblasti ochrany soukromí. Má však pravomoc přikázat organizacím, aby předložily dokumenty a poskytly svědecké výpovědi (viz § 20 zákona o Federální obchodní komisi) a k vymození takových příkazů v případě jejich nesplnění smí použít systém soudů.

⁽⁵¹⁾ Soudní příkazy nebo příkazy FTC mohou společnostem 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.

⁽⁵²⁾ Viz příloha II, oddíl II bod 1 (podbod xi) a oddíl III bod 7 písm. c).

- (57) Tento rozhodčí panel bude sestávat ze skupiny nejméně 20 rozhodců jmenovaných Ministerstvem obchodu a Komisí na základě jejich nezávislosti, bezúhonnosti a zkušeností v právu USA o ochraně soukromí i v právu EU o ochraně údajů. Pro každý jednotlivý spor strany z této skupiny vyberou panel jednoho nebo tří rozhodců⁽⁵³⁾. Řízení se bude řídit standardními rozhodčími pravidly, na nichž se Ministerstvo obchodu a Komise dohodnou. Tato pravidla doplní již uzavřený rámec, který obsahuje několik rysů, jež zvyšují dostupnost tohoto mechanismu pro subjekty údajů z EU: i) při přípravě podnětů pro panel může subjekt údajů pomáhat jeho vnitrostátní orgán pro ochranu údajů; ii) přestože se řízení bude konat ve Spojených státech, mají subjekty údajů v EU 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 obvykle⁽⁵⁴⁾ a zdarma poskytnuto tlumočení; iv) a konečně poněvadž každá ze stran musí hradit odměnu pro svého právního zástupce, je-li jím před panelem zastupována, zřídí Ministerstvo obchodu fond financovaný z ročních příspěvků organizací štítu na ochranu soukromí, z nějž budou hrazeny způsobilé náklady rozhodčího řízení až do maximální částky, kterou stanoví orgány USA v konzultaci s Komisí.
- (58) Panel štítu na ochranu soukromí bude mít pravomoc ukládat „individuální, nepeněžité přiměřené opatření“⁽⁵⁵⁾, které je nezbytné k nápravě nedodržení zásad. Panel sice ve svém rozhodování zohlední jiné opravné prostředky získané prostřednictvím jiných mechanismů štítu na ochranu soukromí, pokud však mají fyzické osoby za to, že tyto jiné opravné prostředky jsou nepostačující, mohou využít rozhodčího řízení. To subjektům údajů z EU umožní, aby využívali rozhodčího řízení ve všech případech, kdy opatření 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 autocertifikované společnosti z USA ze zákona oprávněn řešit orgán pro ochranu údajů, zejména v případech, kdy je organizace buď povinna spolupracovat a řídit se doporučením orgánu pro ochranu údajů, pokud jde o zpracování údajů o lidských zdrojích shromážděných v kontextu zaměstnávání, 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 společnost nedodrží zásady ochrany údajů.
- (59) Za sedmé, pokud organizace poruší svůj závazek dodržovat zásady a politiku ochrany soukromí, kterou zveřejnila, mohou dodatečné možnosti soudní nápravy poskytovat právní předpisy jednotlivých států USA, které stanoví procesní prostředky v rámci práva mimosmluvních občanskoprávních deliktů a v případech podvodného uvedení v omyl, nekalého nebo klamavého jednání či praktik nebo porušení smlouvy.
- (60) Pokud navíc orgán pro ochranu údajů po přijetí nároku subjektu údajů z EU shledá, že předání osobních údajů fyzické osoby organizaci ve Spojených státech proběhlo v rozporu s právem EU v oblasti ochrany údajů, včetně případů, kdy vývozce údajů z EU má důvod se domnívat, že organizace nedodržuje zásady, může také uplatnit své pravomoci vůči vývozci údajů a v případě potřeby vydat příkaz k pozastavení předání údajů.
- (61) Ve světle informací uvedených v tomto oddíle má Komise za to, že zásady vydané Ministerstvem obchodu USA jako takové zajišťují úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni ochrany zaručené hmotněprávními základními zásadami stanovenými ve směrnici 95/46/ES.
- (62) Účinné uplatňování zásad kromě toho zaručují povinnosti ohledně transparentnosti a správa štítu na ochranu soukromí a přezkum dodržování zásad štítu vykonávané Ministerstvem obchodu.
- (63) Komise má dále za to, že dohledové, odvolací a donucovací mechanismy stanovené štítem na ochranu soukromí jako celek umožňují, aby porušení zásad ze strany organizací, které jsou součástí štítu na ochranu soukromí, byla v praxi odhalována a postihována, a poskytují subjektu údajů procesní prostředky, které mu umožní získat přístup k osobním údajům, které se jej týkají, a v konečném důsledku dosáhnout opravy nebo výmazu takových údajů.

⁽⁵³⁾ Na počtu rozhodců v panelu se strany budou muset dohodnout.

⁽⁵⁴⁾ Panel však může shledat, že za okolností konkrétního rozhodčího řízení by krytí těchto výdajů vedlo k bezdůvodným nebo neúměrným nákladům.

⁽⁵⁵⁾ Fyzické osoby se sice v rozhodčím řízení nemohou domáhat náhrady škody, využití rozhodčího řízení ovšem nevylučuje možnost domáhat se náhrady škody u běžných soudů USA.

3. PŘÍSTUP ORGÁNŮ VEŘEJNÉ MOCI USA K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM V RÁMCI ŠTÍTU EU–USA NA OCHRANU SOUKROMÍ A POUŽITÍ TĚCHTO ÚDAJŮ TĚMITO ORGÁNY

- (64) Jak vyplývá z přílohy II oddílu I bodu 5, přijetí zásad je omezeno v rozsahu nezbytném ke splnění požadavků národní bezpečnosti, veřejného zájmu či prosazování práva.
- (65) Komise posoudila omezení a ochranná opatření, která jsou k dispozici v právu USA, pokud jde o přístup orgánů veřejné moci USA k osobním údajům předávaným v rámci štítu EU–USA na ochranu soukromí a použití těchto údajů těmito orgány pro účely národní bezpečnosti, prosazování práva a jiné účely veřejného zájmu. Vláda USA kromě toho prostřednictvím Úřadu ředitele národních zpravodajských služeb (*Office of the Director of National Intelligence*, ODNI) ⁽⁵⁶⁾ poskytla Komisi podrobná prohlášení a závazky, které jsou uvedeny v příloze VI tohoto rozhodnutí. Dopisem ministra zahraničních věcí, který tvoří přílohu III tohoto rozhodnutí, se vláda USA zavázala rovněž vytvořit nový mechanismus pro dohled nad zásahy z důvodu národní bezpečnosti, úřad ombudsmana ve věcech štítu na ochranu soukromí, který je nezávislý na zpravodajské komunitě. A konečně prohlášení Ministerstva spravedlnosti USA, které tvoří přílohu VII tohoto rozhodnutí, popisuje omezení a ochranná opatření použitelná na přístup orgánů veřejné správy k údajům a jejich použití těmito orgány pro účely prosazování práva a jiné účely veřejného zájmu. Pro vyšší transparentnost a aby byla podtrhnuta právní povaha těchto závazků, bude každý z výše uvedených dokumentů připojených k tomu rozhodnutí zveřejněn ve Federálním úředním věstníku USA (*U.S. Federal Register*).
- (66) Zjištění Komise o omezeních přístupu orgánů veřejné moci USA k osobním údajům předávaným z Evropské unie do Spojených států, o omezení jejich použití těmito orgány a o existenci účinné právní ochrany jsou dále podrobně rozvedena níže.

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

- (67) Z analýzy Komise plyne, že právo USA obsahuje několik omezení přístupu orgánů veřejné moci USA k osobním údajům předávaným v rámci štítu EU–USA na ochranu soukromí pro účely národní bezpečnosti a použití těchto údajů těmito orgány, jakož i dohledové a nápravné mechanismy, které poskytují dostatečná ochranná opatření k tomu, aby byly tyto údaje účinně ochráněny před nezákonnými zásahy a rizikem zneužití ⁽⁵⁷⁾. Od roku 2013, kdy Komise zveřejnila dvě sdělení k tomuto tématu (viz 7. bod odůvodnění), byl tento právní rámec významně posílen, jak je popsáno níže.

3.1.1 Omezení

- (68) Podle Ústavy USA spadá zajištění národní bezpečnosti do pravomoci prezidenta jakožto vrchního velitele ozbrojených sil a vrchního představitele výkonné moci, a pokud jde o zahraniční zpravodajství, do jeho pravomoci jednat v zahraničních věcech USA ⁽⁵⁸⁾. Kongres USA sice má právo ukládat omezení, a v minulosti tak v mnoha ohledech učinil, v těchto mezích však prezident smí řídit činnost zpravodajské komunity USA, zejména prostřednictvím výkonných dekretů nebo prezidentských směrnic. To se samozřejmě týká i oblastí, pro které pokyny Kongresu neexistují. Dvěma ústředními právními nástroji v tomto smyslu v současnosti jsou výkonný dekret 12333 (*Executive Order 12333*, dále také jen „EO 12333“) ⁽⁵⁹⁾ a prezidentská politická směrnice 28.

⁽⁵⁶⁾ Ředitel národních zpravodajských služeb (DNI) předsedá zpravodajské komunitě a je hlavním poradcem prezidenta USA a Národní bezpečnostní rady. Viz zákon o reformě zpravodajských služeb a prevenci terorismu, *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. 108-458, ze dne 17. prosince 2004. Úřad kromě jiného stanoví požadavky na úkolování, sběr, analýzu, zpracování a šíření národních zpravodajských informací zpravodajskou komunitou a spravuje a řídí tyto činnosti, a to mimo jiné vypracováním pokynů o přístupu k informacím nebo zpravodajským poznatkům, jejich použití a sdílení. Viz § 1.3(a), (b) výkonného dekretu EO 12333.

⁽⁵⁷⁾ Viz *Schrems*, bod 91.

⁽⁵⁸⁾ Ústava USA, článek II. Viz také úvod směrnice PPD-28.

⁽⁵⁹⁾ EO 12333: *United States Intelligence Activities*, Federal Register Vol. 40, No. 235 (ze dne 8. prosince 1981). V rozsahu, v jakém je tento dokument veřejně přístupný, definuje tento výkonný dekret cíle, směry, povinnosti a odpovědnosti zpravodajské činnosti USA (včetně úloh jednotlivých prvků zpravodajské komunity) a stanoví obecné parametry provádění zpravodajské činnosti (zejména potřebu stanovit konkrétní procesní pravidla). Dle § 3.2 EO 12333 vydává takové příslušné směrnice, postupy a pokyny, jaké mohou být nezbytné k provedení dekretu, prezident, jemuž je nápomocna Národní bezpečnostní rada.

(69) Prezidentská politická směrnice 28 (*Presidential Political Directive*, dále také jen „PPD-28“) ze dne 17. ledna 2014 ukládá řadu omezení operací „signálového zpravodajství“⁽⁶⁰⁾. Tato prezidentská směrnice je závazná pro zpravodajské orgány USA⁽⁶¹⁾ a zůstává v platnosti i po změně administrativy USA⁽⁶²⁾. Směrnice PPD-28 je zvláště důležitá pro osoby, které nejsou občany USA, včetně subjektů údajů z EU. Směrnice mimo jiné stanoví, že:

- a) sběr signálových zpravodajských informací musí být podložen zákonem nebo zmocněním prezidenta a musí být prováděn v souladu s Ústavou USA (zejména jejím čtvrtým dodatkem) a zákony USA;
- b) se všemi osobami by mělo být zacházeno důstojně a s úctou bez ohledu na jejich státní příslušnost či bydliště;
- c) všechny osoby mají z hlediska ochrany soukromí legitimní zájem o to, jak je s jejich osobními informacemi nakládáno;
- d) soukromí a občanské svobody jsou nedílnou součástí plánování činnosti signálového zpravodajství USA;
- e) činnosti signálového zpravodajství USA proto musí obsahovat příslušná opatření na ochranu osobních informací všech fyzických osob neohledně na jejich státní příslušnost či bydliště.

(70) Směrnice PPD-28 ukládá, aby signálové zpravodajské informace byly shromažďovány výhradně tehdy, existuje-li z důvodu zahraničního zpravodajství či kontrašpionáže účel podpory národních a ministerských misí, a pro žádný jiný účel (např. pro poskytnutí konkurenční výhody společností z USA). V tomto ohledu, jak vysvětluje ODNI, by prvky zpravodajské komunity „měly vyžadovat, aby sběr, kdykoli je to proveditelné, byl soustředěn na konkrétní cíle nebo témata zahraničního zpravodajství, a to za použití diskriminantů (např. specifických komunikačních prostředků, selekčních termínů a identifikátorů)“⁽⁶³⁾. Prohlášení poskytují dále ujištění v tom smyslu, že rozhodnutí o sběru zpravodajských informací nejsou na uvážení jednotlivých zpravodajských úředníků, nýbrž podléhají politice a postupům, které jsou jednotlivé prvky (agentury) zpravodajské komunity USA povinny zavést v rámci provádění směrnice PPD-28⁽⁶⁴⁾. Hledání a určování vhodných selektorů tak probíhá v zastřešujícím „rámcu priorit národního zpravodajství“ (*National Intelligence Priorities Framework*, NIPF), jehož cílem je, aby zpravodajské priority byly stanovovány tvůrci politik na vysoké úrovni a aby byly pravidelně přezkoumávány tak, aby pohotově reagovaly na aktuální hrozby národní bezpečnosti a zohledňovaly možná rizika, včetně rizik z hlediska ochrany soukromí⁽⁶⁵⁾. Na tomto základě pracovníci zpravodajské agentury vyhledávají a určují konkrétní selekční termíny, díky nimž budou nasbírány zahraniční zpravodajské informace, které pohotově reagují na priority⁽⁶⁶⁾. Selektory musí být pravidelně přezkoumávány, zda i nadále poskytují cenné zpravodajské informace v souladu s prioritami⁽⁶⁷⁾.

⁽⁶⁰⁾ Podle EO 12333 je funkčním manažerem pro signálové zpravodajství a jednotnou organizaci činností signálového zpravodajství řídí ředitel Národní bezpečnostní agentury (NSA).

⁽⁶¹⁾ Definice termínu „zpravodajská komunita“ viz § 3.5 (h) EO 12333 spolu s pozn. 1 ve směrnici PPD-28.

⁽⁶²⁾ Viz dokument Memorandum by the Office of Legal Counsel, Department of Justice, to President Clinton, ze dne 29. ledna 2000. Podle tohoto právního stanoviska mají prezidentské směrnice „stejný hmotněprávní účinek jako výkonný dekret“.

⁽⁶³⁾ Prohlášení ODNI (příloha VI), s. 3.

⁽⁶⁴⁾ Viz § 4(b),(c) směrnice PPD-28. Podle veřejně dostupných informací potvrdil přezkum za rok 2015 stávajících šest účelů. Viz dokument ODNI – Signals Intelligence Reform, 2016 Progress Report.

⁽⁶⁵⁾ Prohlášení ODNI (příloha VI), s. 6 (s odkazem na směrnici Intelligence Community Directive 204). Viz také § 3 směrnice PPD-28.

⁽⁶⁶⁾ Prohlášení ODNI (příloha VI), s. 6. Viz např. dokument Kanceláře NSA pro občanské svobody a soukromí (NSA CLPO) – NSA’s Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 ze dne 7. října 2014. Dále viz dokument ODNI Status Report 2014. Pro žádosti o přístup podle § 702 zákona FISA se žádosti řídí minimalizačními postupy schválenými Soudem pro uplatňování zákona FISA. Viz dokument NSA CLPO – NSA’s Implementation of Foreign Intelligence Surveillance Act Section 702 ze dne 16. dubna 2014.

⁽⁶⁷⁾ Viz dokument Signals Intelligence Reform, 2015 Anniversary Report. Viz také prohlášení ODNI (příloha VI), s. 6, 8–9, 11.

- (71) Dále požadavky uvedené ve směrnici PPD-28 ukládají, aby sběr zpravodajských informací byl vždy ⁽⁶⁸⁾ „v nejvyšší možné míře uzpůsoben na míru,“ a aby zpravodajská komunita upřednostňovala jiné dostupné informace a vhodné a proveditelné alternativy ⁽⁶⁹⁾, a reflektovala obecné pravidlo upřednostňování cíleného sběru nad hromadným. Dle ujištění ODNI tyto požadavky zejména zajišťují, aby hromadný sběr nebyl „masový“ ani „nahodilý“ aby se z výjimky nestalo pravidlo ⁽⁷⁰⁾.
- (72) Směrnice PPD-28 vysvětluje, že prvky zpravodajské komunity musí někdy za určitých okolností shromažďovat signálové zpravodajské informace hromadně, např. aby mohly identifikovat a vyhodnocovat nové nebo vznikající hrozby, zároveň ale těmto prvkům ukládá, aby upřednostňovaly alternativy, které umožní provádění cíleného signálového zpravodajství ⁽⁷¹⁾. Z toho plyne, že k hromadnému sběru dojde jen tehdy, pokud cílený sběr pomocí determinantů – tj. identifikátoru asociovaného s konkrétním cílem (např. e-mailová adresa nebo telefonní číslo cíle) – není možný „z technických či provozních důvodů“ ⁽⁷²⁾. To se týká jak způsobu sběru signálových zpravodajských informací, tak toho, jaké informace jsou shromažďovány ⁽⁷³⁾.
- (73) Podle prohlášení ODNI se zpravodajská komunita snaží „co nejvíce“ zúžit sběr i v případech, kdy nemůže použít specifické identifikátory pro cílený sběr. Dosahuje toho tím, že „používá filtry a jiné technické nástroje, aby sběr soustředila na ty prostředky, které budou pravděpodobně obsahovat komunikaci, která má hodnotu z hlediska zahraničních zpravodajských informací“ (a bude tedy responsivní k požadavkům stanoveným politiky USA v souladu s postupem popsaným v 70. bodě odůvodnění). U hromadného sběru tedy bude cílení prováděno alespoň dvěma způsoby. Za prvé, bude se vždy týkat pouze konkrétních zahraničně zpravodajských cílů (např. získávání signálového zpravodajství o činnostech teroristické skupiny operující v konkrétní oblasti) a zaměří sběr na komunikace, které s tím mají souvislost. Podle ujištění poskytnutých ODNI se toto odráží ve skutečnosti, že „činnosti Spojených států v oblasti signálového zpravodajství se dotýkají jen zlomku komunikace na internetu“ ⁽⁷³⁾. Za druhé, ODNI v prohlášeních vysvětluje, že filtry a jiné použité technické nástroje budou navrženy tak, aby sběr soustřeďovaly „co možná nej přesněji“ tak, aby bylo zajištěno, že objem „irelevantních informací“ bude minimalizován.
- (74) I v případech, kdy Spojené státy považují za nezbytné shromažďovat signálové zpravodajství hromadně za podmínek stanovených v 70.–73. bodě odůvodnění, omezuje směrnice PPD-28 využívání takových informací na šest konkrétních účelů, jejichž cílem je ochrana soukromí a občanských svobod všech osob bez ohledu na jejich státní příslušnost či bydliště ⁽⁷⁴⁾. Tyto přípustné účely zahrnují opatření na odhalování a potírání hrozeb pro ozbrojené síly nebo vojsko plynoucích ze špionáže, terorismu, zbraní hromadného ničení, hrozeb kybernetické

⁽⁶⁸⁾ Viz poznámka pod čarou 63.

⁽⁶⁹⁾ Je rovněž třeba poznamenat, že podle § 2.4 EO 12333 prvky zpravodajské komunity „použijí co nejméně obtěžující metody sběru, jaké jsou proveditelné uvnitř Spojených států“. Pokud jde o omezení nahrazení veškerého hromadného sběru cíleným sběrem, viz výsledky hodnocení National Research Council, jak o nich referovala Agentura Evropské unie pro základní práva v dokumentu Sledování zpravodajskými službami: záruky ochrany základních práv a prostředky nápravy v Evropské unii (2015), s. 18.

⁽⁷⁰⁾ Prohlášení ODNI (příloha VI), s. 4.

⁽⁷¹⁾ Viz také § 5(d) směrnice PPD-28, která řediteli národních zpravodajských služeb ukládá, aby v koordinaci s řediteli příslušných prvků zpravodajské komunity a Úřadem pro vědeckotechnickou politiku předložil prezidentovi „zprávu vyhodnocující proveditelnost vytvoření softwaru, který by zpravodajské komunitě umožnil snadněji provádět cílený, a nikoli hromadný, sběr informací“. Podle veřejně dostupných informací bylo výsledkem této zprávy to, že „neexistuje alternativa založená na softwaru, která bude představovat kompletní náhradu hromadného sběru z hlediska odhalování některých hrozeb národní bezpečnosti.“ Viz dokument Signals Intelligence Reform, 2015 Anniversary Report.

⁽⁷²⁾ Viz poznámka pod čarou 63.

⁽⁷³⁾ Prohlášení ODNI (příloha VI). Toto se konkrétně týká obavy vnitrostátních orgánů pro ochranu údajů, kterou vyjádřily ve svém stanovisku k návrhu rozhodnutí o odpovídající úrovni ochrany. Viz dokument pracovní skupiny pro ochranu údajů zřízené podle článku 29, stanovisko 01/2016 k návrhu rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (přijaty dne 13. dubna 2016), s. 38 s pozn. 47.

⁽⁷⁴⁾ Viz § 2 směrnice PPD-28.

bezpečnosti, jakož i přeshraničních hrozeb trestné činnosti týkajících se ostatních pěti účelů, a budou přezkoumávány alespoň jednou ročně. Podle prohlášení orgánů vlády USA posílily jednotlivé prvky zpravodajské komunity svoji analytickou praxi a normy pro dotazování nevyhodnocených signálových zpravodajských informací tak, aby bylo těmto požadavkům vyhověno; použití cílených dotazů „zajišťuje, že analytikům budou k přezkoumání předloženy jen ty informace, které jsou potenciálně zpravodajsky hodnotné“ ⁽⁷⁵⁾.

- (75) Tato omezení jsou obzvláště relevantní pro osobní údaje předávané v rámci štítu EU–USA na ochranu soukromí, zejména v případech, kdy má ke sběru osobních údajů dojít mimo Spojené státy, mimo jiné během jejich cesty transatlantickými kabely z Unie do Spojených států. Na takový sběr, jak potvrdily orgány USA v prohlášeních ODNI, se vztahují v nich stanovená omezení a ochranná opatření, včetně omezení a ochranných opatření podle směrnice PPD-28 ⁽⁷⁶⁾.
- (76) Tyto zásady vystihují podstatu zásady nezbytnosti a zásady proporcionality, ačkoli těmito právními termíny nejsou vyjádřeny. Jasně upřednostňován je cílený sběr, zatímco hromadný sběr je omezen na (výjimečné) situace, kdy cílený sběr není možný z technických nebo provozních důvodů. I v případech, kdy je *hromadný sběr* nevyhnutelný, je další „využívání“ těchto údajů formou přístupu k nim *striktně omezeno* na konkrétní, legitimní účely národní bezpečnosti ⁽⁷⁷⁾.
- (77) Tyto požadavky, které mají podobu směrnice vydané prezidentem jakožto vrchním představitelem výkonné moci, zavazují celou zpravodajskou komunitu a byly dále implementovány prostřednictvím provozních řádů jednotlivých zpravodajských agentur, které transponují obecné zásady do konkrétních pokynů pro každodenní operace. Přestože Kongres sám není směrnici PPD-28 vázán, i on přijal opatření k zajištění toho, aby sběr osobních údajů a přístup k nim ve Spojených státech byl cílený, a nikoli „všeobecný“.
- (78) Z dostupných informací, včetně prohlášení vlády USA, vyplývá, že jakmile jsou údaje předány organizacím umístěným ve Spojených státech a autocertifikovaným v rámci štítu EU–USA na ochranu soukromí, mohou zpravodajské agentury USA prohledávat osobní údaje pouze ⁽⁷⁸⁾ tehdy, pokud je jejich žádost v souladu se zákonem o zabezpečování informací o činnostech cizí moci (*Foreign Intelligence Surveillance Act*, FISA) nebo pokud žádost podal Federální vyšetřovací úřad (FBI) na základě tzv. *National Security Letter* (NSL) ⁽⁷⁹⁾. V zákoně FISA existuje několik právních základů pro sběr (a následné zpracování) osobních údajů subjektů údajů z EU

⁽⁷⁵⁾ Prohlášení ODNI (příloha VI), s. 4. Viz také směrnice Intelligence Community Directive 203.

⁽⁷⁶⁾ Prohlášení ODNI (příloha VI), s. 2. Podobně platí omezení stanovená v EO 12333 (např. to, že shromažďované informace musí odpovídat prioritám stanoveným prezidentem).

⁽⁷⁷⁾ Viz *Schrems*, bod 93.

⁽⁷⁸⁾ Sběr údajů ze strany FBI může být podložen také zákonnými pravomocemi při prosazování práva (viz oddíl 3.2 tohoto rozhodnutí).

⁽⁷⁹⁾ Bližší informace o použití NSL viz prohlášení ODNI (příloha VI) s. 13–14 spolu s pozn. 38. Jak je v nich uvedeno, FBI může NSL využít jen k vyžádání neobsahových informací relevantních pro povolené vyšetřování v oblasti národní bezpečnosti, jehož cílem je ochrana před mezinárodním terorismem nebo tajnými výzvědnými aktivitami. Pokud jde o předávání údajů v rámci štítu EU–USA na ochranu soukromí, nejrelevantnější zákonnou pravomocí se zdá být zákon o ochraně soukromí elektronických komunikací (*Electronic Communications Privacy Act*, 18 U.S.C. § 2709), podle něhož musí jakákoli žádost o informace o účastníkovi nebo o transakční záznam obsahovat „termín, který konkrétně identifikuje osobu, subjekt, telefonní číslo nebo účet“.

předávaných v rámci štítu EU–USA na ochranu soukromí. Kromě § 104 zákona FISA ⁽⁸⁰⁾, kterým se řídí tradiční elektronické sledování fyzických osob, a § 402 zákona FISA ⁽⁸¹⁾ o instalaci zařízení k záznamu příchozích a odchozích telefonních čísel jsou dvěma ústředními nástroji § 501 zákona FISA (bývalý § 215 zákona U.S. PATRIOT ACT) a § 702 FISA ⁽⁸²⁾.

- (79) V tomto ohledu zákon USA FREEDOM Act, který byl přijat 2. června 2015, zakazuje hromadný sběr záznamů na základě § 402 zákona FISA (instalace zařízení k záznamu příchozích a odchozích telefonních čísel), § 501 zákona FISA (bývalý § 215 zákona U.S. PATRIOT ACT) ⁽⁸³⁾ a prostřednictvím NSL, a požaduje místo toho použití konkrétních „selekčních termínů“ ⁽⁸⁴⁾.

- (80) Ačkoli zákon FISA obsahuje další zákonná zmocnění k provádění národní zpravodajské činnosti, včetně signálového zpravodajství, z hodnocení Komise vyplynulo, že pokud jde o osobní údaje, které mají být předávány v rámci štítu EU–USA na ochranu soukromí, omezují tato zákonná zmocnění rovněž veřejný zásah do cíleného sběru údajů a přístupu k nim.

- (81) To je jasné u tradičního elektronického sledování fyzických osob podle § 104 zákona FISA ⁽⁸⁵⁾. Pokud jde o § 702 zákona FISA, který představuje základ pro dva významné zpravodajské programy zpravodajských agentur USA (PRISM, UPSTREAM), vyhledávání je prováděno cíleně použitím individuálních selektorů, které identifikují konkrétní komunikační prostředky, jako např. e-mailovou adresu nebo telefonní číslo cíle, avšak nikoli pomocí klíčových slov či dokonce jmen cílených fyzických osob ⁽⁸⁶⁾. Tudíž, jak poznamenal Výbor pro dohled nad

⁽⁸⁰⁾ 50 U.S.C. § 1804. Tato zákonná pravomoc vyžaduje „popis skutečností a okolností, o něž se žádající strana opírala při odůvodnění své domněnky, že (A) cíl elektronického sledování je cizí moc nebo agent cizí moci“, přičemž takovým cílem mohou být osob, 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)). Souvislost s osobními údaji předávanými v rámci štítu EU–USA je však jen teoretická, neboť tento popis skutečností musí rovněž odůvodnit domněnku, že „každý z prostředků nebo míst, která jsou elektronicky sledována, je používán, nebo bude v dohledné době použit cizí mocí nebo agentem cizí moci“. Použití této pravomoci však v každém případě vyžaduje podání žádosti u Soudu pro uplatňování zákona FISA, který mimo jiné posoudí, zda na základě předložených skutečností existuje důvodné podezření, že tomu tak opravdu je.

⁽⁸¹⁾ 50 U.S.C. § 1842 ve spojení s § 1841(2) a 18 U.S.C. § 3127. Tato pravomoc se netýká obsahu komunikací, nýbrž je zaměřena na informace o zákazníkovi či účastníkovi, který používá službu (např. jméno, adresa, účastnické číslo, délka/druh poskytované služby, zdroj/způsob úhrady). Vyžaduje, aby u Soudu pro uplatňování zákona FISA (nebo u magistrátního soudce) byla podána žádost o příkaz a aby byl použit specifický selekční termín ve smyslu § 1841(4), tzn. termín, který konkrétně identifikuje osobu, účet atd. a který má v co největší přijatelné míře omezit záběr vyhledávaných informací.

⁽⁸²⁾ Zatímco § 501 zákona FISA (bývalý § 215 zákona U.S. PATRIOT ACT) opravňuje FBI požádat o soudní příkaz k vydání „hmatatelných věcí“ (zejména telefonních metadat, ale také obchodních záznamů) pro účely zahraničního zpravodajství, § 702 zákona FISA umožňuje prvkům zpravodajské komunity USA žádat o přístup k informacím, včetně obsahu internetové komunikace, z území Spojených států, jejichž cílem jsou však určité osoby, které nejsou osobami USA a které jsou mimo USA.

⁽⁸³⁾ Na základě tohoto ustanovení může FBI zažádat o „hmatatelné věci“ (např. záznamy, listiny, dokumenty), prokáže-li Soudu pro uplatňování zákona FISA, že má důvodné podezření, že jsou tyto věci relevantní pro konkrétní vyšetřování FBI. Při vyhledávání musí FBI používat selekční termíny schválené Soudem pro uplatňování zákona FISA, u kterých existuje „důvodné a pojmenovatelné podezření“, že mají souvislost s jednou nebo několika cizími mocemi nebo jejich agenty zapojenými do mezinárodního terorismu nebo jeho přípravy. Viz dokument PCLOB – Sec. 215 Report, s. 59; dokument NSA CLPO – Transparency Report: The USA Freedom Act Business Records FISA Implementation ze dne 15. ledna 2016, s. 4–6.

⁽⁸⁴⁾ Prohlášení ODNI (příloha VI), s. 13 (pozn. 38).

⁽⁸⁵⁾ Viz poznámka pod čarou 81.

⁽⁸⁶⁾ Dokument PCLOB – Sec. 702 Report, s. 32–33 s dalšími odkazy. Podle kanceláře NSA pro ochranu soukromí musí NSA 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 NSA a celý postup musí být zaznamenán pro účely následných kontrol dodržování předpisů, které provádí ODNI a Ministerstvo spravedlnosti. Viz dokument NSA CLPO – NSA's Implementation of Foreign Intelligence Act Section 702 ze dne 16. dubna 2014.

ochranou soukromí a občanských svobod (PCLOB), sledování podle § 702 „spočívá zcela ve sledování konkrétních osob, [které nejsou občany USA a] o kterých bylo učiněno individualizované zjištění“⁽⁸⁷⁾. Podle ustanovení o skončení platnosti bude § 702 zákona FISA přezkoumán v roce 2017, kdy také bude Komise muset přehodnotit ochranná opatření, které mají subjekty údajů v EU k dispozici.

- (82) Kromě toho vláda USA ve svých prohlášeních Evropskou komisi výslovně ujistila, že zpravodajská komunita USA „neprovádí nahodilé sledování kohokoli, ani běžných evropských občanů“⁽⁸⁸⁾. Pokud jde o osobní údaje shromažďované na území Spojených států, je toto prohlášení podloženo empirickými důkazy, které dokládají, že *žádosti o přístup* podávané prostřednictvím NSL a podle zákona FISA se jak jednotlivě, tak jako celek týkají pouze relativně malého počtu cílů vzhledem k celkovému toku dat na internetu⁽⁸⁹⁾.
- (83) Pokud jde o *přístup* k shromážděným údajům a *bezpečnost údajů*, směrnice PPD-28 požaduje, aby přístup byl „omezen na pracovníky s oprávněním, kteří mají potřebu informace znát, aby mohli plnit svoje úkoly“, a aby osobní informace byly „zpracovávány a uchovávány za podmínek, které v souladu s platnými opatřeními na ochranu citlivých informací zajišťují odpovídající ochranu a zabraňují osobám bez oprávnění v přístupu k nim“. Zpravodajští pracovníci jsou patřičně a příslušně obeznámeni se zásadami uvedenými ve směrnici PPD-28⁽⁹⁰⁾.
- (84) Pokud jde o *uchovávání* a další šíření osobních údajů subjektů údajů z EU shromažďovaných orgány zpravodajství USA, stanoví směrnice PPD-28, že se všemi osobami (včetně osob, které nejsou osobami USA) by mělo být zacházeno důstojně a s úctou, že všechny osoby mají z hlediska ochrany soukromí legitimní zájem o to, jak je s jejich osobními informacemi nakládáno, a že prvky zpravodajské komunity tedy musí vypracovat politiky, které poskytnou vhodná opatření na ochranu těchto údajů a budou „navrženy tak, aby bylo minimalizováno šíření a uchovávání [těchto údajů]“⁽⁹¹⁾.

⁽⁸⁷⁾ Viz dokument PCLOB – Sec. 702 Report, s. 111. Viz také prohlášení ODNI (příloha VI), s. 9. („Sběr údajů podle § 702 [zákonu FISA] není „masový a nahodilý“, nýbrž úzce zaměřený na sběr zahraničního zpravodajství od jednotlivě identifikovaných legitimních cílů“) a s. 13, pozn. 36 (s odkazem na stanovisko Soudu pro uplatňování zákona FISA z roku 2014); dokument NSA CLPO – NSA's Implementation of Foreign Intelligence Act Section 702 ze dne 16. dubna 2014. I v případě programu UPSTREAM smí NSA pouze požádat o odposlech elektronických komunikací směrem od zadaných selektorů, směrem k nim nebo o nich.

⁽⁸⁸⁾ Prohlášení ODNI (příloha VI), s. 18. Viz také s. 6, kde stojí, že použitelné postupy „prokazují odhodlání předcházet svévolnému a nahodilému shromažďování informací prostřednictvím signálového zpravodajství a naplňovat – od nejvyšších úrovní naší vlády – zásadu přiměřenosti“.

⁽⁸⁹⁾ Viz dokument Statistical Transparency Report Regarding Use of National Security Authorities ze dne 22. dubna 2015. Celkový tok dat na internetu viz např. dokument Agentury EU pro základní práva – Sledování zpravodajskými službami: záruky ochrany základních práv a prostředky nápravy v Evropské unii (2015), s. 15–16. Pokud jde o program UPSTREAM, dle odtajněného stanoviska Soudu pro uplatňování zákona FISA z roku 2011 pocházelo více než 90 % elektronické komunikace získané podle § 702 zákona FISA z programu PRISM, zatímco program UPSTREAM poskytl méně než 10 % údajů. Viz dokument FISC – Memorandum Opinion, 2011 WL 10945618 (FISA Ct., ze dne 3. října 2011), pozn. 21 (k dispozici zde: <http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>).

⁽⁹⁰⁾ Viz § 4(a)(ii) směrnice PPD-28. Dále viz dokument ODNI – Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, červenec 2014, s. 5, podle kterého by „politiky jednotlivých prvků zpravodajské komunity měly posilovat existující analytickou praxi a normy tak, aby analytici museli své dotazy a jiné vyhledávací termíny či metody strukturovat tak, aby vyhledávaly zpravodajské informace, které jsou relevantní pro platný zpravodajský nebo donucovací úkol; zužovat dotazy na osoby na kategorie zpravodajských informací, které reagují na zpravodajský nebo donucovací požadavek; a minimalizovat vyhodnocování osobních informací, které nesouvisí se zpravodajským nebo donucovacím požadavkem“. Viz např. dokument CIA – Signals Intelligence Activities, s. 5; dokument FBI – Presidential Policy Directive 28 Policies and Procedures, s. 3. Podle průběžné zprávy z roku 2016 o reformě signálového zpravodajství (2016 Progress Report on the Signals Intelligence Reform) přijaly prvky zpravodajské komunity (včetně FBI, CIA a NSA) kroky k tomu, aby se jejich pracovníci začali řídit požadavky směrnice PPD-28, např. vypracováním nových nebo úpravou stávajících politik školení a odborné přípravy.

⁽⁹¹⁾ Podle prohlášení ODNI se tato omezení uplatňují neohledně na to, zda byly informace shromážděny hromadně nebo cíleně, a na státní příslušnost fyzické osoby.

- (85) Vláda USA vysvětlila, že tento požadavek na přiměřenost znamená, že prvky zpravodajské komunity nebudou muset přijímat „jakékoli teoreticky možné opatření“, nýbrž budou muset „vyvažovat snahu vyhovět legitimním zájmům o ochranu soukromí a občanských svobod s praktickými potřebami činností signálového zpravodajství“⁽⁹²⁾. V tomto ohledu bude s osobami, které nejsou osobami USA, zacházeno stejně jako s osobami USA na základě postupů schválených ministrem spravedlnosti USA⁽⁹³⁾.
- (86) Podle těchto pravidel je uchovávání obecně omezeno na nejvýše pět let, nestanoví-li výslovně jinak právní předpisy nebo ředitel národních zpravodajských služeb po pečlivém vyhodnocení obav v oblasti ochrany soukromí – a s přihlédnutím ke stanoviskům vedoucího odboru ODNI pro otázky ochrany občanských svobod a úředníků ODNI pro otázky ochrany soukromí a občanských svobod – v tom smyslu, že pokračující uchování údajů je v zájmu národní bezpečnosti⁽⁹⁴⁾. Šíření je omezeno na případy, kdy jsou informace relevantní pro původní a základní účel sběru, a reagují tudíž na oprávněný zahraničně zpravodajský nebo donucovací požadavek⁽⁹⁵⁾.
- (87) Podle ujištění vlády USA nesmí být osobní informace šířeny pouze proto, že dotčená osoba není osobou USA, a „signálové zpravodajské informace o rutinních činnostech cizí osoby by nebyly považovány za zahraniční zpravodajské informace, které by bylo možno šířit nebo trvale uchovávat pouze na základě této skutečnosti, ledaže by reagovaly na oprávněný zahraničně zpravodajský požadavek“⁽⁹⁶⁾.
- (88) Na základě výše uvedeného Komise konstatuje, že ve Spojených státech jsou zavedena pravidla, jejichž smyslem je omezovat jakékoli zásahy pro účely národní bezpečnosti do základních práv osob, jejichž osobní údaje jsou předávány z Unie do USA v rámci štítu EU–USA na ochranu soukromí, na rozsah striktně nezbytný k tomu, aby bylo dosaženo příslušného legitimního cíle.
- (89) Jak vyplývá z výše uvedené analýzy, právo USA zajišťuje, že opatření ke sledování budou využita jen k získání zahraničních zpravodajských informací – což je legitimní politický cíl⁽⁹⁷⁾ – a budou co nejvíce přizpůsobené.

⁽⁹²⁾ Viz prohlášení ODNI (příloha VI).

⁽⁹³⁾ Viz § 4(a)(i) směrnice PPD-28 spolu s § 2.3 dekrety EO 12333.

⁽⁹⁴⁾ § 4(a)(i) směrnice PPD-28; prohlášení ODNI (příloha VI), s. 7. Například u osobních informací shromažďovaných podle § 702 zákona FISA uplatňují minimalizační postupy NSA schválené Soudem pro uplatňování zákona FISA pravidlo, že metadata a nevyhodnocený obsah získaný z programu PRISM se uchovává po dobu maximálně pěti let a u programu UPSTREAM po dobu maximálně dvou let. NSA tato omezení na délku uchovávání údajů plní prostřednictvím automatizovaného procesu, kterým jsou na konci příslušné doby uchovávání shromážděné údaje smazány. Viz dokument NSA – Sec. 702 FISA Minimization Procedures, Sec. 7 s Sec. 6(a)(1); dokument NSA CLPO – NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 ze dne 16. dubna 2014. Podobně pak uchovávání údajů podle § 501 zákona FISA (bývalý § 215 zákona U.S. PATRIOT ACT) je omezeno na pět let, ledaže jsou předmětné osobní údaje součástí řádně schváleného šíření zahraničních zpravodajských informací, nebo ledaže Ministerstvo spravedlnosti písemně sdělí NSA, že předmětné záznamy podléhají povinnosti uchování v rámci probíhajícího nebo nadcházejícího soudního řízení. Viz dokument NSA CLPO – Transparency Report: The USA Freedom Act Business Records FISA Implementation ze dne 15. ledna 2016.

⁽⁹⁵⁾ Konkrétně v případě § 501 zákona FISA (bývalý § 215 zákona U.S. PATRIOT ACT) může k šíření osobních informací dojít jen pro účely boje proti terorismu nebo dokazování trestného činu; v případě § 702 zákona FISA pak jen tehdy, existuje-li platný zahraničně zpravodajský nebo donucovací účel. Srov. dokumenty NSA CLPO – NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 ze dne 16. dubna 2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation ze dne 15. ledna 2016. Viz také dokument NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 ze dne 7. října 2014.

⁽⁹⁶⁾ Prohlášení ODNI (příloha VI), s. 7 (s odkazem na směrnici Intelligence Community Directive (ICD) 203).

⁽⁹⁷⁾ Soudní dvůr objasnil, že národní bezpečnost je legitimním politickým cílem. Viz *Schrems*, bod 88. Viz také věc *Digital Rights Ireland a další*, body 42–44 a 51, ve kterých Soudní dvůr konstatoval, že boj proti závažné trestné činnosti, zejména organizované trestné činnosti a terorismu, může do velké míry záviset na použití moderních vyšetřovacích metod. Navíc na rozdíl od vyšetřování trestné činnosti, které se obvykle týká zpětného stanovení odpovědnosti a viny za dřívější chování, zpravodajská činnost se často zaměřuje na předcházení hrozbám národní bezpečnosti ještě předtím, než dojde ke škodě. Taková vyšetřování se proto často musí zaměřovat na větší rozsah možných aktérů („cílů“) a širší zeměpisnou oblast. Srov. Evropský soud pro lidská práva, věc *Weber and Saravia v. Germany*, rozhodnutí ze dne 29. června 2006, stížnost č. 54934/00, body 105–118 (o tzv. „strategickém monitorování“).

Konkrétně hromadný sběr bude povolen pouze výjimečně v případech, kdy cílený sběr není možný, a bude doprovázen dodatečnými ochrannými opatřeními za účelem minimalizace množství sbíraných údajů a následného přístupu k nim (který bude muset být cílený a povolen pouze pro konkrétní účely).

- (90) Podle posouzení Komise je toto v souladu s normou stanovenou Soudním dvorem v rozsudku *Schrems*, podle něž právní úprava zasahující do základních práv zaručených články 7 a 8 Listiny musí stanovit „minimální požadavky“⁽⁹⁸⁾ a „na naprosto nezbytné se tedy neomezuje taková právní úprava, která globálně dovoluje uchovávání všech osobních údajů všech osob, jejichž osobní údaje byly předány z Unie do Spojených států bez jakéhokoli rozlišení, omezení nebo výjimky činěných v závislosti na sledovaném cíli a bez stanovení objektivního kritéria umožňujícího vymezit přístup veřejných orgánů k údajům a jejich následné využití pro konkrétní účely, striktně omezené a způsobilé odůvodnit zásah způsobený jak přístupem k těmto údajům, tak jejich využíváním“⁽⁹⁹⁾. Nebude docházet ani k neomezenému sběru a uchovávání údajů všech osob bez jakýchkoli omezení, ani k neomezenému přístupu. Prohlášení poskytnutá Komisi, včetně ujištění, že signálové zpravodajské činnosti USA se dotýkají pouze zlomku komunikace na internetu, navíc vylučují, že by existoval „globální“⁽¹⁰⁰⁾ přístup k obsahu elektronických komunikací.

3.1.2 Účinná právní ochrana

- (91) Komise posoudila jak mechanismy dohledu, které existují ve Spojených státech v souvislosti s jakýmkoli zásahem zpravodajských orgánů USA do osobních dat předávaných do Spojených států, tak možnosti individuální nápravy, jaké mají subjekty údajů z EU k dispozici.

Dohled

- (92) Zpravodajská komunita USA podléhá řadě přezkumných a dohledových mechanismů, které spadají do působnosti tří složek státní moci. Mezi tyto mechanismy patří interní a externí subjekty v rámci výkonné moci, několik výborů Kongresu a soudní dohled – posledně jmenovaný pak konkrétně v souvislosti s činnostmi podle zákona FISA.
- (93) Zpravodajská činnost orgánů USA je v první řadě předmětem rozsáhlého dohledu ze strany výkonné moci.
- (94) Podle § 4(a)(iv) směrnice PPD-28 politiky a postupy prvků zpravodajské komunity „obsahují odpovídající opatření k usnadnění dohledu nad prováděním opatření na ochranu osobních informací“; k takovým opatřením by měl patřit pravidelný audit⁽¹⁰¹⁾.

⁽⁹⁸⁾ *Schrems*, bod 91 s dalšími odkazy.

⁽⁹⁹⁾ *Schrems*, bod 93.

⁽¹⁰⁰⁾ Srov. *Schrems*, bod 94.

⁽¹⁰¹⁾ Dokument ODNI – Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, s. 7. Viz např. dokument CIA – Signals Intelligence Activities, s. 6 (Compliance); dokument FBI – Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4); dokument NSA – PPD-28 Section 4 Procedures ze dne 12. ledna 2015, Sec. 8.1, 8.6(c).

- (95) V tomto ohledu bylo zavedeno několik vrstev dohledu, mimo jiné úředníci pro otázky ochrany občanských svobod nebo soukromí, generální inspektoři, odbor ODNI pro otázky ochrany občanských svobod a soukromí, Výbor pro dohled nad ochranou soukromí a občanských svobod (PCLOB), a Výbor prezidenta pro dohled nad zpravodajstvím. Ve všech zpravodajských agenturách jsou tyto dohledové funkce dále doplněny činností pracovníků pověřených kontrolou dodržování předpisů (compliance) ⁽¹⁰²⁾.
- (96) Jak vysvětluje vláda USA ⁽¹⁰³⁾, na řadě ministerstev, která mají v náplni práce zpravodajskou činnost, a ve zpravodajských agenturách ⁽¹⁰⁴⁾ existují *úředníci pro otázky ochrany občanských svobod nebo soukromí*, k jejichž pracovním povinnostem patří dohled. 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 adekvátně k ochraně občanských svobod a soukromí, že zavedlo adekvátní postupy pro řešení stížností fyzických osob, které mají za to, že jejich soukromí nebo občanské svobody byly porušeny (a v některých případech, např. na ODNI, mohou mít sami pravomoc šetřit stížnosti ⁽¹⁰⁵⁾). Vedoucí ministerstva/agentury pak musí zajistit, aby tento úředník obdržel veškeré informace a aby dostal přístup k veškerým materiálům, které k výkonu své funkce potřebuje. Úředníci pro otázky ochrany občanských svobod a soukromí předkládají Kongresu a Výboru pro dohled nad ochranou soukromí a občanských svobod pravidelné zprávy, mimo jiné o počtu a povaze stížností obdržaných ministerstvem/agenturou, a shrnutí o povaze stížností, provedených kontrolách a šetřeních a dopadu kroků podniknutých úředníkem ⁽¹⁰⁶⁾. Podle posouzení vnitrostátních orgánů pro ochranu údajů lze vnitřní dohled prováděný úředníky pro otázky ochrany občanských svobod nebo soukromí považovat za „poměrně robustní“, přestože dle jejich mínění nesplňuje požadovanou úroveň nezávislosti ⁽¹⁰⁷⁾.
- (97) Každý prvek zpravodajské komunity má dále vlastního *generálního inspektora*, do jehož popisu práce patří mimo jiné dohled nad zahraniční zpravodajskou činností ⁽¹⁰⁸⁾. Sem patří odbor generálního inspektora v rámci 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 ODNI a/nebo programy či činnostmi zpravodajské komunity ⁽¹⁰⁹⁾. Generální inspektoři jsou ze zákona nezávislá ⁽¹¹⁰⁾ oddělení odpovědná za provádění auditů a vyšetřování týkajících se programů a operací prováděných příslušnou agenturou pro účely národního zpravodajství, a mimo jiné za zneužití nebo porušení zákona ⁽¹¹¹⁾. Jsou oprávněni mít přístup ke všem záznamům, zprávám, auditům, přezkumům, dokumentům, listinám, doporučením a dalším
-
- ⁽¹⁰²⁾ Například NSA zaměstnává na ředitelství pro compliance více než 300 pracovníků compliance. Viz prohlášení ODNI (příloha VI), s. 7.
- ⁽¹⁰³⁾ Viz mechanismus ombudsmana (příloha III), bod 6 písm. b) bod i) až iii).
- ⁽¹⁰⁴⁾ Viz 42 U.S.C. § 2000ee-1. Patří k nim např. Ministerstvo zahraničních věcí, Ministerstvo spravedlnosti (včetně FBI), Ministerstvo vnitřní bezpečnosti, Ministerstvo obrany, NSA, CIA a ODNI.
- ⁽¹⁰⁵⁾ Podle vlády USA pokud odbor ODNI pro otázky ochrany občanských svobod a soukromí obdrží stížnost, koordinuje s ostatními prvky zpravodajské komunity způsob dalšího zpracování této stížnosti uvnitř zpravodajské komunity. Viz mechanismus ombudsmana (příloha III), bod 6 písm. b) bod ii).
- ⁽¹⁰⁶⁾ Viz 42 U.S.C. § 2000ee-1 (f)(1),(2).
- ⁽¹⁰⁷⁾ Viz dokument pracovní skupiny pro ochranu údajů zřízené podle článku 29, stanovisko 01/2016 k návrhu rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (přijato dne 13. dubna 2016), s. 41.
- ⁽¹⁰⁸⁾ Prohlášení ODNI (příloha VI), s. 7. Viz např. dokument NSA – PPD-28 Section 4 Procedures ze dne 12. ledna 2015, Sec. 8.1; dokument CIA – Signals Intelligence Activities, s. 7 (Responsibilities).
- ⁽¹⁰⁹⁾ Tento generální inspektor (jehož post byl zřízen v říjnu 2010) je jmenován prezidentem USA po potvrzení Senátu a odvolat jej může jen prezident, nikoli ředitel národních zpravodajských služeb.
- ⁽¹¹⁰⁾ Tito generální inspektoři jsou jmenováni nastalo a smí je odvolat pouze prezident, který při tom musí Kongresu 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 poňnat příslušného ministra/ředitele k odpovědnosti. Viz např. zákon o generálních inspektorech, *Inspector General Act of 1978*, § 8 (o generálním inspektorovi Ministerstva obrany); § 8E (o generálním inspektorovi Ministerstva spravedlnosti), § 8G (d)(2)(A),(B) (o generálním inspektorovi NSA); 50. U.S.C. § 403q (b) (o generálním inspektorovi CIA); zákon o povolení zpravodajské činnosti pro fiskální rok 2010 (*Intelligence Authorization Act For Fiscal Year 2010*), § 405(f) (o generálním inspektorovi zpravodajské komunity). Podle posouzení vnitrostátních orgánů pro ochranu údajů generální inspektoři „pravděpodobně vyhovují kritériu organizační nezávislosti, jak je definoval Soudní dvůr Evropské unie a Evropský soud pro lidská práva, alespoň od okamžiku, kdy se nový proces jmenování vztahuje na všechny“. Viz dokument pracovní skupiny pro ochranu údajů zřízené podle článku 29, stanovisko 01/2016 k návrhu rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (přijato dne 13. dubna 2016), s. 40.
- ⁽¹¹¹⁾ Viz prohlášení ODNI (příloha VI), s. 7. Viz také *Inspector General Act of 1978*, as amended Pub. L. 113-126 ze dne 7. července 2014.

relevantním materiálům, v případě potřeby i prostřednictvím předvolání, a mohou vyslyšet⁽¹¹²⁾. Generální inspektoři sice mohou vydávat jen nezávazná doporučení k nápravě, avšak jejich zprávy, včetně zpráv o následných krocích (nebo jejich absenci) se zveřejňují a navíc předkládají Kongresu, který na tomto základě může vykonat svou funkci dohledu⁽¹¹³⁾.

- (98) Dále je zde Výbor pro dohled nad ochranou soukromí a občanských svobod (*Privacy and Civil Liberties Oversight Board*, PCLOB), nezávislá agentura⁽¹¹⁴⁾ v rámci výkonné moci zahrnující výbor složený z pěti zástupců obou politických stran⁽¹¹⁵⁾ jmenovaných prezidentem se souhlasem Senátu na pevné období šesti let, které je svěřena ochrana soukromí a občanských svobod v oblasti politiky boje proti terorismu a jejich provádění. V rámci přezkumu činnosti zpravodajské komunity smí tento výbor přistupovat ke všem relevantním záznamům, zprávám, auditům, přezkumům, dokumentům, listinám, doporučením a dalším relevantním materiálům jednotlivých agentur, včetně utajovaných informací, a provádět pohovory a vyslyšet svědky. Výboru jsou předkládány zprávy úředníků pro otázky ochrany občanských svobod a soukromí několika federálních ministerstev či agentur⁽¹¹⁶⁾, jimž může vydávat doporučení, a naopak on předkládá pravidelné zprávy výborům Kongresu a prezidentovi⁽¹¹⁷⁾. Jedním z úkolů výboru je v mezích jeho mandátu připravit hodnotící zprávu o provádění směrnice PPD-28.
- (99) Výše uvedené mechanismy dohledu doplňuje nakonec Výbor pro dohled nad zpravodajstvím zřízený v rámci Poradního výboru prezidenta pro zpravodajství, který dohlíží na to, jak a zda zpravodajské orgány USA dodržují Ústavu USA a veškeré platné předpisy.
- (100) Za účelem usnadnění dohledu mají prvky zpravodajské komunity budovat informační systémy umožňující monitoring, zaznamenávání a kontrolu dotazů a jiných vyhledávání osobních informací⁽¹¹⁸⁾. Subjekty pro dohled a dodržování předpisů budou pravidelně kontrolovat praxi prvků zpravodajské komunity z hlediska ochrany osobních informací obsažených v signálovém zpravodajství a to, zda tyto postupy dodržují⁽¹¹⁹⁾.
- (101) Na tyto funkce dohledu pak navazují rozsáhlé požadavky na hlášení případů nedodržování předpisů. Postupy jednotlivých agentur musí konkrétně zajišťovat, aby každé závažné porušení předpisů, které se týká osobních informací jakékoli osoby bez ohledu na její státní příslušnost shromážděných signálovým zpravodajstvím, bylo bezodkladně hlášeno řediteli tohoto prvku zpravodajské komunity, který je dále nahlásí řediteli národních zpravodajských služeb, který pak podle směrnice PPD-28 posoudí, zda je nutná náprava⁽¹²⁰⁾. Podle EO 12333 jsou navíc všechny prvky zpravodajské komunity povinny hlásit případy nedodržení předpisů Výboru pro dohled nad zpravodajstvím⁽¹²¹⁾. Tyto mechanismy zaručují, že věc bude řešena na nejvyšší úrovni zpravodajské komunity.

⁽¹¹²⁾ Viz *Inspector General Act of 1978*, § 6.

⁽¹¹³⁾ Viz prohlášení ODNI (příloha VI), s. 7. Viz také *Inspector General Act of 1978*, § 4(5), 5. Podle § 405(b)(3), (4) zákona *Intelligence Authorization Act For Fiscal Year 2010*, Pub. L. 111-259, ze dne 7. října 2010, informuje generální inspektor zpravodajské komunity jak ředitele národních zpravodajských služeb, tak Kongres o nutnosti nápravných opatření a o jejich pokroku.

⁽¹¹⁴⁾ Podle posouzení vnitrostátních orgánů pro ochranu údajů PCLOB v minulosti „demonstroval své nezávislé pravomoci“. Viz dokument pracovní skupiny pro ochranu údajů zřízené podle článku 29, stanovisko 01/2016 k návrhu rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (přijato dne 13. dubna 2016), s. 42.

⁽¹¹⁵⁾ Kromě nich PCLOB zaměstnává asi 20 řadových pracovníků. Viz <https://www.pclob.gov/about-us/staff.html>.

⁽¹¹⁶⁾ 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 označil za příslušné ke kontrole.

⁽¹¹⁷⁾ Viz 42 U.S.C. § 2000ee. Viz také mechanismus ombudsmana (příloha III), bod 6 písm. b) bod iv). PCLOB je mimo jiné povinen hlásit, pokud se některá agentura výkonné moci odmítne řídit jejím doporučením.

⁽¹¹⁸⁾ Dokument ODNI – *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, s. 7–8.

⁽¹¹⁹⁾ Tamtéž, s. 8. Viz také prohlášení ODNI (příloha VI), s. 9.

⁽¹²⁰⁾ Dokument ODNI – *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, s. 7. Viz např. dokument NSA – PPD-28 Section 4 Procedures ze dne 12. ledna 2015, Sec. 7.3, 8.7(c),(d); dokument FBI – Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4); dokument CIA – Signals Intelligence Activities, s. 6 (Compliance) a s. 8 (Responsibilities).

⁽¹²¹⁾ Viz EO 12333, Sec. 1.6(c).

V případech, ve kterých jde o osobu, která není osobou USA, rozhodne ředitel národních zpravodajských služeb v konzultaci s ministrem zahraničních věcí a ředitelem ministerstva nebo agentury, která případ nahlásila, zda je třeba přijmout kroky k informování příslušné cizí vlády v souladu s pravidly ochrany zdrojů a metod a pracovníků vlády USA ⁽¹²²⁾.

- (102) Za druhé, kromě těchto mechanismů dohledu v rámci výkonné moci má odpovědnost za dohled nad veškerou zahraniční zpravodajskou činností USA, včetně signálového zpravodajství USA, Kongres USA, konkrétně *výbory Sněmovny reprezentantů a Senátu pro zpravodajství a pro justici*. Podle zákona o národní bezpečnosti (*National Security Act*) „prezident 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“ ⁽¹²³⁾. Dále „prezident zajistí, aby byly výbory Kongresu pro zpravodajství bezodkladně informovány o veškeré nelegální činnosti i o nápravných krocích, jež byly nebo mají být přijaty v souvislosti s takovou nelegální činností“ ⁽¹²⁴⁾. Členové těchto výborů mají přístup k utajovaným informacím i ke zpravodajským metodám a programům ⁽¹²⁵⁾.
- (103) Pozdější předpisy dále rozšířily a zpřesnily požadavky na hlášení, pokud jde jak o prvky zpravodajské komunity a příslušné generální inspektory, tak o ministra spravedlnosti. Podle zákona FISA je například ministr spravedlnosti povinen „plně informovat“ výbory Senátu a Sněmovny reprezentantů pro zpravodajství a pro justici o činnostech vlády podle určitých paragrafů tohoto zákona ⁽¹²⁶⁾. 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. Konkrétně pokud jde o sledování podle § 702 zákona FISA, probíhá 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, především zprávami Ministerstva spravedlnosti a Úřadu ředitele národních zpravodajských služeb o dodržování předpisů a popisem všech případů nedodržení ⁽¹²⁷⁾, a samostatné pololetní hodnocení ministra spravedlnosti a ředitele národních zpravodajských služeb o dodržování postupů cíleného sběru a minimalizace, včetně dodržování postupů k zajištění toho, že údaje jsou shromažďovány pro platný účel zahraničního zpravodajství ⁽¹²⁸⁾. Kongresu adresují zprávy také generální inspektoři, kteří jsou oprávněni hodnotit, jak agentury dodržují postupy cíleného sběru a minimalizace a pokyny ministra spravedlnosti.
- (104) Podle zákona *USA FREEDOM Act* z roku 2015 musí vláda USA každý rok Kongresu (a veřejnosti) oznamovat počet příkazů a pokynů vyžádaných a obdržených podle zákona o zpravodajském sledování cizích cílů a mimo jiné odhad počtu osob USA a osob, které nejsou osobami USA, které se staly cílem sledování ⁽¹²⁹⁾. Zákon dále

⁽¹²²⁾ PPD-28, § 4(a)(iv).

⁽¹²³⁾ Viz § 501(a)(1) (50 U.S.C. § 413(a)(1)). Toto ustanovení obsahuje obecné požadavky, pokud jde o dohled Kongresu v oblasti národní bezpečnosti.

⁽¹²⁴⁾ Viz § 501(b) (50 U.S.C. § 413(b)).

⁽¹²⁵⁾ Srov. § 501(d) (50 U.S.C. § 413(d)).

⁽¹²⁶⁾ Viz 50 U.S.C. § 1808, 1846, 1862, 1871, 1881f.

⁽¹²⁷⁾ Viz 50 U.S.C. § 1881f.

⁽¹²⁸⁾ Viz 50 U.S.C. § 1881a(l)(1).

⁽¹²⁹⁾ Viz *USA FREEDOM Act of 2015*, Pub. L. No. 114-23, § 602(a). 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 obsahuje 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“.

stanoví povinnost zveřejňovat počty vydaných NSL, a to opět jak u osob USA, tak u osob, které nejsou osobami USA (příčemž adresátům příkazů a osvědčení podle zákona FISA i žádosti na základě NSL dovoluje za určitých podmínek vydávat zprávy o transparentnosti) ⁽¹³⁰⁾.

- (105) Za třetí, zpravodajská činnost orgánů veřejné moci USA založená na zákoně FISA počítá s přezkumem a v některých případech s předchozím povolením opatření Soudem pro uplatňování zákona FISA (FISA Court, FISC) ⁽¹³¹⁾, nezávislým soudem ⁽¹³²⁾, jehož rozhodnutí je možné napadnout u Odvolacího soudu pro uplatňování zákona FISA (FISCR) ⁽¹³³⁾ a dále u Nejvyššího soudu Spojených států ⁽¹³⁴⁾. V případě nutnosti předchozího povolení musí žádající orgány (FBI, NSA, CIA atd.) předložit návrh žádosti právníkům odboru národní bezpečnosti Ministerstva spravedlnosti, kteří ji zkontrolují a v případě potřeby vyžádají doplňující informace ⁽¹³⁵⁾. Jakmile je žádost finalizována, musí ji schválit ministr spravedlnosti, zástupce ministra spravedlnosti nebo náměstek ministra spravedlnosti pro otázky národní bezpečnosti ⁽¹³⁶⁾. Poté Ministerstvo spravedlnosti žádost předloží Soudu pro uplatňování zákona FISA, který ji vyhodnotí a předběžně rozhodne o dalších krocích ⁽¹³⁷⁾. Koná-li se ve věci jednání, má Soud pro uplatňování zákona FISA pravomoc vyslyšet, a to i znalce ⁽¹³⁸⁾.

- (106) Soudu pro uplatňování zákona FISA (i Odvolacímu soudu pro uplatňování zákona FISA) je nápomocen stálý panel pěti osob se zkušenostmi ve věcech národní bezpečnosti i občanských svobod ⁽¹³⁹⁾. 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 ⁽¹⁴⁰⁾. 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* poskytl 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) ⁽¹⁴¹⁾.

⁽¹³⁰⁾ USA FREEDOM Act, § 602(a), 603(a).

⁽¹³¹⁾ U některých druhů sledování může mít pravomoc projednávat žádosti a vydávat příkazy také magistrátní soudce veřejně jmenovaný předsedou Nejvyššího soudu Spojených států.

⁽¹³²⁾ Soud pro uplatňování zákona FISA je složen z jedenácti 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 okrsků. Viz § 103 zákona FISA (50 U.S.C. 1803 (a)); dokument PCLOB – Sec. 215 Report, s. 174–187. Soudcům jsou nápomocni zkušení soudní právníci, kteří tvoří právnícký personál soudu a kteří připravují právní analýzy žádostí o sběr údajů. Viz dokument PCLOB – Sec. 215 Report, s. 178; dopis předsedy Soudu pro uplatňování zákona FISA Reggie B. Waltona předsedovi výboru Senátu USA pro justici Patricku J. Leahymu (ze dne 29. července 2013) („Waltonův dopis“), s. 2–3.

⁽¹³³⁾ Odvolací soud pro uplatňování zákona FISA je složen z tří soudců jmenovaných předsedou Nejvyššího soudu Spojených států ze soudců okrskových nebo odvolacích soudů, kteří slouží v překrývajících se sedmiletých funkčních obdobích. Viz § 103 zákona FISA (50 U.S.C. § 1803 (b)).

⁽¹³⁴⁾ Viz 50 U.S.C. § 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

⁽¹³⁵⁾ Např. dodatečné faktické podrobnosti o cíli sledování, technické informace o metodě sledování nebo ujištění o tom, jak budou získané informace využity a šířeny. Viz dokument PCLOB – Sec. 215 Report, s. 177.

⁽¹³⁶⁾ 50 U.S.C. § 1804 (a), 1801 (g).

⁽¹³⁷⁾ Soud pro uplatňování zákona FISA může žádost schválit, vyžádat doplňující informace, rozhodnout o nezbytnosti jednání, nebo naznačit případné zamítnutí žádosti. Na základě tohoto předběžného posouzení pak vláda podá finální žádost. Ta se kvůli předběžným poznámkám soudce může od původní žádosti významně lišit. Soud pro uplatňování zákona FISA nakonec sice velkou část všech finálních žádostí schválí, u podstatné části z nich však oproti původní žádosti dojde k zásadním změnám, např. u žádostí schválených od července do září 2013 to bylo 24 %. Viz dokument PCLOB – Sec. 215 Report, s. 179; Waltonův dopis, s. 3.

⁽¹³⁸⁾ Viz dokument PCLOB – Sec. 215 Report, s. 179, pozn. 619.

⁽¹³⁹⁾ 50 U.S.C. § 1803 (i)(1),(3)(A). Tento nový právní předpis provádí doporučení Výboru pro dohled nad ochranou soukromí a občanských svobod na zřízení skupiny odborníků na ochranu soukromí a občanských svobod, která může sloužit jako *amicus curiae* a poskytovat soudu právní argumenty na podporu ochrany soukromí a občanských svobod. Viz dokument PCLOB – Sec. 215 Report, s. 183–187.

⁽¹⁴⁰⁾ 50 U.S.C. § 1803 (i)(2)(A). Podle informací ODNI již tato jmenování proběhla. Viz dokument Signals Intelligence Reform, 2016 Anniversary Report.

⁽¹⁴¹⁾ 50 U.S.C. § 1803 (i)(2)(B).

- (107) Pokud jde o dvě zákonná zmocnění ke sledování podle zákona FISA, která jsou nejdůležitější z hlediska předávání údajů v rámci štítu EU–USA na ochranu soukromí, dohled ze strany Soudu pro uplatňování zákona FISA se různí.
- (108) Podle § 501 zákona FISA ⁽¹⁴²⁾, kterým je povolen sběr „jakýchkoli hmatatelných věcí (včetně knih, záznamů, papírů, dokumentů a jiných položek)“, musí žádost podávaná u Soudu pro uplatňování zákona FISA obsahovat skutkový popis, který dokládá, že existuje důvodné podezření, že hledané hmatatelné věci jsou relevantní pro povolené vyšetřování (jiné než posouzení hrozby) za účelem získání zahraničních zpravodajských informací netýkajících se osoby USA nebo ochrany před mezinárodním terorismem nebo tajnými výzvědnými aktivitami. V žádosti musí být rovněž uveden výčet minimalizačních postupů přijatých ministrem spravedlnosti za účelem uchovávání a šíření shromážděných zpravodajských informací ⁽¹⁴³⁾.
- (109) Naproti tomu podle § 702 zákona FISA ⁽¹⁴⁴⁾ nepovoluje Soud pro uplatňování zákona FISA jednotlivá sledovací opatření, nýbrž povoluje celé sledovací programy (např. PRISM, UPSTREAM), a to na základě ročních osvědčení, která vypracovávají ministr spravedlnosti a ředitel národních zpravodajských služeb. Paragraf 702 zákona FISA dovoluje cílené sledování osob, o nichž se lze důvodně domnívat, že se nacházejí mimo území Spojených států, za účelem získávání zahraničních zpravodajských informací ⁽¹⁴⁵⁾. Toto cílené sledování provádí NSA ve dvou krocích: nejprve analytici NSA identifikují osoby, které nejsou osobami USA a které se nacházejí v zahraničí a jejichž sledování povede na základě posouzení analytiků k získání zahraničního zpravodajství, které je konkrétně stanoveno v osvědčení. Za druhé, jakmile jsou tyto individualizované osoby identifikovány a jejich cílené sledování schváleno rozsáhlým přezkumným mechanismem uvnitř NSA ⁽¹⁴⁶⁾, budou „zaúkolovány“ (tj. vyvinuty a použity) selektory identifikující komunikační prostředky (např. e-mailová adresa) používané cíli ⁽¹⁴⁷⁾. Jak bylo uvedeno výše, osvědčení, která Soud pro uplatňování zákona FISA schvaluje, neobsahují žádné informace o jednotlivých osobách, které jsou předmětem cíleného sledování, nýbrž jen identifikují kategorie zahraničních zpravodajských informací ⁽¹⁴⁸⁾. Soud pro uplatňování zákona FISA sice nezjišťuje – podle principu důvodného podezření či jiného principu –, zda jsou za účelem získání zahraničních zpravodajských informací fyzické osoby cíleny správně ⁽¹⁴⁹⁾, kontroluje však podmínku, že „důležitým účelem získávání informací je získání zahraničních zpravodajských informací“ ⁽¹⁵⁰⁾. Podle § 702 zákona FISA je totiž NSA oprávněna shromažďovat komunikaci osob, které nejsou osobami USA a které pobývají mimo území USA, jen tehdy, lze-li se důvodně domnívat, že předmětný způsob komunikace je používán k předávání zahraničních zpravodajských informací (např. souvisí s mezinárodním terorismem, šířením jaderných zbraní nebo nepřátelskými aktivitami v kyberprostoru). Rozhodnutí v tomto ohledu podléhají soudnímu přezkumu ⁽¹⁵¹⁾. Osvědčení musí rovněž stanovit postupy cíleného sběru a minimalizace ⁽¹⁵²⁾. Dodržování předpisů ověřují ministr spravedlnosti a ředitel národních zpravodajských služeb,

⁽¹⁴²⁾ 50 U.S.C. § 1861.

⁽¹⁴³⁾ 50 U.S.C. § 1861 (b).

⁽¹⁴⁴⁾ 50 U.S.C. § 1881.

⁽¹⁴⁵⁾ 50 U.S.C. § 1881a (a).

⁽¹⁴⁶⁾ Viz dokument PCLOB – Sec. 702 Report, s. 46.

⁽¹⁴⁷⁾ 50 U.S.C. § 1881a (h).

⁽¹⁴⁸⁾ 50 U.S.C. § 1881a (g). Podle výboru PCLOB se doposud tyto kategorie týkaly především mezinárodního terorismu a témat jako získávání zbraní hromadného ničení. Viz dokument PCLOB – Sec. 702 Report, s. 25.

⁽¹⁴⁹⁾ Dokument PCLOB – Sec. 702 Report, s. 27.

⁽¹⁵⁰⁾ 50 U.S.C. § 1881a.

⁽¹⁵¹⁾ Dokument „Liberty and Security in a Changing World“, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies ze dne 12. prosince 2013, s. 152.

⁽¹⁵²⁾ 50 U.S.C. § 1881a (i).

příčemž agentury mají povinnost hlásit veškeré případy nedodržení Soudu pro uplatňování zákona FISA ⁽¹⁵³⁾ (jakož i Kongresu a Výboru prezidenta pro dohled nad zpravodajstvím), který na tomto základě může povolení změnit ⁽¹⁵⁴⁾.

- (110) Za účelem zvýšení účinnosti dohledu prováděného Soudem pro uplatňování zákona FISA souhlasila vláda USA dále s tím, že provede doporučení výboru PCLOB poskytovat tomuto soudu dokumentaci k rozhodnutím o cíleném sběru podle § 702, a to včetně náhodného vzorku úkolovacích listů, aby tento soud mohl posoudit, jak je požadavek účelu zahraničního zpravodajství plněn v praxi ⁽¹⁵⁵⁾. Vláda USA zároveň s tím přijala a podnikla kroky k revizi postupů cíleného sběru v NSA tak, aby lépe dokumentovaly zahraničně zpravodajské důvody pro rozhodnutí o cíleném sběru ⁽¹⁵⁶⁾.

Individuální náprava

- (111) Právní předpisy USA poskytují subjektům údajů z EU několik možností nápravy, pokud se obávají, zda jejich osobní údaje byly zpracovány prvky zpravodajské komunity USA (zda je shromáždily, získaly k nim přístup apod.) a pokud ano, zda byla dodržena omezení podle platných právních předpisů. Tato omezení se v zásadě týkají těchto tří oblastí: zásah podle zákona FISA; nezákonný úmyslný přístup vládních úředníků k osobním údajům; a přístup k informacím podle zákona o svobodě informací (Freedom of Information Act, FOIA) ⁽¹⁵⁷⁾.
- (112) Za prvé, zákon o zabezpečování informací o činnostech cizí moci obsahuje řadu opravných prostředků, jimiž lze napadnout nezákonné elektronické sledování a jež jsou dostupné i osobám, které nejsou osobami USA ⁽¹⁵⁸⁾. Patří k nim možnost domáhat se občanskoprávními žalobami proti Spojeným státům peněžité náhrady škody v případě, kdy informace o nich byly použity nebo zveřejněny nezákonně a vědomě ⁽¹⁵⁹⁾; žalovat úředníky vlády USA soukromě (za „zneužití pravomoci“) o peněžitou náhradu škody ⁽¹⁶⁰⁾; 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 ve Spojených státech ⁽¹⁶¹⁾.
- (113) Za druhé, vláda USA odkázala Komisi na několik dalších možností, jimiž by se subjekty údajů z EU mohly domáhat právního postihu vůči vládním úředníkům za nezákonný přístup vlády k jejich osobním údajům nebo jejich nezákonné použití, včetně k účelům národní bezpečnosti (např. na zákon o počítačových podvodech

⁽¹⁵³⁾ Podle pravidla 13(b) jednacího řádu Soudu pro uplatňování zákona FISA je vláda povinna soud písemně informovat bezprostředně po zjištění, že pravomoc nebo schválení udělené soudem bylo provedeno způsobem, který je v rozporu s oprávněním nebo schválením soudu nebo s platnými právními předpisy. Podle tohoto pravidla je také vláda povinna písemně informovat soud o skutečnostech a okolnostech, které jsou relevantní pro takové nedodržení předpisů. Ve většině případů vláda podá finální oznámení podle pravidla 13(a), jakmile jsou známy všechny relevantní zkušenosti a veškeré neoprávněně shromážděné údaje zničeny. Viz Waltonův dopis, s. 10.

⁽¹⁵⁴⁾ 50 U.S.C. § 1881 (l). Viz také dokument PCLOB – Sec. 702 Report, s. 66–76; dokument NSA CLPO – NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 ze dne 16. dubna 2014. Sběr osobních údajů pro zpravodajské účely podle § 702 zákona FISA podléhá jak internímu, tak externímu dohledu v rámci výkonné moci. Interní dohled mimo jiné zahrnuje interní programy compliance, které vyhodnocují a sledují dodržování postupů cíleného sběru a minimalizace; hlášení případů nedodržení, jak interně, tak externě, úřadu ODNI, Ministerstvu spravedlnosti a Soudu pro uplatňování zákona FISA; a každoroční přezkumy zasílané tamtéž. Pokud jde o externí dohled, ten zahrnuje především přezkumy cíleného sběru a minimalizace prováděné úřadem ODNI, Ministerstvem spravedlnosti a generálními inspektory, kteří pak podávají zprávy a hlásí případy nedodržení Kongresu a Soudu pro uplatňování zákona FISA. Významné případy nedodržení předpisů musí být Soudu pro uplatňování zákona FISA hlášeny okamžitě, ostatní formou čtvrtletních zpráv. Viz dokument PCLOB – Sec. 702 Report, s. 66–77.

⁽¹⁵⁵⁾ Dokument PCLOB – Recommendations Assessment Report ze dne 29. ledna 2015, s. 20.

⁽¹⁵⁶⁾ Dokument PCLOB – Recommendations Assessment Report ze dne 29. ledna 2015, s. 16.

⁽¹⁵⁷⁾ Paragraf 10 zákona o zacházení s utajovanými skutečnostmi (*Classified Information Procedures Act*) pak navíc stanoví, že v trestním stíhání, ve kterém Spojené státy musí prokázat, že materiál představuje utajovanou skutečnost (např. protože vyžaduje ochranu proti neoprávněnému vyzrazení z důvodu národní bezpečnosti), informují Spojené státy obviněného, o které části materiálu pravděpodobně opírou svoje zdůvodnění toho, že trestný čin obsahuje prvek utajované skutečnosti.

⁽¹⁵⁸⁾ Viz k následujícímu prohlášení ODNI (příloha VI), s. 16.

⁽¹⁵⁹⁾ 18 U.S.C. § 2712.

⁽¹⁶⁰⁾ 50 U.S.C. § 1810.

⁽¹⁶¹⁾ 50 U.S.C. § 1806.

a zneužití počítače (*Computer Fraud and Abuse Act*) ⁽¹⁶²⁾; zákon o soukromí elektronických komunikací (*Electronic Communications Privacy Act*) ⁽¹⁶³⁾; a zákon o právu na finanční soukromí (*Right to Financial Privacy Act*) ⁽¹⁶⁴⁾). 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) ⁽¹⁶⁵⁾. Obecnější možnost nápravy umožňuje zákon o správním řízení (*Administrative Procedure Act*, 5 U.S.C. § 702), podle kterého „kdokoli, jemuž krok agentury způsobí právní křivdu nebo kdo je krokem agentury negativně postižen nebo poškozen,“ má právo domáhat se soudního přezkumu. Sem spadá možnost požádat soud, „aby prohlásil za neplatné nebo zrušil krok, zjištění a závěry agentury, které jsou výsledkem [...] aktu svévolie či zvlů, zneužitím diskreční pravomoci či jinak v rozporu se zákonem“ ⁽¹⁶⁶⁾.

- (114) A konečně vláda USA upozornila to, že na základě zákona o svobodě informací se osoby, které nejsou osobami USA, mohou domáhat přístupu k existujícím záznamům federálních vládních agentur, včetně případů, kdy tyto záznamy obsahují osobní údaje této osoby ⁽¹⁶⁷⁾. Vzhledem ke svému zaměření neposkytuje tento zákon fyzickým osobám žádnou možnost obrátit se na soud kvůli zásahu do osobních údajů, ačkoli by jim měl v zásadě umožnit přístup k relevantním informacím, které drží národní zpravodajské agentury. I v tomto ohledu se možnosti zdají být omezené, neboť agentury nemusí poskytnout informace, které spadají pod několik vyjmenovaných výjimek, mimo jiné pod přístup k utajovaným informacím souvisejícím s národní bezpečností a k informacím o vyšetřovaných donucovacích orgánech ⁽¹⁶⁸⁾. Fyzické osoby mohou využívání těchto výjimek národními zpravodajskými agenturami napadnout u soudu a domáhat se jak správního, tak soudního přezkumu.
- (115) Zatímco fyzické osoby, včetně subjektů údajů z EU, tedy mají k dispozici několik možností nápravy, pokud se staly předmětem nezákonného (elektronického) sledování z důvodu národní bezpečnosti, je stejně tak jasné, že přinejmenším některých z právních základů, které zpravodajské orgány USA mohou využít (např. EO 12223), se to netýká. Navíc i tehdy, pokud pro osoby, které nejsou osobami USA, možnosti nápravy v zásadě existují, např. u sledování podle zákona FISA, jsou dostupné právní kroky omezené ⁽¹⁶⁹⁾ a nároky vznesené fyzickými osobami (včetně osob USA), které neprokáží „aktivní legitimaci“, budou prohlášeny za nepřipustné ⁽¹⁷⁰⁾, což omezuje přístup k běžným soudům ⁽¹⁷¹⁾.
- (116) Ve snaze poskytnout dodatečnou možnost nápravy, k níž by měli přístup všechny subjekty údajů z EU, rozhodla se vláda USA vytvořit mechanismus ombudsmana, který je popsán v dopise ministra zahraničí Komisi, jenž tvoří přílohu III tohoto rozhodnutí. Tento mechanismus vychází z toho, že podle směrnice PPD-28 je na Ministerstvu zahraničních věcí zřízen post senior koordinátora (na úrovni tajemníka ministra), který slouží jako kontaktní místo, u nějž mohou cizí vlády vyjádřit své obavy v souvislosti se signálovým zpravodajstvím USA, avšak tento základní koncept dále podstatně rozvádí.

⁽¹⁶²⁾ 18 U.S.C. § 1030.

⁽¹⁶³⁾ 18 U.S.C. § 2701-2712.

⁽¹⁶⁴⁾ 12 U.S.C. § 3417.

⁽¹⁶⁵⁾ Prohlášení ODNI (příloha VI), s. 17.

⁽¹⁶⁶⁾ 5 U.S.C. § 706(2)(A).

⁽¹⁶⁷⁾ 5 U.S.C. § 552. Podobné zákony existují na úrovni jednotlivých federálních států USA.

⁽¹⁶⁸⁾ 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).

⁽¹⁶⁹⁾ Viz prohlášení ODNI (příloha VI), s. 16. Podle poskytnutých vysvětlení závisí dostupné právní kroky buď na existenci škody (18 U.S.C. § 2712; 50 U.S.C. § 1810), nebo na prokázání toho, že vláda hodlá použít nebo zveřejnit informace získané nebo odvozené z elektronického sledování dotčené osoby proti této osobě v soudním nebo správním řízení ve Spojených státech (50 U.S.C. § 1806). Jak však opakovaně zdůraznil Soudní dvůr, pro prokázání existence zásahu do základního práva na respektování soukromého života není důležité, zda dotčené informace o soukromém životě představují citlivé údaje nebo zda dotčené osoby utrpěly z důvodu tohoto zásahu případné nepříznivé následky. Viz *Schrems*, bod 89 s dalšími odkazy.

⁽¹⁷⁰⁾ Toto kritérium přípustnosti plyne z požadavku *case or controversy* podle článku III Ústavy Spojených států.

⁽¹⁷¹⁾ Viz věc *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). Pokud jde o použití NSL, zákon *USA FREEDOM Act* (§ 502(f)–503) stanoví, že požadavky na nezveřejnění musí být pravidelně přezkoumávány a že příjemci NSL musí být informováni, jakmile pominou skutečnosti, které odůvodňují požadavek na nezveřejnění (viz prohlášení ODNI (příloha VI), s. 13). Tím však není zajištěno, že subjekt údajů z EU bude informován o tom, že byl cílem vyšetřování.

- (117) Podle závazků vlády USA mechanismus ombudsmana zejména zaručí, aby jednotlivé stížnosti byly řádně prošetřeny a řešeny a aby fyzické osoby obdržely nezávislé potvrzení o tom, že právní předpisy USA byly dodrženy, nebo že v případě jejich porušení bylo toto nedodržení napraveno ⁽¹⁷²⁾. Tento mechanismus obsahuje „ombudsmana ve věcech štítu na ochranu soukromí“, tj. tajemníka ministra a další zaměstnance a dále subjekty dohledu, které jsou příslušné dohlížet na jednotlivé prvky zpravodajské komunity a na jejichž spolupráci se ombudsman ve věcech štítu na ochranu soukromí bude spoléhat při vyřizování stížností. Konkrétně pokud se žádost fyzické osoby týká slučitelnosti sledování se zákony USA, bude se ombudsman ve věcech štítu na ochranu soukromí moci spoléhat na nezávislé subjekty dohledu s vyšetřovacími pravomocemi (jako jsou generální inspektoři nebo PCLOB). V každém případě ministr zahraničních věcí zajistí, aby ombudsman měl možnost zajistit, aby jeho odpověď na žádosti fyzických osob byla založena na veškerých nezbytných informacích.
- (118) Touto „smíšenou strukturou“ mechanismu ombudsmana je zajištěn nezávislý dohled a individuální náprava. Spoluprací s jinými subjekty dohledu je pak také zajištěn přístup k nezbytným odborným znalostem. A konečně tím, že má ombudsman ve věcech štítu na ochranu soukromí povinnost potvrdit dodržování zásad nebo nápravu nedodržení zásad, odráží tento mechanismus závazek vlády USA jako celku řešit stížnosti fyzických osob z EU.
- (119) Za prvé, na rozdíl od čistě mezivládního mechanismu se ombudsman ve věcech štítu na ochranu soukromí bude zabývat stížnostmi jednotlivých fyzických osob. Tyto stížnosti mohou být adresovány orgánům dohledu v členských státech odpovědným za dohled nad službami národní bezpečnosti a/nebo zpracováváním osobních údajů orgány veřejné moci, které pak tyto stížnosti budou předávat centralizovanému subjektu na úrovni EU, který je bude postupovat ombudsmanovi ve věcech štítu na ochranu soukromí ⁽¹⁷³⁾. To bude ku prospěchu fyzických osob z EU, které se mohou obracet na jim blízký vnitrostátní subjekt a v jejich vlastním jazyce. Úkolem takového orgánu bude pomáhat fyzické osobě při podávání žádosti ombudsmanovi ve věcech štítu na ochranu soukromí, která obsahuje základní informace, a kterou tak lze považovat za „úplnou“. Fyzická osob přitom nemusí prokázat, že vláda USA činností signálového zpravodajství získala přístup k jeho osobním údajům.
- (120) Za druhé, vláda USA se zavazuje zajistit, že při výkonu svých funkcí se ombudsman ve věcech štítu na ochranu soukromí bude moci spoléhat na spolupráci jiných mechanismů dohledu a přezkumu dodržování předpisů, které existují v právu USA. To bude někdy zahrnovat národní zpravodajské orgány, zejména tam, kdy má žádost být vykládána jako žádost o přístup k dokumentům podle zákona o svobodě informací. V jiných případech, zejména pokud se žádosti týkají slučitelnosti sledování s právem USA, bude taková spolupráce zahrnovat nezávislé subjekty dohledu (např. generální inspektory) s odpovědností a pravomocí provádět důkladné vyšetřování (zejména přístupem ke všem relevantním dokumentům a pravomocí žádat o informace a prohlášení) a řešit případy nedodržení zásad ⁽¹⁷⁴⁾. Ombudsman ve věcech štítu na ochranu soukromí bude také moci postupovat věci Výboru pro dohled nad ochranou soukromí a občanských svobod k posouzení ⁽¹⁷⁵⁾. Zjistí-li některý z těchto subjektů dohledu nedodržení, bude muset dotčený prvek zpravodajské komunity (např. zpravodajská služba) toto nedodržení napravit, neboť jen tak bude ombudsman moci dát fyzické osobě „kladnou“ odpověď (tj. že

⁽¹⁷²⁾ Pokud stěžovatel usiluje o přístup k dokumentům, které drží orgány veřejné moci USA, použijí se pravidla a postupy uvedené v zákoně o svobodě informací (FOIA). Sem patří možnost domáhat se nápravy u soudu (a nejen nezávislého dohledu) v případě, kdy je žádost zamítnuta, v souladu s podmínkami uvedenými v zákoně FOIA.

⁽¹⁷³⁾ Podle mechanismu ombudsmana (příloha III, bod 4 písm. f)) bude ombudsman ve věcech štítu na ochranu soukromí komunikovat přímo se subjektem pro vyřizování stížností fyzických osob z EU, který pak bude mít na starosti komunikaci fyzickou osobou podávající stížnost. Je-li komunikace součástí „podkladových procesů“, které mohou poskytnout požadovanou nápravu (např. žádost o přístup podle zákona o svobodě informací, viz bod 5), bude taková komunikace probíhat v souladu s platnými postupy.

⁽¹⁷⁴⁾ Viz mechanismus ombudsmana (příloha III), bod 2 písm. a). Viz také 0. až 0. bod odůvodnění.

⁽¹⁷⁵⁾ Viz mechanismus ombudsmana (příloha III), bod 2 písm. c). Podle vysvětlení vlády USA Výbor pro dohled nad ochranou soukromí a občanských svobod průběžně přezkoumává politiky a postupy orgánů USA odpovědných za boj proti terorismu a jejich provádění za účelem stanovení, zda jejich činnost „náležitě ochraňuje soukromí a občanské svobody a zda je v souladu s platnými zákony, předpisy a politikami v oblasti ochrany soukromí a občanských svobod“. Výbor dále „posuzuje zprávy a další informace mu předkládané úředníky pro otázky ochrany soukromí a občanských svobod a ve vhodných případech jim vydává doporučení ohledně jejich činnosti“.

nedodržení bylo napraveno), k čemuž se vláda USA zavázala. Součástí spolupráce bude také informování ombudsmana ve věcech štítu na ochranu soukromí o výsledku vyšetřování a ombudsman bude mít možnost zajistit, aby obdržel veškeré nezbytné informace pro přípravu odpovědi.

- (121) A konečně ombudsman ve věcech štítu na ochranu soukromí bude nezávislý, a tudíž nepodléhající pokynům zpravodajské komunity USA ⁽¹⁷⁶⁾. To je zásadně důležité, jelikož ombudsman bude muset „osvědčit“, zda i) byla stížnost řádně prošetřena a zda ii) bylo dodrženo právo USA – včetně omezení a ochranných opatření uvedených v příloze VI –, nebo v případě nedodržení bylo takové porušení napraveno. Aby mohl toto nezávislé osvědčení vydat, ombudsman ve věcech štítu na ochranu soukromí bude muset disponovat nezbytnými informacemi o vyšetřování, aby mohl posoudit přesnost odpovědi stěžovateli. Ministr zahraničních věcí se kromě toho zavázal zajistit, že tajemník ministra bude funkci ombudsmana ve věci štítu na ochranu soukromí vykonávat objektivně a nezávisle na jakémkoli nevhodném vlivu, který by mohl mít dopad na odpověď, která má být poskytnuta.
- (122) Celkově vzato tento mechanismus zajišťuje, že jednotlivé stížnosti fyzických osob budou důkladně vyšetřeny a vyřešeny a že přinejmenším v oblasti sledování bude toto zahrnovat nezávislé subjekty dohledu s nezbytnými zkušenostmi a vyšetřovacími pravomocemi a ombudsmana, který bude schopen vykonávat své funkce nezávisle na nevhodném, zejména politickém vlivu. Fyzické osoby budou navíc stížnosti moci podávat, aniž by musely dokazovat či jen poskytovat náznaky o tom, že byly předmětem sledování ⁽¹⁷⁷⁾. Ve světle těchto vlastností je Komise přesvědčena o tom, že existují odpovídající a účinné záruky proti zneužití.
- (123) Na základě výše uvedeného Komise konstatuje, že Spojené státy zajišťují účinnou právní ochranu před zásahy jejich zpravodajských orgánů do základních práv osob, jejichž data jsou předávána z Unie do Spojených států v rámci štítu EU–USA na ochranu soukromí.
- (124) V tomto ohledu Komise bere na vědomí rozsudek Soudního dvora ve věci *Schrems*, podle nějž „právní úprava, která nestanoví procesním subjektům žádnou možnost využít právních prostředků s cílem získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu těchto údajů, nerespektuje podstatu základního práva na účinnou právní ochranu zakotveného v článku 47 Listiny“ ⁽¹⁷⁸⁾. Posouzení Komise potvrdilo, že ve Spojených státech jsou takové právní prostředky k dispozici, a to mimo jiné zavedením mechanismu ombudsmana. Mechanismus ombudsmana poskytuje nezávislý dohled s vyšetřovacími pravomocemi. Účinnost tohoto mechanismu bude vyhodnocena v rámci průběžného monitorování štítu na ochranu soukromí ze strany Komise, včetně prostřednictvím výročního společného přezkumu, který bude rovněž zahrnovat ombudsmana.

3.2 Přístup orgánů veřejné moci USA k údajům a použití údajů těmito orgány pro účely prosazování práva a veřejného zájmu

- (125) Pokud jde o zásahy do osobních údajů předávaných v rámci štítu EU–USA na ochranu soukromí pro účely prosazování práva, poskytla vláda USA (prostřednictvím Ministerstva spravedlnosti) ujištění týkající se použitelných omezení a ochranných opatření, která dle posouzení Komise dokládají odpovídající úroveň ochrany.

⁽¹⁷⁶⁾ Viz věc *Roman Zakharov v. Russia*, rozsudek ze dne 4. prosince 2015 (velký senát), stížnost č. 47143/06, bod 275 („ačkoli je v zásadě žádoucí svěřit dohled soudci, dohled ze strany nesoudních subjektů lze považovat za slučitelný s Úmluvou za předpokladu, že je tento subjekt dohledu nezávislý na orgánech provádějících sledování a jsou mu svěřeny dostatečné a účinné pravomoci dohledu“).

⁽¹⁷⁷⁾ Viz věc *Kennedy v. the United Kingdom*, rozsudek ze dne 18. května 2010, stížnost č. 26839/05, bod 167.

⁽¹⁷⁸⁾ *Schrems*, bod 95. Jak vyplývá u bodů 91 a 96 rozsudku, bod 95 se týká úrovně ochrany zaručené právním řádem Unie, jíž musí být úroveň ochrany ve třetí zemi „v zásadě rovnocenná“. Podle bodů 73 a 74 rozsudku to sice neznamená, že úroveň ochrany nebo prostředky, které třetí země v tomto směru využívá, musí být stejná, ale prostředky, které mají být využity, se musí v praxi ukázat jako účinné.

- (126) Podle těchto informací je v souladu s čtvrtým dodatkem Ústavy USA ⁽¹⁷⁹⁾ pro účel domovní prohlídky a zabavení ze strany donucovacích orgánů především ⁽¹⁸⁰⁾ požadován soudní příkaz vystavený na základě prokázání „důvodného podezření“. V několika málo konkrétně stanovených a výjimečných případech, kdy se požadavek soudního příkazu nepoužije ⁽¹⁸¹⁾, je prosazení práva podmíněno ověřením „přiměřenosti“ ⁽¹⁸²⁾. Zda je domovní prohlídka nebo zabavení věci přiměřené, „se stanoví na straně jedné posouzením míry, do jaké tento úkon zasahuje do soukromí fyzické osoby, a na straně druhé posouzením míry, do jaké je tento úkon nutný za účelem prosazení legitimních zájmů vlády“ ⁽¹⁸³⁾. Obecněji řečeno tedy čtvrtý dodatek americké ústavy zaručuje soukromí, důstojnost a chrání před svévolnými a invazivními akty úředníků vlády USA ⁽¹⁸⁴⁾. Toto pojetí vystihuje myšlenku nezbytnosti a proporcionality v právu Unie. Jakmile donucovací orgány přestanou mít potřebu použít zabavené věci jako důkaz, měly by být věci vráceny ⁽¹⁸⁵⁾.
- (127) Ačkoli práva plynoucí ze čtvrtého dodatku se nevztahují na osoby, které nejsou osobami USA a které nepobývají ve Spojených státech, jsou tyto osoby jeho ochranou částečně chráněny z toho titulu, že osobní údaje drží společností z USA, což má ten účinek, že donucovací orgány musí v každém případě žádat soud o povolení (anebo alespoň řídit se požadavkem přiměřenosti) ⁽¹⁸⁶⁾. Další ochrana je poskytována prostřednictvím zvláštních právních předpisů a pokynů Ministerstva spravedlnosti, které omezují přístup donucovacích orgánů k údajům z důvodů rovnocenných zásadám nezbytnosti a proporcionality (např. požadavkem, aby FBI používala co nejméně invazivní vyšetřovací metody, jaké jsou možné, s ohledem na jejich dopad na soukromí a občanské svobody) ⁽¹⁸⁷⁾. Podle prohlášení vlády USA platí stejná nebo vyšší úroveň ochrany pro vyšetřování donucovacích orgánů na úrovni federálních států (s ohledem na vyšetřování prováděná podle zákonů státu) ⁽¹⁸⁸⁾.
- (128) Ačkoli předchozí povolení soudu nebo velké poroty (vyšetřující složky soudu sestavené soudcem nebo magistrátním soudcem) se nevyžaduje ve všech případech ⁽¹⁸⁹⁾, správní předvolání (*subpoena*) jsou omezena na konkrétní případy a budou předmětem nezávislého soudního přezkumu alespoň v případech, kdy se vláda domáhá prosazení práva před soudem ⁽¹⁹⁰⁾.
- ⁽¹⁷⁹⁾ Podle čtvrtého dodatku „[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 neexistuje 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“. Takové příkazy smějí vydávat pouze (magistrátní) soudci. Federální příkazy ke kopírování elektronicky uložených informací se dále řídí pravidlem 41 federálního trestního řádu (*Federal Rules of Criminal Procedure*).
- ⁽¹⁸⁰⁾ Nejvyšší soud domovní prohlídky bez soudního příkazu opakovaně nazývá „výjimečné“. Viz např. *Johnson v. United States*, 333 U.S. 10, 14 (1948); *McDonald v. United States*, 335 U.S. 451, 453 (1948); *Camara v. Municipal Court*, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352-53, 355 (1977). Nejvyšší soud také pravidelně zdůrazňuje, že „nejzákladnějším ústavním pravidlem v této oblasti je, že prohlídky prováděné mimo soudní proces, bez předchozího souhlasu soudce jsou ze své podstaty nepřiměřené podle čtvrtého dodatku Ústavy – s výhradou pouze několika specifických a přesně vymezených výjimek.“ Viz např. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352-53, 358 (1977).
- ⁽¹⁸¹⁾ Věc *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).
- ⁽¹⁸²⁾ Dokument PCLOB – Sec. 215 Report, s. 107, s odkazem na věc *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).
- ⁽¹⁸³⁾ Dokument PCLOB – Sec. 215 Report, s. 107, s odkazem na věc *Samson v. California*, 547 U.S. 843, 848 (2006).
- ⁽¹⁸⁴⁾ Věc *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.
- ⁽¹⁸⁵⁾ Viz např. *United States v. Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).
- ⁽¹⁸⁶⁾ Srov. věc *Roman Zakharov v. Russia*, rozsudek ze dne 4. prosince 2015 (velký senát), stížnost č. 47143/06, bod 269, podle nějž „požadavek předložit povolení k odposlouchávání poskytovateli komunikačních služeb ještě před získáním přístupu ke komunikacím osoby je jedním z důležitých opatření na ochranu před zneužitím ze strany donucovacích orgánů, které zajišťuje, aby ve všech případech odposlouchávání bylo předloženo řádné povolení“.
- ⁽¹⁸⁷⁾ Prohlášení Ministerstva spravedlnosti (příloha VII), s. 4 s dalšími odkazy.
- ⁽¹⁸⁸⁾ Prohlášení Ministerstva spravedlnosti (příloha VII), pozn. 2.
- ⁽¹⁸⁹⁾ Podle informací, které Komise získala, a nehledě na specifické oblasti, které jsou z hlediska předávání údajů v rámci štítu EU–USA na ochranu soukromí nejspíše irrelevantní (např. vyšetřování podvodů v oblasti zdravotnictví, týrání dítěte, zneužívání kontrolovaných látek), týká se toto hlavně určitých pravomocí podle zákona o soukromí elektronických komunikací (ECPA), zejména pak žádostí o základní informace o účastníkovi, hovorech a fakturaci (18 U.S.C. § 2703(c)(1)(2)), např. adresa, druh/délka služby) a o obsah e-mailů starších než 180 dnů (18 U.S.C. § 2703(a), (b)). V druhém jmenovaném případě však musí být fyzická osoba informována, a má tak příležitost napadnout takovou žádost u soudu. Viz také přehled v dokumentu Ministerstva spravedlnosti – Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, kapitola 3: The Stored Communications Act, s. 115–138.
- ⁽¹⁹⁰⁾ Podle prohlášení vlády USA mohou příjemci správních předvolání taková předvolání napadnout u soudu pro jeho nepřiměřenost, tj. proto, že je přehnané, utiskující nebo zatěžující. Viz prohlášení Ministerstva spravedlnosti (příloha VII), s. 2.

- (129) Totéž platí pro správní předvolání pro účely veřejného zájmu. Kromě toho podle prohlášení vlády USA platí podobná hmotněprávní omezení v tom, že agentury se mohou domáhat přístupu pouze k těm údajům, které mají souvislost s věcmi, jež spadají do jejich pravomoci, a musí respektovat zásadu přiměřenosti.
- (130) 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. 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.
- (131) Obecně podle zákona o správním řízení ⁽¹⁹¹⁾ „kdokoli, jemuž krok agentury způsobí právní křivdu nebo kdo je krokem agentury negativně postižen nebo poškozen,“ má právo domáhat se soudního přezkumu ⁽¹⁹²⁾. Sem spadá možnost požádat soud, „aby prohlásil za neplatné nebo zrušil krok, zjištění a závěry agentury, které byly shledány [...] aktem svévole či zvláště, zneužitím diskreční pravomoci či jinak v rozporu se zákonem“ ⁽¹⁹³⁾.
- (132) Konkrétněji pak hlava II zákona o soukromí elektronických komunikací ⁽¹⁹⁴⁾ stanoví systém zákonných práv v oblasti soukromí a jako taková upravuje přístup donucovacích orgánů k obsahu telefonních, ústních nebo elektronických komunikací uložených třetími stranami-poskytovateli služeb ⁽¹⁹⁵⁾. Trestně postihuje nezákonný (tj. nepovolený soudem nebo jinak přípustný) přístup k takovým komunikacím a umožňuje postižené fyzické osobě možnost právní ochrany podáním občanskoprávní žaloby u federálního soudu USA na náhradu škody skutečné a punitivní, jakož i na vydání přiměřeného nebo deklaratorního nápravného opatření proti úředníkovi vlády, který takové nezákonné činy vědomě spáchal, nebo proti Spojeným státům.
- (133) Podle zákona o svobodě informací (FOIA, 5 U.S.C. § 552) má také každá osoba právo získat přístup k záznamům federální agentury a po vyčerpání správních opravných prostředků domáhat se tohoto práva u soudu, kromě případů, kdy jsou takové záznamy chráněny proti zveřejnění výjimkou nebo zvláštním vyloučením pro účely prosazení práva ⁽¹⁹⁶⁾.

⁽¹⁹¹⁾ 5 U.S.C. § 702.

⁽¹⁹²⁾ Soudnímu přezkumu podléhá obecně jen „konečný“, nikoli „předběžný, procesní nebo zprostředkovací“ úkon agentury. Viz 5 U.S.C. § 704.

⁽¹⁹³⁾ 5 U.S.C. § 706(2)(A).

⁽¹⁹⁴⁾ 18 U.S.C. § 2701-2712.

⁽¹⁹⁵⁾ 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.

⁽¹⁹⁶⁾ Tato vyloučení jsou však přesně definována. 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)).

- (134) Několik dalších zákonů dává fyzickým osobám právo žalovat orgán veřejné moci USA nebo úředníka, pokud jde o zpracování osobních údajů, například zákon o odposleších (*Wiretap Act*) ⁽¹⁹⁷⁾, zákon o počítačových podvodech a zneužití počítače (*Computer Fraud and Abuse Act*) ⁽¹⁹⁸⁾, zákon o deliktích žalobách u federálního soudu (*Federal Torts Claim Act*) ⁽¹⁹⁹⁾, zákon o právu na finanční soukromí (*Right to Financial Privacy Act*) ⁽²⁰⁰⁾, a zákon o spravedlivém informování o úvěrové spolehlivosti (*Fair Credit Reporting Act*) ⁽²⁰¹⁾.
- (135) Komise tedy konstatuje, že ve Spojených státech jsou zavedena pravidla, jejichž smyslem je omezovat zásahy pro účely prosazování práva ⁽²⁰²⁾ nebo jiné účely veřejného zájmu do základních práv osob, jejichž osobní údaje jsou předávány z Unie do Spojených států v rámci štítu EU–USA na ochranu soukromí, na rozsah striktně nezbytný k tomu, aby bylo dosaženo příslušného legitimního cíle, a která zajišťují účinnou právní ochranu před takovými zásahy.

4. ODPOVÍDAJÍCÍ ÚROVEŇ OCHRANY V RÁMCI ŠTÍTU EU–USA NA OCHRANU SOUKROMÍ

- (136) Ve světle těchto zjištění Komise konstatuje, že Spojené státy zajišťují odpovídající úroveň ochrany osobních údajů předáváných z Unie autocertifikovaným organizacím ve Spojených státech v rámci štítu EU–USA na ochranu soukromí.
- (137) Komise má zejména za to, že zásady vydané Ministerstvem obchodu USA jako celek zajišťují úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni ochrany zaručené základními zásadami stanovenými ve směrnici 95/46/ES.
- (138) Účinné uplatňování zásad kromě toho zaručují povinnosti ohledně transparentnosti a správa štítu na ochranu soukromí Ministerstvem obchodu.
- (139) Komise má dále za to, že dohlížecí a odvolací mechanismy poskytované štítem na ochranu soukromí jako celek umožňují, aby porušení zásad ze strany organizací, které jsou součástí štítu na ochranu soukromí, byla v praxi odhalována a postihována, a poskytují subjektu údajů procesní prostředky, které mu umožní získat přístup k osobním údajům, která se jej týkají, a v konečném důsledku dosáhnout opravy nebo výmazu takových údajů.
- (140) Konečně na základě dostupných informací o právním řádu USA, včetně prohlášení a závazků vlády USA, Komise konstatuje, že jakýkoli zásah orgány veřejné moci USA do základních práv osob, jejichž údaje jsou předávány z Unie do Spojených států v rámci štítu na ochranu soukromí za účelem národní bezpečnosti, prosazování práva nebo jiného veřejného zájmu, a z toho plynoucí omezení kladená na autocertifikované společnosti s ohledem na jejich přijetí zásad bude omezen na rozsah striktně nezbytný k tomu, aby bylo dosaženo příslušného legitimního cíle, a že existuje účinná právní ochrana proti takovým zásahům.

⁽¹⁹⁷⁾ 18 U.S.C. § 2510 a násl. Podle zákona o odposleších (18 U.S.C. § 2520) může osoba, jejíž telefonní, ústní nebo elektronické komunikace je odposlouchávána, zveřejněna nebo úmyslně použita, zahájit občanskoprávní řízení pro porušení zákona o odposleších, a to v určitých okolnostech i proti jednotlivému vládnímu úředníkovi nebo Spojeným státům. Pokud jde o sběr adresových a jiných neobsahových informací (např. adresy IP, e-mailové adresy odesílatele/příjemce) viz také kapitola o zařízeních k záznamu příchozích a odchozích telefonních čísel (*Pen Registers and Trap and Trace Devices*) hlavy 18 (18 U.S.C. § 3121–3127 a pro občanskoprávní řízení § 2707).

⁽¹⁹⁸⁾ 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 nebo jiného konkrétního počítače vlády USA.

⁽¹⁹⁹⁾ 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.“

⁽²⁰⁰⁾ 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.

⁽²⁰¹⁾ 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.

⁽²⁰²⁾ Soudní dvůr objasnil, že národní bezpečnost je legitimním politickým cílem. Viz spojené věci C-293/12 a C-594/12, *Digital Rights Ireland a další*, EU:C:2014:238, bod 42. Viz také čl. 8 odst. 2 Evropské úmluvy o ochraně lidských práv a rozsudek Evropského soudu pro lidská práva ve věci *Weber and Saravia v. Germany*, stížnost č. 54934/00, bod 104.

- (141) Komise došla k závěru, že tím jsou splněny požadavky článku 25 směrnice 95/46/ES vykládaného ve světle Listiny základních práv Evropské unie, jak vysvětlil Soudní dvůr zejména v rozsudku ve věci *Schrems*.

5. POSTUP ORGÁNŮ PRO OCHRANU ÚDAJŮ A INFORMACE PRO KOMISI

- (142) Soudní dvůr v rozsudku ve věci *Schrems* vysvětlil, že Komise není příslušná omezovat pravomoci orgánů pro ochranu údajů, které vyplývají z článku 28 směrnice 95/46/ES (včetně pravomoci zastavit přenosy údajů) v případě, že osoba v rámci žádosti podané na základě tohoto ustanovení zpochybní sloučitelnost rozhodnutí Komise o odpovídající úrovni ochrany s ochranou základního práva na soukromí a ochranu údajů ⁽²⁰³⁾.
- (143) Aby mohla Komise účinně monitorovat fungování štítu na ochranu soukromí, měly by ji členské státy informovat o relevantních krocích orgánů pro ochranu údajů.
- (144) Soudní dvůr dále konstatoval, že v souladu s čl. 25 odst. 6 druhým pododstavcem směrnice 95/46/ES musí členské státy a jejich orgány přijmout opatření nezbytná pro 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. V důsledku toho je rozhodnutí Komise o odpovídající úrovni ochrany podle čl. 25 odst. 6 směrnice 95/46/ES závazné pro všechny orgány členských států, kterým je určeno, a to i pro nezávislé orgány dozoru ⁽²⁰⁴⁾. Jestliže takový orgán obdrží stížnost, jež zpochybňuje soulad rozhodnutí Komise o odpovídající úrovni ochrany s ochranou základního práva na soukromí a ochranu údajů, a usoudí, že stížnost je opodstatněná, musí mu vnitrostátní právo poskytnout procesní prostředek, který mu umožní uplatnit tyto námitky před vnitrostátním soudem, který v případě pochybností přeruší řízení a předloží Soudnímu dvoru žádost o rozhodnutí o předběžné otázce ⁽²⁰⁵⁾.

6. PRAVIDELNÝ PŘEZKUM ZJIŠTĚNÍ O ODPOVÍDAJÍCÍ ÚROVNI OCHRANY

- (145) S ohledem na skutečnost, že úroveň ochrany poskytovaná právním řádem USA se může změnit, bude Komise po přijetí tohoto rozhodnutí pravidelně ověřovat, zda zjištění týkající se odpovídající úrovně ochrany zajištěné Spojenými státy v rámci štítu EU–USA na ochranu soukromí je nadále skutkově i právně podložené. Takové ověření se požaduje v každém případě, obdrží-li Komise jakoukoli informaci, která v tomto směru vyvolá oprávněné pochybnosti ⁽²⁰⁶⁾.
- (146) Komise bude proto průběžně monitorovat celkový rámec předávání osobních údajů tvořený štítem EU–USA na ochranu soukromí a taktéž to, zda orgány USA dodržují prohlášení a závazky uvedené v dokumentech, které tvoří přílohu tohoto rozhodnutí. Aby byl tento postup usnadněn, zavázaly se Spojené státy informovat Komisi o důležitém vývoji v právu USA, pokud je relevantní pro štít na ochranu soukromí v oblasti ochrany údajů a omezení a ochranných opatření použitelných v oblasti přístup k osobním údajům ze strany orgánů veřejné moci. Toto rozhodnutí bude dále předmětem výročního společného přezkumu, který se bude týkat všech aspektů fungování štítu EU–USA na ochranu soukromí, včetně použití omezení zásad z důvodu národní bezpečnosti a prosazování práva. Jelikož toto rozhodnutí o odpovídající úrovni ochrany může být ovlivněno právním vývojem v Unii, Komise kromě toho vyhodnotí úroveň ochrany poskytované štítem na ochranu soukromí po dni použitelnosti obecného nařízení o ochraně údajů.
- (147) Za účelem provedení výročního společného přezkumu podle příloh I, II a VI se Komise sejde s Ministerstvem obchodu a Federální obchodní komisí a případně s dalšími ministerstvy a agenturami, které se účastní provádění ujednání štítu EU–USA na ochranu soukromí, a dále ve věcech týkajících se národní bezpečnosti se zástupci ODNI, dalších prvků zpravodajské komunity a ombudsmanem. Účast na těchto schůzkách bude otevřena orgánům pro ochranu údajů z EU a zástupcům pracovní skupiny zřízené podle článku 29.

⁽²⁰³⁾ *Schrems*, body 40 a násl., 101–103.

⁽²⁰⁴⁾ *Schrems*, body 51, 52 a 62.

⁽²⁰⁵⁾ *Schrems*, bod 65.

⁽²⁰⁶⁾ *Schrems*, bod 76.

- (148) V rámci výročního společného přezkumu požádá Komise Ministerstvo obchodu, aby předložilo úplné informace o všech relevantních aspektech fungování štítu EU–USA na ochranu soukromí, včetně případů postoupených orgány pro ochranu údajů Ministerstvu obchodu a výsledků kontrol dodržování zásad prováděných z moci úřední. Komise bude rovněž požadovat vysvětlení ohledně jakýchkoli otázek či věcí týkajících se štítu EU–USA na ochranu soukromí a jeho fungování pramenících z jakýchkoli dostupných informací, např. zpráv o transparentnosti podle zákona USA *FREEDOM Act*, veřejných zpráv národních zpravodajských orgánů USA, orgánů pro ochranu údajů, skupin činných v oblasti ochrany soukromí, zpráv sdělovacích prostředků či z jakéhokoli jiného zdroje. Aby členské státy úkol Komisi v tomto ohledu usnadnily, měly by ji informovat o případech, kdy opatření subjektů odpovědných za zajištění dodržování zásad ve Spojených státech dodržení zásad nezajistí, a o veškerých známkách toho, že opatření orgánů veřejné moci USA odpovědných za národní bezpečnost nebo prevenci, vyšetřování, odhalování či stíhání trestných činů nezajišťují odpovídající úroveň ochrany.
- (149) Na základě výročního společného přezkumu Komise připraví veřejnou zprávu, kterou předloží Evropskému parlamentu a Radě.

7. POZASTAVENÍ ROZHODNUTÍ O ODPOVÍDAJÍCÍ ÚROVNI OCHRANY

- (150) Pokud Komise na základě kontrol nebo jakýchkoli jiných dostupných informací dojde k závěru, že úroveň ochrany poskytované štítem na ochranu soukromí již nelze považovat za v zásadě rovnocennou ochraně poskytované v Unii, nebo pokud existují jasné známky toho, že účinné dodržování zásad již nelze ve Spojených státech zajistit, nebo že opatření orgánů veřejné moci USA odpovědných za národní bezpečnost nebo prevenci, vyšetřování, odhalování či stíhání trestných činů nezajišťují odpovídající úroveň ochrany, informuje o tom Ministerstvo obchodu a požádá, aby byla přijata odpovídající opatření za účelem urychleného vyřešení jakéhokoli možného nedodržení zásad ve stanovené přiměřené lhůtě. Pokud po uplynutí této stanovené lhůty orgány USA uspokojivě neprokáží, že štít EU–USA na ochranu soukromí nadále zaručuje účinné dodržování zásad a odpovídající úroveň ochrany, zahájí Komise postup vedoucí k částečnému nebo úplnému pozastavení nebo zrušení tohoto rozhodnutí ⁽²⁰⁷⁾. Komise může také navrhnout změnu tohoto rozhodnutí, například omezením působnosti zjištění o odpovídající úrovni ochrany jen na přenosy údajů podléhající dodatečným podmínkám.
- (151) Komise zahájí postup vedoucí k pozastavení nebo zrušení zejména v případech:
- a) kdy jsou známky toho, že orgány USA nedodržují prohlášení a závazky obsažené v dokumentech, které tvoří přílohu tohoto rozhodnutí, včetně těch, které se týkají podmínek a omezení přístupu orgánů veřejné moci USA za účelem prosazení práva, národní bezpečnosti a jiného veřejného zájmu k údajům předávaným v rámci štítu na ochranu soukromí;
 - b) kdy stížnosti subjektů údajů z EU jsou fakticky neřešeny; v tomto případě Komise vezme v úvahu všechny okolnosti, které mají dopad na to, zda subjekty údajů z EU mohou uplatnit svá práva, včetně zejména dobrovolného závazku autocertifikovaných společností z USA spolupracovat s orgány pro ochranu údajů a řídit se jejich doporučeními; nebo
 - c) kdy ombudsman ve věcech štítu na ochranu soukromí včas náležitě neodpovídá na žádosti subjektů údajů z EU.
- (152) Komise také zváží zahájení postupu vedoucího ke změně, pozastavení nebo zrušení tohoto rozhodnutí, pokud v souvislosti s výročním společným přezkumem fungování štítu EU–USA na ochranu soukromí nebo jinak Ministerstvo obchodu či jiná ministerstva či agentury, které se účastní provádění štítu na ochranu soukromí, nebo ve věcech souvisejících s národní bezpečností zástupci zpravodajské komunity USA nebo ombudsman neposkytnou informace nebo objasnění nezbytná k posouzení dodržování zásad, k účinnosti postupů vyřizování

⁽²⁰⁷⁾ Ke dni použitelnosti obecného nařízení o ochraně údajů využije Komise svoji pravomoc přijmout v naléhavých a řádně odůvodněných případech prováděcí akt o pozastavení tohoto rozhodnutí, který bude použitelný okamžitě bez předchozího předložení příslušnému výboru v rámci postupu projednávání ve výboru a zůstane v platnosti po dobu nepřesahující šest měsíců.

stížností nebo ke snížení požadované úrovně ochrany v důsledku kroků národních zpravodajských orgánů USA, zejména v důsledku sběru osobních údajů nebo přístupu k nim, které nejsou omezeny na rozsah striktně nezbytný a přiměřený. V tomto směru Komise vezme v potaz míru, do jaké lze relevantní informace získat z jiných zdrojů, včetně zpráv a hlášení autocertifikovaných společností z USA podle zákona *USA FREEDOM Act*.

- (153) Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená podle článku 29 směrnice 95/46/ES vydala stanovisko k odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí ⁽²⁰⁸⁾, k němuž bylo přihlédnuto při přípravě tohoto rozhodnutí.
- (154) Evropský parlament přijal usnesení o transatlantickém toku údajů ⁽²⁰⁹⁾.
- (155) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem výboru zřízeného podle čl. 31 odst. 1 směrnice 95/46/ES,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

1. Pro účely čl. 25 odst. 2 směrnice 95/46/ES Spojené státy zajišťují odpovídající úroveň ochrany osobních údajů předávaných z Unie organizacím ve Spojených státech v rámci štítu EU–USA na ochranu soukromí.
2. Štít EU–USA na ochranu soukromí sestává ze zásad vydaných Ministerstvem obchodu dne 7. července 2016, které jsou obsaženy v příloze II, a oficiálních prohlášení a závazků, které jsou obsaženy v přílohách I a III až VII.
3. Pro účely odstavce 1 jsou osobní údaje předávány v rámci štítu EU–USA na ochranu soukromí, jsou-li předávány z Unie organizacím ve Spojených státech uvedeným na „seznamu organizací štítu na ochranu soukromí“, který vede a zpřístupňuje Ministerstvo obchodu USA v souladu s částí I a III zásad uvedených v příloze II.

Článek 2

Toto rozhodnutí nemá vliv na uplatňování jiných ustanovení směrnice 95/46/ES než čl. 25 odst. 1, která se týkají zpracování osobních údajů uvnitř členských států, a zejména článku 4 uvedené směrnice.

Článek 3

Pokud příslušné orgány v členských státech uplatní pravomoc podle čl. 28 odst. 3 směrnice 95/46/ES vedoucí k dočasnému nebo trvalému zákazu toku údajů do organizace ve Spojených státech, která je uvedena na seznamu organizací štítu na ochranu soukromí, v souladu s částí I a III zásad uvedených v příloze II za účelem ochrany fyzických osob s ohledem na zpracování jejich osobních údajů, oznámí dotčený členský stát tuto skutečnost bezodkladně Komisi.

Článek 4

1. Komise bude průběžně monitorovat fungování štítu EU–USA na ochranu soukromí za účelem posouzení, zda Spojené státy nadále zajišťují odpovídající úroveň ochrany osobních údajů předávaných v rámci tohoto štítu z Unie organizacím ve Spojených státech.

⁽²⁰⁸⁾ Stanovisko 01/2016 k návrhu rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí, vydané dne 13. dubna 2016.

⁽²⁰⁹⁾ Usnesení Evropského parlamentu ze dne 26. května 2016 o transatlantickém toku údajů (2016/2727(RSP)).

2. Členské státy a Komise se vzájemně informují o případech, kdy se zdá, že vládní subjekty ve Spojených státech se zákonnou pravomocí prosazovat dodržování zásad uvedených v příloze II neposkytují účinné mechanismy odhalování a dohledu, díky kterým lze v praxi odhalovat a postihovat případy porušení zásad ochrany soukromí.

3. Členské státy a Komise se vzájemně informují o jakýchkoli známkách toho, že zásahy orgánů veřejné moci USA odpovědných za národní bezpečnost, prosazování práva nebo jiné veřejné zájmy do práva fyzických osob na ochranu jejich osobních údajů přesahují rámec toho, co je striktně nezbytné a/nebo že proti takovým zásahům není účinné právní ochrany.

4. Během jednoho roku ode dne oznámení tohoto rozhodnutí členskými státy a poté jednou za rok Komise vyhodnotí zjištění v čl. 1 odst. 1 na základě veškerých dostupných informací, včetně informací získaných v rámci výročního společného přezkumu podle přílohy I, II a VI.

5. Komise nahlásí jakkoli relevantní zjištění výboru zřízenému podle článku 31 směrnice 95/46/ES.

6. Komise předloží návrh opatření v souladu s postupem uvedeným v čl. 31 odst. 2 směrnice 95/46/ES za účelem pozastavení, změny nebo zrušení tohoto rozhodnutí nebo omezení oblasti působnosti mimo jiné tehdy, jsou-li známky:

- toho, že orgány veřejné moci USA nedodržují prohlášení a závazky obsažené v dokumentech, které tvoří přílohu tohoto rozhodnutí, včetně těch, které se týkají podmínek a omezení přístupu orgánů veřejné moci USA za účelem prosazení práva, národní bezpečnosti a jiného veřejného zájmu k údajům předávaným v rámci štítu na ochranu soukromí;
- toho, že stížnosti subjektů údajů z EU nejsou na systematickém základě fakticky řešeny; nebo
- toho, že ombudsman ve věcech štítu na ochranu soukromí na systematickém základě neposkytuje příslušnou odpověď na žádosti subjektů údajů z EU, jak je požadováno v oddíle 4 písm. e) přílohy III.

Komise takový návrh opatření předloží v i případě, kdy nedostatečná spolupráce subjektů účastnících se zajišťování fungování štítu EU–USA na ochranu soukromí ve Spojených státech brání Komisi v určení, zda je dotčeno zjištění podle čl. 1 odst. 1.

Článek 5

Členské státy přijmou opatření nezbytná pro dosažení souladu s tímto rozhodnutím.

Článek 6

Toto rozhodnutí je určeno členskými státy.

V Bruselu dne 12. července 2016.

Za Komisi
Věra JOUROVÁ
členka Komise

PŘÍLOHA I

Dopis ministryně obchodu Spojených států Penny Pritzkerové

7. července 2016

Věra Jourová
Komisařka pro spravedlnost, spotřebitele a rovnost žen a mužů
Evropská komise
Rue de la Loi/Westraat 200
1049 Brusel
Belgie

Vážená paní komisařko Jourová,

jménem Spojených států amerických Vám s potěšením předávám soubor materiálů ke štítu EU-USA na ochranu soukromí, který je výsledkem dvou let plodných diskusí našich týmů. Tento soubor, spolu s ostatními materiály, které má Komise k dispozici z veřejných zdrojů, představuje velmi důkladné podklady k novému závěru Evropské komise ve věci odpovídající úrovně ochrany ⁽¹⁾.

Oba týmy by měly být na zlepšení rámce hrdé. Štít na ochranu soukromí vychází ze zásad, na jejichž výrazné podpoře panuje shoda na obou stranách Atlantiku, a nyní jsme jejich působnost ještě posílili. Díky naší spolupráci máme skutečnou příležitost zlepšit ochranu soukromí ve světě.

Soubor materiálů ke štítu na ochranu soukromí obsahuje zásady štítu na ochranu soukromí, spolu s dopisem odboru pro mezinárodní obchod (*International Trade Administration*, ITA) ministerstva obchodu (příloha 1), který program spravuje; dopis popisuje závazky, jež naše ministerstvo přijalo s cílem zajistit účinné fungování štítu. Součástí souboru materiálů je také příloha 2, která obsahuje další závazky ministerstva obchodu, jež se týkají nového rozhodčího modelu, který bude v rámci štítu na ochranu soukromí k dispozici.

Narádila jsem svým zaměstnancům, aby věnovali veškeré nezbytné prostředky na rychlé provedení rámce štítu na ochranu soukromí v plném rozsahu a na zajištění včasného splnění závazků uvedených v přílohách 1 a 2.

Soubor materiálů ke štítu na ochranu soukromí také obsahuje další dokumenty od dalších agentur Spojených států, a to:

- dopis Federální obchodní komise (*Federal Trade Commission*, dále též FTC), který popisuje její prosazování štítu na ochranu soukromí,
- dopis ministerstva dopravy, který popisuje jeho prosazování štítu na ochranu soukromí,
- dva dopisy Úřadu ředitele národních zpravodajských služeb (*Office of the Director of National Intelligence*, ODNI), který se týká ochranných opatření a omezení platných pro vnitrostátní bezpečnostní orgány Spojených států,
- dopis ministerstva zahraničí a průvodní memorandum, které popisují závazek ministerstva zahraničí ustavit nového ombudsmana ve věcech štítu na ochranu soukromí za účelem podávání dotazů k signálovým zpravodajským postupům Spojených států, a
- dopis ministerstva spravedlnosti, který se týká ochranných opatření a omezení v souvislosti s přístupem vlády Spojených států k osobním údajům pro účely prosazování práva a veřejného zájmu.

Ujišťuji Vás, že Spojené státy berou tyto závazky vážně.

⁽¹⁾ Za předpokladu, že rozhodnutí Komise o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí bude platit pro Island, Lichtenštejnsko a Norsko, bude se soubor materiálů ke štítu na ochranu soukromí vztahovat jak na Evropskou unii, tak na tyto tři země.

Do 30 dnů od konečného schválení rozhodnutí o odpovídající úrovni ochrany bude soubor materiálů ke štítu na ochranu soukromí předán ke zveřejnění ve věstníku *Federal Register*.

Těšíme se na spolupráci při provádění štítu na ochranu soukromí a na další fázi tohoto procesu.

S pozdravem
Penny Pritzker

Příloha 1

Dopis úřadujícího tajemníka ministra pro mezinárodní obchod Kena Hyatta

Vážená paní Věra Jourová
Komisařka pro spravedlnost, spotřebitele a rovnost žen a mužů
Evropská komise
Rue de la Loi/Weststraat 200
1049 Brusel
Belgie

Vážená paní komisařko Jourová,

jménem odboru pro mezinárodní obchod bych Vám rád popsal lepší ochranu osobních údajů poskytovanou rámcem štítu EU-USA na ochranu soukromí (dále též „štít na ochranu soukromí“ nebo „rámec“) a závazky, které ministerstvo obchodu (dále též „ministerstvo“) přijalo s cílem zajistit účinné fungování štítu. Dokončení této historické dohody je významným počinem pro ochranu soukromí a pro obchod na obou stranách Atlantiku. Díky této dohodě si mohou být obyvatelé EU jisti, že jejich údaje budou chráněny a že budou mít právní prostředky k řešení případných obav. Dohoda nabízí jistotu, která přispěje k růstu transatlantické ekonomiky, neboť díky ní budou tisíce evropských a amerických podniků moci pokračovat v přeshraničních investicích a podnikání. Štít na ochranu soukromí je výsledkem více než dvouleté tvrdé práce a spolupráce s Vámi, našimi kolegy v Evropské komisi (dále též „Komise“). Těšíme se na další spolupráci s Komisí ve snaze zajistit fungování štítu na ochranu soukromí tak, jak bylo zamýšleno.

S Komisí jsme pracovali na štítu na ochranu soukromí, který organizacím usazeným ve Spojených státech umožní splnit požadavky na odpovídající úroveň ochrany údajů podle práva EU. Nový rámec přinese občanům i podnikům značné výhody. Zaprvé stanoví významný soubor opatření na ochranu osobních údajů fyzických osob z EU. Od zúčastněných organizací USA požaduje, aby vypracovaly vyhovující politiku ochrany soukromí, veřejně se zavázaly dodržovat zásady štítu na ochranu soukromí, aby byl jejich závazek právně vymahatelný podle práva Spojených států, každý rok u ministerstva recifikovaly dodržování uvedených zásad, zajistily fyzickým osobám z EU bezplatné nezávislé řešení sporů a podrobily se pravomoci Federální obchodní komise Spojených států (FTC), ministerstva dopravy (dále též „MD“) nebo jiného donucovacího orgánu. Zadruhé, štít na ochranu údajů umožní tisícům podniků ve Spojených státech a dceřiným společnostem evropských firem ve Spojených státech přijímat osobní údaje z Evropské unie, a usnadní tak toky údajů, které podporují transatlantický obchod. Transatlantický hospodářský vztah je již největší na světě, představuje polovinu celosvětové hospodářské produkce a obchod se zbožím a službami o objemu téměř jeden bilion amerických dolarů, a podporuje tak miliony pracovních míst na obou stranách Atlantiku. Společnosti, které se opírají o transatlantické toky údajů, pocházejí ze všech výrobních odvětví a jsou mezi nimi některé z 500 nejvýznamnějších firem podle časopisu Fortune i mnoho malých a středních podniků (dále též „MSP“). Transatlantické toky údajů umožňují organizacím USA zpracovávat údaje potřebné k nabízení zboží, služeb a pracovních příležitostí Evropanům. Štít na ochranu soukromí podporuje společné zásady ochrany soukromí, překlenuje rozdíly v našich právních přístupech a zároveň prosazuje obchodní a hospodářské cíle Evropy i Spojených států.

I když rozhodnutí společnosti autocertifikovat se podle tohoto nového rámce bude dobrovolné, jakmile se k dodržování štítu na ochranu soukromí veřejně zaváže, je její závazek právně vymahatelný podle práva Spojených států Federální obchodní komisí nebo ministerstvem dopravy v závislosti na tom, který orgán má nad organizací štítu na ochranu soukromí pravomoc.

Zlepšení podle zásad štítu na ochranu soukromí

Výsledný štít na ochranu soukromí posiluje ochranu soukromí, neboť:

- zásada oznamovací povinnosti požaduje, aby byly fyzickým osobám poskytovány další informace, včetně prohlášení o přináležitosti organizace ke štítu na ochranu soukromí, prohlášení o právu fyzických osob na přístup k osobním údajům a určení příslušného nezávislého orgánu zabývajícího se řešením sporů,
- posiluje ochranu osobních údajů předávaných organizací štítu na ochranu soukromí třetí straně, která je správcem, neboť požaduje, aby strany uzavřely smlouvu, jež stanoví, že tyto údaje lze zpracovávat pouze k omezeným a stanoveným účelům v souladu se souhlasem poskytnutým dotyčnou fyzickou osobou a že příjemce poskytne tutéž úroveň ochrany jako tyto zásady,

- posiluje ochranu osobních údajů předávaných organizací štítu na ochranu soukromí třetí straně, která je jí pověřená a jedná podle jejích pokynů, neboť mj. požaduje, aby organizace štítu na ochranu soukromí přijala přiměřené a vhodné kroky, jež zajistí, aby osoba, která je jí pověřená a jedná podle jejích pokynů, účinně zpracovávala předané osobní informace v souladu s povinnostmi organizace podle těchto zásad, na žádost přijala přiměřené a vhodné kroky k zastavení a nápravě neoprávněného zpracování a na požádání poskytla ministerstvu shrnutí nebo reprezentativní kopii příslušných ustanovení smlouvy s uvedenou osobou, jež je jí pověřená a jedná podle jejích pokynů, o ochraně soukromí,
- stanoví, že organizace štítu na ochranu soukromí je odpovědná za zpracování osobních informací, které obdrží v rámci štítu na ochranu soukromí a následně předá třetí straně, jež je jí pověřená a jedná podle jejích pokynů, a že organizace štítu na ochranu soukromí zůstane odpovědná podle těchto zásad, jestliže osoba, která je jí pověřená a jedná podle jejích pokynů, zpracuje tyto osobní informace způsobem, jenž není v souladu se zásadami, pokud organizace neprokáže, že za okolnost, která vedla ke vzniku škody, není odpovědná,
- objasňuje, že organizace štítu na ochranu soukromí musí osobní informace omezit na informace, které jsou s ohledem na účely zpracování podstatné,
- požaduje, aby organizace u ministerstva každý rok certifikovala svůj závazek používat tyto zásady na informace, které obdržela, když náležela ke štítu na ochranu soukromí, jestliže štít opustí a rozhodne se si tyto údaje ponechat,
- požaduje, aby dotyčné fyzické osobě byly bezplatně poskytnuty nezávislé odvolací mechanismy,
- požaduje, aby organizace a jejich vybrané nezávislé odvolací orgány rychle reagovaly na dotazy a žádosti ministerstva o informace o štítu na ochranu soukromí,
- požaduje, aby organizace rychle reagovaly na stížnosti na dodržování zásad postoupené prostřednictvím ministerstva orgány členských států EU, a
- požaduje, aby organizace štítu na ochranu soukromí zveřejnila veškeré příslušné části případné zprávy o dodržování předpisů nebo hodnotící zprávy předložené Federální obchodní komisi, které se týkají štítu na ochranu soukromí, stane-li se předmětem usnesení FTC či soudu z důvodu nedodržení předpisů.

Správa programu štítu na ochranu soukromí a dohled nad ním ze strany ministerstva obchodu

Ministerstvo potvrzuje svůj závazek vést a poskytnout veřejnosti oficiální seznam organizací USA, které u ministerstva autocertifikovaly svůj závazek dodržovat tyto zásady (dále též „seznam organizací štítu na ochranu soukromí“). Seznam organizací štítu na ochranu soukromí bude aktuální, neboť ministerstvo z něj bude organizace odstraňovat, pokud dobrovolně vystoupí, neabsolvuji každoroční recertifikaci v souladu s postupy ministerstva nebo bude shledáno, že soustavně nedodržují zásady. Ministerstvo také povede a poskytne veřejnosti oficiální rejstřík organizací USA, které se dříve u ministerstva autocertifikovaly, ale byly ze seznamu organizací štítu na ochranu soukromí odstraněny, včetně organizací, jež byly odstraněny z důvodu soustavného nedodržování zásad. Ministerstvo označí důvod odstranění každé organizace.

Kromě toho se ministerstvo zavazuje posílit správu štítu na ochranu soukromí a dohled nad ním. Konkrétně ministerstvo:

Poskytne další informace na internetových stránkách štítu na ochranu soukromí

- povede seznam organizací štítu na ochranu soukromí i rejstřík organizací, které dříve autocertifikovaly dodržování zásad, ale již nepožívají výhod štítu,
- na viditelném místě zveřejní vysvětlení, které objasní, že všechny organizace odstraněné ze seznamu organizací štítu na ochranu soukromí již nepožívají výhod štítu, ale přesto musí na osobní informace, jež obdržely, když ke štítu náležely, používat tyto zásady, dokud si tyto informace ponechají, a
- poskytne odkaz na seznam věcí FTC, které se týkají štítu na ochranu soukromí, vedený na internetových stránkách FTC.

Bude ověřovat požadavky na autocertifikaci

- než dokončí autocertifikaci organizace (nebo každoroční recertifikaci) a umístí organizaci na seznam organizací štítu na ochranu soukromí, ověří, že organizace:
 - poskytla své požadované kontaktní údaje,
 - popsala svou činnost v souvislosti s osobními údaji přijímanými z EU,
 - uvedla, jakých osobních informací se její autocertifikace týká,
- má-li organizace veřejné internetové stránky, poskytla webovou adresu, na které je dostupná politika ochrany soukromí, a že je politika ochrany soukromí na poskytnuté webové adrese dostupná, nebo nemá-li organizace veřejné internetové stránky, že uvedla údaj o tom, kde je tato politika přístupná k nahlédnutí veřejnosti,
- zařadila do politiky ochrany soukromí prohlášení, že dodržuje zásady štítu na ochranu soukromí, a je-li politika ochrany soukromí dostupná on-line, hypertextový odkaz na internetové stránky ministerstva věnované štítu na ochranu soukromí,
- 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 štítu na ochranu soukromí či v jejich budoucí příloze),
- jestliže se organizace rozhodla vyhovět požadavkům v písm. a) bodech i) a iii) zásady odvolání, prosazování a odpovědnosti tak, že se zavázala spolupracovat s příslušnými orgány pro ochranu údajů z EU, dala najevo svůj záměr spolupracovat s orgány pro ochranu údajů při vyšetřování a řešení stížností předložených v rámci štítu na ochranu soukromí, zejména reagovat na jejich dotazy, pokud subjekty údajů EU podají své stížnosti přímo ke svým vnitrostátním orgánům pro ochranu údajů,
- označila případné programy na ochranu soukromí, jichž se organizace účastní,
- označila způsob ověřování toho, zda je zajištěno dodržování zásad (např. vnitřní, prostřednictvím třetí strany),
- ve své autocertifikaci i ve své politice ochrany soukromí označila nezávislý odvolací orgán pro vyšetřování a řešení stížností,
- je-li příslušná politika ochrany soukromí dostupná on-line, organizace v nich uvedla hypertextový odkaz na internetové stránky nezávislého odvolacího orgánu pro vyšetřování nevyřešených stížností nebo jeho formulář pro podávání stížností, a
- uvedla-li organizace, že má v úmyslu přijímat údaje o lidských zdrojích předávané z EU pro využití v rámci zaměstnaneckých vztahů, deklarovala svůj závazek spolupracovat s orgány pro ochranu údajů a vyhovět jim při řešení stížností, které se týkají jejich aktivit v souvislosti s těmito údaji, poskytla ministerstvu kopii své politiky ochrany soukromí v souvislosti s lidskými zdroji a uvedla, kde se s uvedenou politikou mohou seznámit dotčení zaměstnanci,
- bude pracovat s nezávislými odvolacími orgány na ověření skutečnosti, že se organizace opravdu zaevidovaly u příslušného orgánu uvedeného v jejich autocertifikaci, je-li tato evidence vyžadována.

Prohloubí úsilí o sledování organizací, které byly odstraněny ze seznamu organizací štítu na ochranu soukromí

- uvědomí organizace odstraněné ze seznamu organizací štítu na ochranu soukromí z důvodu „soustavného nedodržování zásad“, že nemají nárok ponechat si informace shromážděné v rámci štítu, a
- bude organizacím, jejichž autocertifikace pozbudou platnosti nebo jež dobrovolně vystoupí ze štítu na ochranu soukromí, rozesílat dotazníky s cílem ověřit, zda organizace osobní informace, které obdržela, když náležela ke štítu, vrátí, vymaže, či na ně bude dále používat tyto zásady, a jestliže si osobní informace ponechá, ověřit, kdo v organizaci bude sloužit jako stálá kontaktní osoba pro otázky spojené se štítem na ochranu soukromí.

Bude hledat a řešit nepravdivá tvrzení o účasti

- bude přezkoumávat opatření na ochranu soukromí prováděná organizacemi, které se dříve účastnily programu štítu na ochranu soukromí, ale byly odstraněny ze seznamu organizací štítu na ochranu soukromí, s cílem nalézt případná nepravdivá tvrzení o přináležitosti ke štítu,
- průběžně, jestliže organizace: a) odstoupí od účasti na štítu na ochranu soukromí, b) neregistruje dodržování zásad nebo c) bude ze štítu na ochranu soukromí vyloučena zejména z důvodu „soustavného nedodržování zásad“, bude z moci úřední ověřovat, že organizace z příslušné zveřejněné politiky ochrany soukromí odstranila veškeré odkazy na štít na ochranu soukromí, ze kterých vyplývá, že se organizace štítu nadále aktivně účastní a má nárok na jeho výhody. Zjistí-li ministerstvo, že tyto odkazy nebyly odstraněny, upozorní organizaci, že záležitost popřípadě postoupí příslušnému orgánu za účelem potenciálního prosazení práva, bude-li organizace nadále tvrdit, že je certifikovaná v souvislosti se štítem na ochranu soukromí. Jestliže organizace neodstraní odkazy ani neautocertifikuje dodržování štítu na ochranu soukromí, ministerstvo záležitost z moci úřední postoupí FTC, MD nebo jinému příslušnému donucovacímu orgánu, popřípadě přijme opatření za účelem prosazení práva v souvislosti s certifikační ochrannou známkou štítu na ochranu soukromí,
- bude vyvíjet další úsilí o nalezení nepravdivých tvrzení o přináležitosti ke štítu na ochranu soukromí a nevhodného užití certifikační ochranné známky štítu, mj. prohledáváním internetu s cílem zjistit, kde jsou vystavena vyobrazení certifikační ochranné známky štítu na ochranu soukromí, a nalézt odkazy na štít v opatřeních na ochranu soukromí prováděných organizacemi,
- bude neprodleně řešit veškeré problémy, které zjistíme při úředním sledování nepravdivých tvrzení o účasti a zneužití certifikační ochranné známky, včetně varování organizací, jež klamou o své přináležitosti ke štítu na ochranu soukromí, jak je popsáno výše,
- přijme jiné vhodné nápravné opatření, včetně usilování o právní postih v pravomoci ministerstva a postoupení záležitosti FTC, MD nebo jinému příslušnému donucovacímu orgánu, a
- neprodleně přezkoumá a bude řešit stížnosti na nepravdivá tvrzení o účasti, které obdržíme.

Ministerstvo bude přezkoumávat opatření na ochranu soukromí prováděná organizacemi s cílem účinněji nalézat a řešit nepravdivá tvrzení o přináležitosti ke štítu na ochranu soukromí. Konkrétně bude ministerstvo přezkoumávat opatření na ochranu soukromí prováděná organizacemi, jejichž autocertifikace pozbyla platnosti, neboť neregistruovaly dodržování zásad. Ministerstvo bude tento typ přezkumu provádět s cílem ověřit, že tyto organizace z příslušné zveřejněné politiky ochrany soukromí odstranily veškeré odkazy, ze kterých vyplývá, že se štítu na ochranu soukromí dále aktivně účastní. Na základě těchto přezkumů označíme organizace, které tyto odkazy neodstranily, a zašleme jim dopis kanceláře generálního rady ministerstva, jenž je upozorní na potenciální opatření za účelem prosazení práva, nebudou-li odkazy odstraněny. Ministerstvo přijme návazná opatření s cílem zajistit, aby organizace odstranily nevhodné odkazy nebo recertifikovaly dodržování zásad. Kromě toho bude ministerstvo usilovat o nalezení nepravdivých tvrzení o přináležitosti ke štítu na ochranu soukromí ze strany organizací, které se programu štítu na ochranu soukromí nikdy neúčastnily, a přijme v souvislosti s těmito organizacemi podobné nápravné opatření.

Bude provádět pravidelné úřední přezkumy dodržování zásad a hodnocení programu

- bude průběžně sledovat účinné dodržování zásad, mj. zasíláním podrobných dotazníků zúčastněným organizacím s cílem označit problémy, které mohou vyžadovat další návazná opatření. Tyto přezkumy dodržování zásad se budou konat zejména tehdy, jestliže: a) ministerstvo obdrží konkrétní vážně míněné stížnosti na dodržování zásad organizací, b) organizace uspokojivě nezareaguje na žádosti ministerstva o informace v souvislosti se štítem na ochranu soukromí nebo c) existují věrohodné důkazy, že organizace nedodržuje své závazky v rámci štítu na ochranu soukromí. Ministerstvo bude tyto přezkumy dodržování zásad popřípadě konzultovat s příslušnými orgány pro ochranu údajů a
- bude pravidelně hodnotit správu programu štítu na ochranu soukromí a dohled nad ním s cílem zajistit, aby sledování dokázalo řešit nové problémy, když nastanou.

Ministerstvo navýšilo prostředky, které budou věnovány na správu programu štítu na ochranu soukromí a na dohled nad ním, včetně zdvojnásobení počtu zaměstnanců odpovědných za správu programu a dohled nad ním. Na toto úsilí nadále věnujeme vhodné prostředky, abychom zajistili účinné sledování a správu programu.

Uzpůsobí internetové stránky štítu na ochranu soukromí cílovým adresátům

Ministerstvo uzpůsobí internetové stránky štítu na ochranu soukromí tak, aby se zaměřovaly na tři cílové skupiny adresátů: fyzické osoby z EU, podniky z EU a podniky ze Spojených států. Zařazení materiálu přímo zaměřeného na fyzické osoby a podniky z EU v mnoha ohledech pomůže ke transparentnosti. Pokud jde o fyzické osoby z EU, materiál zřetelně vysvětlí: 1) práva, která štít na ochranu soukromí poskytuje fyzickým osobám z EU, 2) odvolací mechanismy dostupné fyzickým osobám z EU, jsou-li přesvědčeny, že kterákoli organizace porušila svůj závazek dodržovat zásady, a 3) jak nalézt informace, jež se týkají autocertifikace organizace v souvislosti se štítem na ochranu soukromí. Pokud jde o podniky z EU, materiál usnadní ověřování: 1) toho, zda organizace požívá výhod štítu na ochranu soukromí, 2) typu informací, na které se vztahuje autocertifikace organizace v souvislosti se štítem na ochranu soukromí, 3) politiky ochrany soukromí, jež pro dotčené informace platí, a 4) metody, kterou organizace používá k ověřování toho, že dodržuje zásady.

Prohloubí spolupráci s orgány pro ochranu údajů

S cílem rozšířit příležitosti spolupráce s orgány pro ochranu údajů ustaví ministerstvo specializovanou kontaktní osobu, která bude působit jako prostředník pro orgány pro ochranu údajů. Bude-li kterýkoli orgán pro ochranu údajů přesvědčen, že kterákoli organizace nedodržuje zásady, a to i na základě stížnosti fyzické osoby z EU, může se orgán pro ochranu údajů obrátit na specializovanou kontaktní osobu na ministerstvu a požádat ji o postoupení organizace k dalšímu přezkumu. Kontaktní osoba bude také přijímat případy organizací, které nepravdivě tvrdí, že náleží ke štítu na ochranu soukromí, ačkoli nikdy neautocertifikovaly dodržování zásad. Kontaktní osoba bude pomáhat orgánům pro ochranu údajů, které hledají informace o autocertifikaci nebo předchozí účasti konkrétní organizace v programu, a bude odpovídat na dotazy orgánů pro ochranu údajů ohledně provádění zvláštních požadavků štítu na ochranu soukromí. Zadrhé ministerstvo poskytne orgánům pro ochranu údajů materiál o štítu na ochranu soukromí, který budou moci zveřejnit na svých vlastních internetových stránkách za účelem větší transparentnosti vůči fyzickým osobám a podnikům z EU. Větší povědomí o štítu na ochranu soukromí a právech a povinnostech, které na jeho základě vznikají, by mělo usnadnit označování problémů, jakmile vyvstanou, aby je bylo možné vhodně řešit.

Usnadní řešení stížností na nedodržování zásad

Ministerstvo bude prostřednictvím specializované kontaktní osoby přijímat stížnosti postoupené orgány pro ochranu údajů, že organizace štítu na ochranu soukromí nedodržují zásady. Ministerstvo vynaloží maximální úsilí na hladké řešení stížnosti s organizací štítu na ochranu soukromí. Do 90 dnů od obdržení stížnosti poskytne ministerstvo orgánu pro ochranu údajů aktuální informace. S cílem usnadnit podávání těchto stížností vytvoří ministerstvo pro orgány pro ochranu údajů standardní formulář pro podávání stížností specializované kontaktní osobě na ministerstvu. Specializovaná kontaktní osoba bude sledovat všechny případy postoupené orgány pro ochranu údajů ministerstvu a ministerstvo v rámci každoročního přezkumu popsaného níže poskytne zprávu, která souhrnně analyzuje stížnosti, jež každý rok obdrží.

Po konzultaci s Komisí zavede rozhodčí řízení a vybere rozhodce

Ministerstvo splní své závazky podle přílohy I a po dosažení dohody zveřejní postupy.

Společný přezkum fungování štítu na ochranu soukromí

Ministerstvo obchodu, FTC a popřípadě další agentury budou každoročně pořádat zasedání s Komisí, zúčastněnými orgány pro ochranu údajů a příslušnými zástupci pracovní skupiny zřízené podle článku 29, kde ministerstvo poskytne aktuální informace o programu štítu na ochranu soukromí. Součástí každoročních zasedání bude diskuse o aktuálních problémech spojených s fungováním štítu na ochranu soukromí, jeho prováděním, dohledem nad ním a jeho prosazováním, včetně případů postoupených ministerstvu orgány pro ochranu údajů, výsledků úředních přezkumů dodržování zásad a případně diskuse o příslušných změnách právních předpisů. Součástí prvního každoročního přezkumu a případných následných přezkumů bude dialog na další témata, jako je oblast automatizovaného rozhodování, včetně aspektů, které se týkají podobnosti a rozdílů v přístupech v EU a ve Spojených státech.

Aktualizace zákonů

Ministerstvo vynaloží přiměřené úsilí na informování Komise o významném vývoji práva ve Spojených státech, bude-li souviset se štítem na ochranu soukromí v oblasti ochrany osobních údajů a omezení a ochranných opatření platných pro přístup k osobním údajům ze strany orgánů Spojených států a jejich následné využívání.

Výjimka týkající se národní bezpečnosti

V souvislosti s omezeními dodržování zásad štítu na ochranu soukromí pro účely národní bezpečnosti zaslal generální rada Úřadu ředitele národních zpravodajských služeb Robert Litt dva dopisy určené Justinu Antonipillaiovi a Tedu Deanovi z ministerstva obchodu a tyto dva dopisy Vám byly postoupeny. Tyto dva dopisy se obšírně zabývají mj. zásadami, ochrannými opatřeními a omezeními, která se vztahují na signálové zpravodajské činnosti prováděné Spojenými státy. Kromě toho tyto dopisy popisují transparentnost, s níž se k těmto věcem staví zpravodajská komunita. Jelikož Komise hodnotí rámec štítu na ochranu soukromí, informace v těchto dopisech ji ujišťují, že může dospět k závěru, že štít na ochranu soukromí bude fungovat správně v souladu se svými zásadami. Chápeme, že informace zveřejněné zpravodajskou komunitou můžete spolu s dalšími informacemi použít v budoucnu jako podklad každoročního přezkumu rámce štítu na ochranu soukromí.

Na základě zásad štítu na ochranu soukromí a průvodních dopisů a materiálů, včetně závazků ministerstva v souvislosti se správou rámce štítu na ochranu soukromí a s dohledem nad ním, předpokládáme, že Komise rozhodne, že rámec štítu EU-USA na ochranu soukromí poskytuje pro účely práva EU odpovídající úroveň ochrany, a že organizacím, které ke štítu na ochranu soukromí náleží, budou údaje z Evropské unie dále předávány.

S pozdravem

Ken Hyatt

Příloha 2

Rozhodčí model

PŘÍLOHA I

Tato příloha I stanoví podmínky, za kterých jsou organizace štítu na ochranu soukromí 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 štít EU-USA na ochranu soukromí. 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 v rámci štítu na ochranu soukromí.

A. Oblast působnosti

V rozhodčím řízení, které mají fyzické osoby k dispozici, se u zbytkových nároků rozhodne, zda organizace štítu na ochranu soukromí 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⁽¹⁾ nebo s tvrzeními, která se týkají odpovídající úrovně ochrany poskytované štítem na ochranu soukromí.

B. Dostupné opravné prostředky

V rámci této možnosti rozhodčího řízení má poradní panel štítu na ochranu soukromí (*Privacy Shield 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 dotýčné fyzické osoby) nezbytné k nápravě porušení těchto zásad pouze v souvislosti s dotčenou fyzickou osobou. To jsou jediné pravomoci rozhodčího panelu v souvislosti s opravnými prostředky. Při rozhodování o opravných prostředcích musí vzít rozhodčí panel v úvahu jiné opravné prostředky, které již uložily jiné orgány v rámci štítu na ochranu soukromí. K dispozici není náhrada škody, nákladů, poplatků ani jiné opravné prostředky. Každá strana nese své vlastní palmáře.

C. Požadavky před rozhodčím řízením

Fyzická osoba, která se rozhodne využít této možnosti rozhodčího řízení, musí před podáním žaloby učinit tyto kroky: 1) předložit údajné porušení přímo organizaci a poskytnout jí příležitost otázku vyřešit ve lhůtě stanovené v oddíle III bodě 11 písm. d) podbodě i) těchto zásad, 2) využít nezávislý bezplatný odvolací mechanismus podle těchto zásad a 3) předložit problém prostřednictvím svého orgánu pro ochranu údajů ministerstvu obchodu a poskytnout mu příležitost vynaložit maximální úsilí na bezplatné vyřešení otázky ve lhůtě stanovené v dopise odboru pro mezinárodní obchod ministerstva obchodu.

Této možnosti rozhodčího řízení se nelze dovolávat, jestliže totéž údajné porušení těchto zásad žalované fyzickou osobou 1) již bylo předmětem závazného rozhodčího řízení, 2) bylo předmětem pravomocného rozsudku vynesného v soudním sporu, jehož byla fyzická osoba účastníkem, nebo 3) již bylo stranami urovnáno. Kromě toho se této možnosti nelze dovolávat, jestliže orgán pro ochranu údajů z EU 1) má pravomoc podle oddílu III bodů 5 nebo 9 těchto zásad či 2) je oprávněn řešit údajné porušení přímo s organizací. Pravomoc orgánu pro ochranu 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 orgánu pro ochranu 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 v jiné podobě 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.

⁽¹⁾ Oddíl I bod 5 těchto zásad.

E. Přezkum a prosazování

Fyzické osoby a organizace štitu na ochranu soukromí se budou moci domáhat soudního přezkumu a výkonu rozhodčích nálezů podle práva Spojených států na základě federálního zákona o rozhodčím řízení (*Federal Arbitration Act*, FAA) ⁽¹⁾. Veškeré tyto věci musí být předloženy federálnímu okrskovému soudu, který je územně příslušný pro hlavní místo podnikání organizace štitu na ochranu soukromí.

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 FTC.

F. Rozhodčí panel

Strany vyberou rozhodce ze seznamu rozhodců popsaného níže.

V souladu s použitelným právem zpracuje Ministerstvo obchodu Spojených států a Evropská komise seznam alespoň 20 rozhodců vybraných na základě nezávislosti, profesní bezúhonnosti a know-how. V souvislosti s tímto procesem platí následující:

Rozhodci:

- 1) zůstanou na seznamu po dobu 3 let, nenastanou-li výjimečné nebo odůvodněné okolnosti, přičemž toto období lze prodloužit o další 3 roky;
- 2) nepodléhají žádným pokynům žádné ze stran, žádné organizace štitu na ochranu soukromí, Spojených států, EU, žádného členského státu EU ani žádného vládního orgánu, 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 soukromé právo Spojených států a mít know-how právních předpisů EU o ochraně údajů.

G. Postupy pro rozhodčí řízení

V souladu s použitelným právem se ministerstvo obchodu a Evropská komise do 6 měsíců od přijetí rozhodnutí o odpovídající úrovni ochrany dohodnou na přijetí stávajícího zavedeného souboru postupů pro rozhodčí řízení (například organizací AAA nebo JAMS), kterými se budou řízení u panelu štitu na ochranu soukromí řídit 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.

⁽¹⁾ Kapitola 2 zákona FAA stanoví, že „[r]ozhodčí dohoda nebo rozhodčí nález 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. No. 6997 („Newyorská úmluva“)].“ 9 U.S.C. § 202. Zákon FAA dále stanoví, že „[m]á se za to, že dohoda nebo nález 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 nález proti druhé straně rozhodčího řízení. Soud nález potvrdí, neshledá-li žádný z důvodů k odepření nebo odložení uznání či výkonu nálezu uvedený v dotyčné [Newyorské] úmluvě“. Tamtéž § 207. Kapitola 2 dále stanoví, že „[p]ůvodně 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]ísenné 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 nález potvrdí, a soud musí na základě toho tento příkaz vydat, nebude-li nález zrušen, upraven nebo opraven, jak předepisují § 10 a 11 [federálního zákona o rozhodčím řízení]“. Tamtéž § 9.

2. Budou vypracovány postupy, které zajistí, aby u téhož porušení žalovaného fyzickou osobou nebyly uplatněny duplicitní opravné prostředky nebo postupy.
3. Souběžně s rozhodcím řízením může konat FTC.
4. Těchto rozhodcích řízení se nesmí účastnit žádný zástupce Spojených států, EU, žádného členského státu EU ani žádného vládního orgánu, orgánu veřejné moci nebo donucovacího orgánu za předpokladu, že na žádost fyzické osoby z EU mohou orgány pro ochranu údajů z EU 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, 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 rozhodcím 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 rozhodcím řízením.
9. Rozhodčí řízení by měla skončit do 90 dnů od doručení oznámení žalované organizaci, nedohodnou-li se strany jinak.

H. Náklady

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

V závislosti na použitelném právu usnadní ministerstvo obchodu po konzultaci s Evropskou komisí zřízení fondu, do kterého budou organizace štítu na ochranu soukromí muset hradit roční příspěvek založený částečně na jejich velikosti, jenž pokryje 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 zprávy o jeho fungování. Při každoročním přezkumu ministerstvo obchodu a Evropská komise přezkoumají fungování fondu, včetně nutnosti upravit výši příspěvků nebo stropů, a posoudí mj. počet rozhodčích řízení a jejich náklady a načasování, přičemž vzájemně chápou, že organizace štítu na ochranu soukromí nebudou nadměrně finančně zatíženy. Na základě tohoto ustanovení ani z žádného fondu podle tohoto ustanovení se nehradí palmáře.

PŘÍLOHA II

ZÁSADY RÁMCE ŠTÍTU EU-USA NA OCHRANU SOUKROMÍ VYDANÉ MINISTERSTVEM OBCHODU
SPOJENÝCH STÁTŮ

I. PŘEHLED

1. Spojené státy a Evropská unie sice sledují stejný cíl, kterým je zvýšení ochrany soukromí, avšak Spojené státy přistupují k otázkám ochrany soukromí odlišně než Evropská unie. Spojené státy uplatňují odvětvový přístup, který je založen na kombinaci právních předpisů, nařízení a samoregulace. Vzhledem k uvedeným rozdílům a s cílem poskytnout organizacím ve Spojených státech spolehlivý mechanismus předávání osobních údajů do Spojených států z Evropské unie a zároveň zajistit, aby subjekty údajů EU nadále požívaly účinných ochranných opatření a ochrany, jak vyžadují evropské právní předpisy v souvislosti se zpracováním jejich osobních údajů, byly-li předány do zemí mimo EU, vydává ministerstvo obchodu v rámci své zákonné pravomoci pěstovat, podporovat a rozvíjet mezinárodní obchod tyto zásady štítu na ochranu soukromí, včetně doplňkových zásad (dále společně též „zásady“) (15 U.S.C. § 1512). Tyto zásady byly vypracovány na základě konzultací s Evropskou komisí, s představiteli průmyslu a s dalšími zúčastněnými stranami za účelem usnadnění obchodu mezi Spojenými státy a Evropskou unií. Jsou určeny výlučně organizacím ve Spojených státech, které získávají osobní údaje z Evropské unie, aby mohly splnit požadavky štítu na ochranu soukromí, a využít tak rozhodnutí Evropské komise o odpovídající úrovni ochrany⁽¹⁾. Těmito zásadami není dotčeno uplatňování vnitrostátních právních předpisů týkajících se zpracování osobních údajů v členských státech, jimiž se provádí směrnice 95/46/ES (dále též „směrnice“). Zásady také neomezuji povinnosti chránit soukromí, které jinak platí podle práva Spojených států.
2. Chce-li se organizace za účelem předávání osobních údajů z EU opírat o štít na ochranu soukromí, musí u ministerstva obchodu (nebo jeho zmocněnce) autocertifikovat dodržování těchto zásad. I když rozhodnutí organizací vstoupit do štítu na ochranu soukromí jsou zcela dobrovolná, je účinné dodržování těchto zásad povinné: organizace, které u ministerstva autocertifikují a veřejně deklarují svůj závazek dodržovat tyto zásady, je musí dodržovat v plném rozsahu. Chce-li organizace vstoupit do štítu na ochranu soukromí, musí a) podléhat pravomocem v oblasti vyšetřování a prosazování práva svěřeným Federální obchodní komisi (FTC), ministerstvu dopravy nebo jinému subjektu zřízenému zákonem, který účinně zajistí dodržování těchto zásad (*další subjekty Spojených států zřízené zákonem a uznávané EU mohou být v budoucnu zařazeny jako příloha*), b) veřejně deklarovat svůj závazek dodržovat tyto zásady, c) zveřejnit svá opatření na ochranu soukromí v souladu s těmito zásadami a d) provádět je v plném rozsahu. Nedodržování těchto zásad organizací je právně vymahatelné podle § 5 zákona o Federální obchodní komisi (*Federal Trade Commission Act*), který zakazuje nekalé nebo klamavé jednání v obchodě nebo související s obchodem (15 U.S.C. § 45(a)), či podle jiných právních nebo správních předpisů, jež toto jednání zakazují.
3. Ministerstvo obchodu povede a poskytne veřejnosti oficiální seznam organizací USA, které u ministerstva autocertifikovaly svůj závazek dodržovat zásady („seznam organizací štítu na ochranu soukromí“). Výhody štítu na ochranu soukromí jsou zajištěny od data, kdy ministerstvo umístí organizaci na seznam organizací štítu na ochranu soukromí. Ministerstvo organizaci ze seznamu organizací štítu na ochranu soukromí odstraní, jestliže organizace ze štítu dobrovolně vystoupí nebo u ministerstva neabsolvuje každoroční recertifikaci. Odstranění organizace ze seznamu organizací štítu na ochranu soukromí znamená, že organizace pro účely získávání osobních informací z EU již nemůže využívat rozhodnutí Evropské komise o odpovídající úrovni ochrany. Organizace musí na osobní informace, které obdržela, když se účastnila štítu na ochranu soukromí, nadále používat tyto zásady a každý rok ministerstvu potvrdit svůj závazek tak činit po celou dobu, kdy si tyto informace ponechá; v opačném případě musí organizace informace vrátit nebo vymazat či zajistit jejich „odpovídající“ ochranu jinými schválenými prostředky. Ministerstvo ze seznamu organizací štítu na ochranu soukromí také odstraní organizace, které tyto zásady soustavně nedodržují; tyto organizace nesplňují požadavky pro využívání výhod štítu na ochranu soukromí a musí osobní informace, jež v rámci štítu obdržely, vrátit nebo vymazat.
4. Ministerstvo také povede a poskytne veřejnosti oficiální rejstřík organizací USA, které se dříve u ministerstva autocertifikovaly, ale byly ze seznamu organizací štítu na ochranu soukromí odstraněny. Ministerstvo zřetelně upozorní, že tyto organizace nenáleží ke štítu na ochranu soukromí, že odstranění ze seznamu organizací štítu na ochranu soukromí znamená, že tyto organizace nemohou tvrdit, že vyhovují požadavkům štítu na ochranu soukromí, a že se musí vyvarovat veškerých prohlášení nebo zavádějících postupů, ze kterých vyplývá, že náleží ke štítu na ochranu soukromí, a že tyto organizace již nemají nárok využívat rozhodnutí Evropské komise o odpovídající úrovni ochrany, jež by jim umožňovalo přijímat osobní informace z EU. Organizaci, která po

⁽¹⁾ Za předpokladu, že rozhodnutí Komise o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí bude platit pro Island, Lichtenštejnsko a Norsko, bude se soubor materiálů ke štítu na ochranu soukromí vztahovat jak na Evropskou unii, tak na tyto tři země. Odkazy na EU a její členské státy tedy zahrnují i Island, Lichtenštejnsko a Norsko.

odstranění ze seznamu organizací štítu na ochranu soukromí nadále tvrdí, že ke štítu náleží, nebo v souvislosti se štítem jinak uvádí v omyl, hrozí opatření za účelem prosazení práva ze strany FTC, ministerstva dopravy či jiných donucovacích orgánů.

5. Dodržování těchto zásad může být omezeno: a) v rozsahu nezbytném pro splnění požadavků národní bezpečnosti, veřejného zájmu nebo prosazování zákonů, b) zákonem, správním nařízením nebo judikaturou, které vytvářejí protichůdné závazky, nebo výslovným zmocněním za předpokladu, že při výkonu takového zmocnění může organizace prokázat, že nedodržení zásad je omezeno na rozsah nezbytný pro dodržení nadřazených oprávněných zájmů, jimž má takové zmocnění sloužit, nebo c) jestliže směrnice nebo právo členského státu umožňují výjimky nebo odchylky, pokud se takové výjimky nebo odchylky uplatňují ve srovnatelných souvislostech. V souladu s cílem zvýšit ochranu soukromí by organizace měly usilovat o úplné a transparentní uplatňování těchto zásad, včetně toho, že uvedou, v jakých případech se výjimky ze zásad povolené podle písmene b) budou v jejich opatřeních na ochranu soukromí uplatňovat pravidelně. 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. Po vstupu do štítu na ochranu soukromí jsou organizace povinny používat tyto zásady na všechny osobní údaje předané na základě štítu na ochranu soukromí. Organizace, která se rozhodne rozšířit výhody plynoucí ze štítu na ochranu soukromí na osobní informace týkající se lidských zdrojů, předávané z EU pro využití v rámci zaměstnaneckých vztahů musí tuto skutečnost oznámit při autocertifikaci u ministerstva a musí splnit požadavky uvedené v doplňkové zásadě o autocertifikaci.
7. V otázkách výkladu a dodržování zásad a příslušných opatření na ochranu soukromí prováděných organizacemi štítu na ochranu soukromí se uplatňuje právo Spojených států, s výjimkou případů, ve kterých se tyto organizace zavázaly ke spolupráci s evropskými orgány pro ochranu údajů. Není-li stanoveno jinak, uplatní se veškerá ustanovení zásad ve všech relevantních případech.
8. Definice:
 - a. „Osobní údaje“ a „osobní informace“ jsou údaje týkající se určené nebo určitelné fyzické osoby, které spadají do oblasti působnosti směrnice, organizace ve Spojených státech je obdržela z Evropské unie a jsou zaznamenané v jakékoli podobě.
 - b. „Zpracování osobních údajů“ je jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení, šíření a výmaz nebo zničení.
 - c. „Správce“ je osoba nebo organizace, která sama nebo společně s jinými určuje účel a prostředky zpracování osobních údajů.
9. Datem účinku těchto zásad je datum pravomocného schválení rozhodnutí Evropské komise o odpovídající úrovni ochrany.

II. ZÁSADY

1. Oznamovací povinnost

- a. Organizace musí informovat fyzické osoby o:
 - i. skutečnosti, že náleží ke štítu na ochranu soukromí, a musí poskytnout odkaz na seznam organizací štítu na ochranu soukromí nebo jeho webovou adresu;
 - ii. typech shromažďovaných osobních údajů a popřípadě subjektech nebo dceřiných společnostech organizace, které také dodržují tyto zásady;

- iii. svém závazku podrobit těmto zásadám všechny osobní údaje obdržené z EU na základě štítu na ochranu soukromí;
 - iv. tom, za jakým účelem osobní informace o nich shromažďuje a využívá;
 - v. tom, jak se mohou na organizaci obrátit v případě jakýchkoli dotazů nebo stížností, včetně případné příslušné provozovny v EU, která může na tyto dotazy či stížnosti reagovat;
 - vi. typu nebo totožnosti třetích stran, kterým osobní informace předává, 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 předávání svých osobních údajů;
 - ix. nezávislém orgánu zabývajícím se řešením sporů, který má řešit stížnosti a fyzickým osobám bezplatně poskytovat příslušné možnosti odvolání, a o tom, zda je tímto orgánem: 1) orgán vytvořený orgány pro ochranu údajů, 2) poskytovatel alternativního řešení sporů se sídlem v EU, nebo 3) poskytovatel alternativního řešení sporů se sídlem ve Spojených státech;
 - x. skutečnosti, že podléhá pravomocem v oblasti vyšetřování a prosazování práva svěřeným FTC, ministerstvu dopravy nebo jakémukoli jinému schválenému subjektu Spojených států zřízenému zákonem;
 - xi. možnosti fyzické osoby uchýlit se za určitých podmínek k závaznému rozhodčímu řízení;
 - xii. požadavku sdělit 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.
- 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 předá třetí straně.

2. Možnost volby

- a. Organizace musí fyzickým osobám dát vybrat, zda jejich osobní údaje mohou být i) předány 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 je pověřena plněním úkolů jménem organizace a jedná podle jejích pokynů. Organizace však s osobou, která je jí pověřena a jedná podle jejích pokynů, 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 sexuálním životě dané osoby) musí organizace získat potvrzující výslovný souhlas (*opt-in*), jestliže mají být tyto informace i) předány 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 měly 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 dotyčnou 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 je organizací pověřená a jedná podle jejích pokynů, organizace musí: i) předávat tyto údaje pouze k omezeným a stanoveným účelům, ii) zajistit, aby osoba, která je jí pověřená a jedná podle jejích pokynů, byla povinna poskytnout alespoň tutéž úroveň ochrany soukromí, jakou požadují tyto zásady, iii) přijmout přiměřené a vhodné kroky, jež zajistí, aby osoba, která je jí pověřená a jedná podle jejích pokynů, účinně zpracovávala předané osobní informace v souladu s povinnostmi organizace podle těchto zásad, iv) požadovat, aby osoba, jež je jí pověřená a jedná podle jejích pokynů, organizaci uvědomila, zjistí-li, že již není schopna 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 s uvedenou osobou, která je jí pověřená a jedná podle jejích pokynů, o ochraně soukromí.

4. Bezpečnost

- a. Organizace, které vytvářejí, uchovávají, používají nebo šíří osobní údaje, musí přijmout přiměřená a vhodná organizační opatření, aby zabránily jejich ztrátě, zneužití a neoprávněnému přístupu k nim, jejich předávání, 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 ⁽¹⁾. 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 ⁽²⁾, pouze dokud slouží účelu zpracování ve smyslu bodu 5 písm. a). Tato povinnost nebrání organizacím zpracovávat osobní informace 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 podléhá toto zpracování ostatním zásadám a ustanovením rámce. 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 s tím spojené výdaje nebo náklady na poskytnutí přístupu byly v daném případě neúměrné ohrožení soukromí fyzické osoby nebo kdyby byla porušena práva osob jiných než dotčené fyzické osoby.

⁽¹⁾ 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.

⁽²⁾ V této souvislosti je fyzická osoba „určitelná“, pokud by ji organizace nebo třetí strana, měla-li by k údajům přístup, mohla vzhledem k prostředkům identifikace, které by bylo možné s přiměřenou pravděpodobností využít (mj. s ohledem na náklady a čas potřebné k určení a na dostupnou technologii v době zpracování), a k formě, v níž jsou údaje uchovávány, přiměřeně určit.

7. Odvolání, prosazování a odpovědnost

- a. Účinná ochrana soukromí musí zahrnovat robustní 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 orgány budou rychle reagovat na dotazy a žádosti ministerstva o informace o štítu na ochranu soukromí. Organizace musí rychle reagovat na stížnosti na dodržování zásad postoupené prostřednictvím ministerstva orgány členských států EU. Organizace, které se rozhodly spolupracovat s orgány pro ochranu údajů, včetně organizací, jež zpracovávají údaje o lidských zdrojích, musí v souvislosti s vyšetřováním a řešením stížností odpovídat přímo těmto orgánům.
- 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 doručení oznámení žalované organizaci.
- d. V souvislosti s dalším předáním údajů má za zpracování osobních informací obdržených v rámci štítu na ochranu soukromí a následně předaných třetí straně, která je pověřena organizací a jedná podle jejích pokynů, odpovědnost organizace štítu na ochranu soukromí. Organizace štítu na ochranu soukromí zůstane odpovědná podle těchto zásad, jestliže osoba, která je jí pověřena a jedná podle jejích pokynů, 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. Stane-li se organizace předmětem usnesení FTC nebo soudu z důvodu nedodržení předpisů, zveřejní veškeré příslušné části případné zprávy o dodržování předpisů či hodnotící zprávy předložené Federální obchodní komisi, které se týkají štítu na ochranu soukromí, a to v rozsahu odpovídajícím požadavkům na zachování důvěrnosti. Ministerstvo zřídilo pro orgány pro ochranu údajů specializované kontaktní místo pro případy jakýchkoli problémů organizací štítu na ochranu soukromí s dodržováním těchto zásad. FTC bude přednostně posuzovat případy nedodržování těchto zásad postoupené ministerstvem a orgány členských států EU a v závislosti na omezeních ohledně důvěrnosti údajů si bude s orgány postupujícího státu včas vyměňovat informace o postoupených případech.

III. Doplnkové zásady

1. Citlivé údaje

- a. Organizace nemusí získat potvrzující výslovný souhlas (*opt-in*), pokud je zpracování:
- i. v životně důležitém zájmu subjektu údajů nebo jiné osoby;
 - ii. nezbytné pro uplatnění 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 předány 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 a k výjimkám směrnice pro novinářskou činnost tam, kde se právo na svobodný tisk zakotvené v prvním dodatku k Ústavě Spojených států střetává se zájmy na ochraně soukromí, musí vyvážení těchto zájmů, pokud jde o činnost fyzických či právnických osob v USA, upravovat první dodatek.
- b. Na osobní údaje, 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, jakož i na informace nalezené v dříve uveřejněných materiálech pocházejících z mediálních archivů se zásady štítu na ochranu soukromí nevztahují.

3. Druhotná odpovědnost

- a. Poskytovatelé internetových služeb (ISP), telekomunikační společnosti a jiné organizace nenesou odpovědnost podle zásad štítu na ochranu soukromí, jestliže informace pouze přenášejí, přeměňují, přepojují nebo dočasně ukládají jménem jiných organizací. Stejně jako samotná směrnice ani zásady štítu na ochranu soukromí nezakládají druhotnou odpovědnost. Organizace není odpovědná v rozsahu, v němž pouze dále předává údaje přenesené třetími stranami a neurčuje účel ani prostředky zpracování těchto osobních údajů.

4. Provádění hloubkových prověrek a auditů

- a. Činnost auditorů a investičních bankéřů může zahrnovat zpracovávání osobních údajů bez souhlasu či vědomí dotčené fyzické osoby. To za níže popsanych okolností dovolují zásady oznamovací povinnosti, možnosti volby a práva na přístup.
- b. Otevřené i uzavřené akciové společnosti, včetně organizací štítu na ochranu soukromí, se pravidelně podrobují auditům. Tyto audity, zejména takové, které se zabývají potenciálním protiprávním jednáním, mohou být ohroženy, budou-li předčasně prozrazeny. Obdobně bude organizace štítu na ochranu soukromí, 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 auditori, již 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 auditori.

5. Úloha orgánů pro ochranu údajů

- a. Organizace budou provádět svůj závazek spolupracovat s orgány pro ochranu údajů z Evropské unie, jak je popsáno níže. Podle zásad štítu na ochranu soukromí se musí organizace USA, které získávají osobní údaje z EU, zavázat, že budou využívat účinné mechanismy, aby bylo zajištěno dodržování zásad štítu na ochranu soukromí. Jak je konkrétněji uvedeno v zásadě odvolání, prosazování a odpovědnosti, patří sem: 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) iii) povinnost organizací napravit problémy vzniklé v důsledku nedodržení zásad štítu na ochranu soukromí a přijmout příslušné sankce za porušení těchto zásad. Má se za to, že organizace splňuje ustanovení písm. a) bodů i) a iii) zásady odvolání, prosazování a odpovědnosti, jestliže splňuje požadavky stanovené zde pro spolupráci s orgány pro ochranu údajů.

- b. Organizace se zavazuje ke spolupráci s orgány pro ochranu údajů v autocertifikaci, že přijímá zásady štítu na ochranu soukromí, které předloží Ministerstvu obchodu Spojených států (viz doplňková zásada o autocertifikaci), a to prohlášením, ve kterém uvede, že:
- i. se rozhodla splnit požadavky uvedené pod písm. a) body i) a iii) zásady odvolání, prosazování a odpovědnosti v rámci štítu na ochranu soukromí tím, že se zavazuje ke spolupráci s orgány pro ochranu údajů;
 - ii. bude spolupracovat s orgány pro ochranu údajů při vyšetřování a řešení stížností vznesených s odvoláním na zásady štítu na ochranu soukromí a
 - iii. podrobí se doporučení příslušných orgánů pro ochranu údajů v případě, že tyto orgány dojdou k názoru, že organizace musí podniknout konkrétní opatření, aby splnila zásady štítu na ochranu soukromí, včetně opatření vedoucích k nápravě nebo odškodnění ve prospěch fyzických osob, které byly poškozeny v důsledku nedodržení těchto zásad, a poskytne orgánům pro ochranu údajů písemné potvrzení, že takové opatření provedla.
- c. Fungování orgánů vytvořených orgány pro ochranu údajů
- i. Spolupráce ze strany orgánů pro ochranu údajů má podobu informací a doporučení a probíhá tímto způsobem:
 1. Orgány pro ochranu údajů poskytují doporučení prostřednictvím svého neformálního orgánu vytvořeného na úrovni Evropské unie, jehož úkolem bude mimo jiné napomáhat zajišťovat harmonizovaný a soudržný přístup.
 2. Tento orgán bude poskytovat rady dotčeným organizacím USA v případě nevyřešených stížností fyzických osob na nakládání s osobními údaji, které byly předány z Evropské unie v rámci štítu na ochranu soukromí. Doporučení mají zajistit, aby zásady štítu na ochranu soukromí byly uplatňovány správně, a budou zahrnovat veškeré opravné prostředky ve prospěch dotčené fyzické osoby (osob), jež orgány pro ochranu údajů budou považovat za přiměřené.
 3. Tento orgán bude poskytovat rady na základě žádostí dotčených organizací nebo stížností přijatých přímo od fyzických osob na organizace, které se zavázaly ke spolupráci s orgány pro ochranu údajů pro účely štítu na ochranu soukromí, 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. Orgán se bude snažit poskytnout doporučení v co nejkratší době, jak jen to požadavek řádného procesu umožní. Zpravidla se tento orgán bude snažit poskytnout doporučení do 60 dnů od přijetí stížnosti nebo žádosti, a pokud to bude možné, rychleji.
 5. Orgán zveřejní výsledky svého vyšetřování předložených stížností, pokud to bude považovat za vhodné.
 6. Poskytování doporučení tímto orgánem nezakládá žádnou odpovědnost orgánu ani jednotlivých orgánů pro ochranu údajů.
 - ii. Jak bylo uvedeno výše, organizace, které se rozhodnou využít pro řešení sporů této možnosti, se musí zavázat, že se podrobí doporučení orgánů pro ochranu údajů. Jestliže se organizace nepodrobí doporučení do 25 dnů od jeho doručení a zpoždění uspokojivě nevysvětlí, orgán vytvořený orgány pro ochranu údajů oznámí 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 zkresleného prohlášení, nebo konstatovat, že dohoda o spolupráci byla závažným způsobem porušena, a musí být proto považována za neplatnou. V posledně jmenovaném případě informuje orgán Ministerstvo obchodu Spojených států, aby mohl být seznam organizací štítu na ochranu soukromí odpovídajícím způsobem změněn. Jakékoli nesplnění závazku spolupracovat s orgány pro ochranu údajů, jakož i nedodržení zásad štítu na ochranu soukromí je žalovatelné jako klamavé praktiky podle § 5 zákona o FTC nebo jiných podobných zákonů.
- d. Organizace, která si přeje, aby se zásady štítu na ochranu soukromí vztahovaly na údaje v oblasti lidských zdrojů předávané z EU v rámci zaměstnaneckého vztahu, se musí zavázat, že bude v takových případech spolupracovat s orgány pro ochranu údajů (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 orgánu vytvořeného orgány pro ochranu údajů, a mohou být navíc požádány, aby uhradily náklady na veškeré potřebné překlady vyplývající z poradenské činnosti orgánu v souvislosti s vyšetřováním žádostí nebo stížností podaných proti nim. Roční poplatek nepřesáhne 500 USD a pro menší společnosti bude nižší.

6. Autocertifikace

- a. Výhody štítu na ochranu soukromí jsou zajištěny od data, kdy ministerstvo rozhodne, že autocertifikace organizace je úplná, a umístí ji na seznam organizací štítu na ochranu soukromí.
- b. Za účelem autocertifikace přijetí zásad štítu na ochranu soukromí musí organizace ministerstvu poskytnout autocertifikát podepsaný vedoucím pracovníkem jménem organizace, v němž musí být uvedeny alespoň následující informace:
 - i. název organizace, poštovní adresa, e-mailová adresa, číslo telefonu a faxu;
 - ii. popis činnosti organizace v souvislosti s osobními údaji přijímanými z EU; a
 - iii. popis politiky ochrany soukromí u dané organizace uplatňovaných pro takové osobní údaje, obsahující:
 - 1. má-li organizace veřejné internetové stránky, příslušnou webovou 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;
 - 2. datum, kdy nabyla účinnosti;
 - 3. kontaktní místo pro vyřizování stížností, žádostí o přístup k informacím a dalších záležitostí vyplývajících ze štítu na ochranu soukromí;
 - 4. 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 štítu na ochranu soukromí nebo v jejich budoucí příloze);
 - 5. název případných programů na ochranu soukromí, jichž se organizace účastní;
 - 6. způsob ověřování (např. vnitřní, prostřednictvím třetí strany) (viz doplňková zásada o ověřování) a a
 - 7. nezávislý odvolací orgán pro vyšetřování nevyřešených stížností.
- c. Pokud si organizace přeje rozšířit výhody plynoucí ze štítu na ochranu soukromí na údaje o lidských zdrojích 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 o lidských zdrojích a který je uveden v těchto zásadách nebo v jejich budoucí příloze. Organizace musí navíc uvést tuto skutečnost při autocertifikaci a zavázat se ke spolupráci s příslušným(i) orgánem (orgány) v EU v souladu s použitelnými ustanoveními doplňkových zásad údajů v oblasti lidských zdrojů a úlohy orgánů pro ochranu údajů a k tomu, že bude dodržovat doporučení vydaná takovými orgány. 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.
- d. Ministerstvo povede seznam organizací štítu na ochranu soukromí, které se autocertifikují, a kterým tak náleží výhody štítu na ochranu soukromí, a bude takovýto seznam aktualizovat na základě každoroční autocertifikace a oznámení přijatých podle doplňkové zásady o řešení sporů a prosazování. Taková autocertifikace musí proběhnout alespoň jednou ročně; v opačném případě bude organizace odstraněna ze seznamu organizací štítu na ochranu soukromí a nebudou jí již nadále náležet výhody vyplývající ze štítu. Jak tento seznam organizací štítu na ochranu soukromí, tak autocertifikáty předložené organizacemi budou zpřístupněny veřejnosti. Všechny organizace, které ministerstvo umístí na seznam organizací štítu na ochranu soukromí, musí ve své zveřejněné

politice ochrany soukromí uvést, že přijímají zásady štítu na ochranu soukromí. Je-li politika ochrany soukromí dostupná on-line, musí obsahovat hypertextový odkaz na internetové stránky ministerstva věnované štítu na ochranu soukromí a hypertextový odkaz na internetové stránky nezávislého odvolacího orgánu pro vyšetřování nevyřešených stížností nebo jeho formulář pro podávání stížností.

- e. Zásady ochrany soukromí se použijí okamžitě po certifikaci. Vzhledem k tomu, že tyto zásady budou mít dopad na obchodní vztahy s třetími stranami, organizace, které certifikují dodržování rámce štítu na ochranu soukromí v prvních dvou měsících od data účinnosti rámce, co nejdříve, nejpozději však do devíti měsíců od data, kdy certifikují dodržování zásad štítu na ochranu soukromí, uvedou stávající obchodní vztahy s třetími stranami v soulad se zásadou odpovědnosti za další předávání. Pokud organizace v průběhu tohoto přechodného období předají údaje třetí straně, i) použijí zásady oznamovací povinnosti a možnosti volby, a ii) pokud předají osobní údaje třetím stranám, které jsou organizacemi pověřené a jednají podle jejich pokynů, zajistí, aby uvedené třetí strany byly povinny poskytnout alespoň tutéž úroveň ochrany, jakou vyžadují tyto zásady.
- f. Organizace musí zásadám štítu na ochranu soukromí podrobit všechny osobní údaje obdržené z EU na základě štítu. Závazek dodržovat zásady štítu na ochranu soukromí není ve vztahu k osobním údajům, které organizace obdržela v době, v níž požívá výhod štítu na ochranu soukromí, časově omezen. Tento závazek znamená, že se na takové údaje nadále vztahují zásady štítu na ochranu soukromí tak dlouho, dokud je organizace uchovává, používá nebo předává, a to i v případě, že následně z jakéhokoli důvodu štít na ochranu soukromí opustí. Organizace, která ze štítu na ochranu soukromí vystoupí, ale chce si tyto údaje ponechat, musí každý rok ministerstvu potvrdit svůj závazek nadále používat tyto zásady nebo zajistit „odpovídající“ ochranu informací jinými schválenými prostředky (například pomocí smlouvy, do níž se v plném rozsahu promítají požadavky příslušných standardních smluvních doložek přijatých Evropskou komisí); v opačném případě musí organizace informace vrátit či vymazat. Organizace, která ze štítu na ochranu soukromí vystoupí, musí z příslušné politiky na ochranu soukromí odstranit veškeré odkazy na štít na ochranu soukromí, z nichž vyplývá, že se organizace štítu nadále aktivně účastní a má nárok na jeho výhody.
- g. Organizace, která přestane existovat jako samostatná právnická osoba v důsledku fúze nebo převzetí, to musí ministerstvu předem oznámit. Toto oznámení by mělo rovněž obsahovat údaj o tom, zda přebírající subjekt nebo subjekt vzniklý fúzí i) bude nadále podle práva, podle něhož se převzetí nebo fúze uskutečnila, vázán zásadami štítu na ochranu soukromí nebo ii) se rozhodne autocertifikovat, že přijímá zásady štítu na ochranu soukromí, nebo poskytne jiná ochranná opatření, jako např. písemnou dohodu zajišťující dodržování zásad štítu na ochranu soukromí. Neuplatní-li se ani bod i), ani bod ii), musí být veškeré osobní údaje, které byly získány v rámci štítu na ochranu soukromí, neprodleně vymazány.
- h. Pokud organizace štít na ochranu soukromí z jakéhokoli důvodu opustí, musí odstranit všechna prohlášení, ze kterých vyplývá, že ke štítu na ochranu údajů nadále náleží nebo že má nárok na jeho výhody. Také musí odstranit certifikační ochrannou známku štítu EU-USA na ochranu soukromí, užívá-li ji. Jakákoli zkreslená prohlášení vůči veřejnosti o tom, že organizace uplatňuje zásady štítu na ochranu soukromí, mohou být žalována FTC nebo jiným příslušným orgánem veřejné správy. Zkreslená prohlášení vůči ministerstvu mohou být žalována podle zákona o nepravdivých prohlášeních (*False Statements Act*) (18 U.S.C. § 1001).

7. Ověřování

- a. Organizace musí následnými postupy ověřovat, že osvědčení a tvrzení o jejich opatřeních na ochranu soukromí v rámci štítu na ochranu soukromí jsou pravdivá a že se tato opatření provádějí skutečně tak, jak je v nich uvedeno, a v souladu se zásadami štítu na ochranu soukromí.
- b. Organizace, aby splnila požadavky na ověřování podle zásady odvolání, prosazování a odpovědnosti, musí taková osvědčení a tvrzení ověřit buď sama, nebo nechat provést kontrolu externí osobou.
- c. V případě posuzování prováděného samotnou organizací musí být takovým ověřením zjištěno, že zveřejněná politika organizace na ochranu soukromí u osobních údajů získaných z EU je přesná, úplná, oznámená na viditelném místě, plně provedená a přístupná. Dále musí být zjištěno, že tato politika ochrany soukromí jsou v souladu se zásadami štítu na ochranu soukromí; že fyzické osoby jsou informovány o vnitřních postupech pro vyřizování stížností a o nezávislých mechanismech, jejichž prostřednictvím mohou podávat své stížnosti; že organizace má své postupy pro školení zaměstnanců v provádění těchto opatření a že postihuje nedodržování těchto opatření a že má vnitřní postupy pro pravidelnou objektivní kontrolu dodržování výše uvedených

opatření. Prohlášení ověřující posuzování prováděné samotnou organizací musí podepsat vedoucí pracovník nebo jiný zmocněný zástupce organizace alespoň jednou ročně a musí být poskytnuto na žádost fyzických osob nebo v souvislosti s vyšetřováním nebo stížností na nedodržování předpisů.

- d. Pokud se organizace rozhodne pro externí kontrolu dodržování, musí tato kontrola prokázat, že politika organizace na ochranu soukromí u osobních údajů získaných z EU jsou v souladu se zásadami štítu na ochranu soukromí, že se dodržují a že fyzické osoby jsou informovány o způsobech, kterými mohou podávat stížnosti. Metody kontroly mohou bez omezení zahrnovat audit, náhodné kontroly, použití „návnady“ nebo popřípadě použití technologických nástrojů. Prohlášení osvědčující úspěšné provedení externí kontroly musí být podepsáno buď kontrolující osobou, nebo vedoucím pracovníkem či jiným zmocněným zástupcem organizace alespoň jednou ročně a musí být poskytnuto 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 vytvořených podle zásad štítu na ochranu soukromí a na žádost v souvislosti s vyšetřováním nebo stížností na nedodržování předpisů je musí poskytnout nezávislému orgánu 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 štítu na ochranu soukromí 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⁽¹⁾;
 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 rozhovor, aby lépe porozuměla motivu její 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, organizace by měla chráněné informace oddělit a ostatní informace dát k dispozici. Jestliže organizace rozhodne, že v některém konkrétním případě je nutno přístup omezit, musí podat fyzické osobě požadující přístup vysvětlení, proč takto rozhodla, a uvést kontaktní místo, které podá další informace.

b. Výdaje nebo náklady na poskytnutí přístupu

- i. Právo na přístup k osobním údajům lze za výjimečných okolností omezit, kdyby s tím spojené výdaje nebo náklady na poskytnutí přístupu byly v daném případě neúměrné ohrožení soukromí fyzické osoby nebo kdyby byla porušena práva osob jiných než dotčené fyzické osoby. Náklady a zátěž představují důležité hledisko a musí být brány v úvahu, avšak nejsou rozhodujícími faktory pro určení toho, zda je poskytnutí přístupu únosné.

⁽¹⁾ 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 sdělovány.

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

d. Uspořádání databází

- i. Poskytnutí přístupu může mít formu poskytnutí informací o uchovávaných příslušných osobních informacích fyzické osobě a nevyžaduje se, aby fyzická osoba získala přístup k databázi organizace.
- ii. Organizace musí poskytnout přístup pouze v rozsahu, v jakém 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 směrnice může organizace omezit přístup k informacím v rozsahu, v němž by jejich zveřejnění 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. Další důvody pro zamítnutí 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 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 musí být sděleny důvody omezení přístupu a kontaktní místo, které podá další informace.

f. Právo obdržet potvrzení a uložit poplatek na krytí 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 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

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

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

i. Časový rámec pro reakce

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 štítu na ochranu soukromí

- 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 přijímá zásady štítu na ochranu soukromí, požívá předávání výhod štítu. 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 štítu na ochranu soukromí se uplatní, pouze pokud se předávají nebo zpřístupňují záznamy o určených či určitelných fyzických osobách. Statistické výkazy zakládající se na agregovaných údajích o zaměstnancích a obsahující osobní údaje nebo na využívání anonymních údajů nepředstavují ohrožení soukromí.

b. Používání zásad oznamovací povinnosti a možnosti volby

- i. Organizace USA, která přijala informace o zaměstnancích z EU v rámci štítu na ochranu soukromí, 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 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, zavedení anonymity pro určité údaje nebo přidělení kódů či pseudonymů, pokud skutečná jména nejsou pro účel řízení potřebná.
- iv. V rozsahu a po dobu nezbytnou k zachování schopnosti organizace zvyšovat, jmenovat nebo přijímat jiná podobná personální rozhodnutí je organizace od oznamovací povinnosti a od povinnosti umožnit volbu osvobozena.

c. Používání zásady práva na přístup

V doplňkové zásadě o přístupu je uvedeno, z jakých důvodů může být požadovaný přístup k informacím o lidských zdrojích zamítnut nebo omezen. Zaměstnavatelé v Evropské unii musí samozřejmě dodržovat místní právní předpisy a zajistit, aby zaměstnanci z Evropské unie měli takový přístup k těmto informacím, jaký požadují právní předpisy v jejich zemích, bez ohledu na to, kde jsou tyto údaje zpracovávány a uchovávány. Zásady štitu na ochranu soukromí požadují, 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 tyto osobní informace využívají pouze v rámci zaměstnaneckého vztahu, nese vůči zaměstnanci hlavní odpovědnost za údaje nadále organizace usazená 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 orgán pro ochranu údajů nebo orgán příslušný pro pracovněprávní záležitosti v zemi, ve které jsou zaměstnáni. To platí i v případech, kdy za údajné zneužití jejich osobních informací nese odpovědnost organizace USA, která informace od zaměstnavatele obdržela, a jde tedy o údajné porušení zásad štitu na ochranu soukromí. 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 USA, která přistoupila k zásadám štitu na ochranu soukromí, která využívá údaje v oblasti lidských zdrojů předávané z Evropské unie v rámci zaměstnaneckého vztahu a která si přeje, aby se na taková předávání vztahovaly zásady štitu na ochranu soukromí, se tedy musí zavázat, že bude v takových případech spolupracovat při vyšetřováních prováděných příslušnými orgány EU a že se podřídí jejich doporučení.

e. Používání zásady odpovědnosti za další předávání

Pro příležitostné provozní potřeby v rámci zaměstnaneckého vztahu organizace štitu na ochranu soukromí v souvislosti s osobními údaji předanými v rámci štitu na ochranu soukromí, 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 organizace štitu na ochranu soukromí 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 na zásadách štitu na ochranu soukromí.

- ii. Správci údajů v Evropské unii 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 zpracovatel náleží ke štítu na ochranu soukromí, 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 sdělování nebo přístupu a chápe, kdy je povoleno další předávání; a
3. s ohledem na charakter zpracování pomůže správci odpovídat fyzickým osobám, které vykonávají svá práva podle těchto zásad.

- iii. Protože organizace, které náleží ke štítu na ochranu soukromí, poskytují odpovídající ochranu údajů, nemusí být smlouvy uzavírané s organizacemi náležejícími ke štítu na ochranu soukromí o pouhém zpracování údajů předem schvalovány (nebo bude takové schválení poskytnuto členskými státy EU automaticky), jak by to bylo vyžadováno u smluv uzavíraných s příjemci, kteří nenáležejí ke štítu na ochranu soukromí nebo jinak neposkytují odpovídající ochranu.

b. Předávání v rámci kontrolované skupiny korporací nebo subjektů

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 organizace štítu na ochranu soukromí.

c. Předávání mezi správci

U předávání mezi správci musí být přijímajícím správcem organizace štítu na ochranu soukromí nebo musí mít přijímající správce nezávislý odvolací orgán. Organizace štítu na ochranu soukromí musí s třetí stranou, která je přijímajícím správcem, uzavřít smlouvu, jež stanoví tutéž úroveň ochrany, jakou poskytuje štít na ochranu soukromí, a neobsahuje požadavek, aby třetí strana, která je přijímajícím správcem, byla organizací štítu na ochranu soukromí nebo měla nezávislý odvolací orgán, za předpokladu, že poskytne rovnocenný mechanismus.

11. Řešení sporů a prosazování

- a. Zásada odvolání, prosazování a odpovědnosti stanoví, jakým způsobem se vynucuje dodržování zásad štítu na ochranu soukromí. 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 orgány. 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 zahrnují zásady štítu na ochranu soukromí a které obsahují účinný donucovací mechanismus, jak je popsán v zásadě odvolání, prosazování a odpovědnosti; ii) podřízením se orgánům dozoru vytvořeným na základě zákona nebo nařízení, které zajišťují vyřizování individuálních stížností a řešení sporů; nebo iii) závazkem spolupracovat s orgány pro ochranu údajů nacházejícími se v Evropské unii 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 zakazujícího nekalé nebo klamavé jednání nebo podle jiného zákona či nařízení zakazujícího takové jednání.

- c. S cílem pomoci zajistit dodržování závazků v rámci štítu na ochranu soukromí a podpořit správu programu musí organizace i jejich nezávislé odvolací orgány poskytnout informace o štítu na ochranu soukromí na požádání ministerstvu. Kromě toho musí organizace rychle reagovat na stížnosti na dodržování zásad postoupené prostřednictvím ministerstva orgány pro ochranu 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 Spojených států.

d. Odvolací mechanismy

- i. Spotřebitelé by měli být povzbuzováni k tomu, aby vznášeli případné stížnosti u příslušných organizací předtím, než se obrátí na nezávislé odvolací orgány. Organizace musí spotřebiteli odpovědět do 45 dnů od obdržení stížnosti. To, zda je takový odvolací orgán 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. Orgány zabývající se řešením sporů jsou povinny přezkoumat každou stížnost přijatou od fyzických osob, ledaže by stížnosti byly zjevně bezdůvodné nebo nemíněné vážně. To nebrání tomu, aby odvolací orgán stanovil kritéria přípustnosti stížností, avšak taková kritéria musí být transparentní a odůvodněná (mohou například vyloučit stížnosti, které nespádají do oblasti působnosti daného programu na ochranu údajů nebo mají být řešeny jiným subjektem) a nesmí porušovat povinnost zabývat se oprávněnými stížnostmi. Odvolací orgány musí dále 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 orgánem při ochraně soukromí v souladu se zásadami štítu na ochranu soukromí. Orgány by měly rovněž spolupracovat při rozvoji nástrojů pro usnadnění řízení o stížnostech, jako jsou např. standardizované formuláře pro podávání stížností.
- ii. Nezávislé odvolací orgány musí na svých veřejných internetových stránkách uvádět informace o zásadách štítu na ochranu soukromí a službách, které v rámci štítu poskytují. Tyto informace musí obsahovat: 1) informace o požadavcích zásad štítu na ochranu soukromí týkajících se nezávislých odvolacích orgánů nebo odkaz na uvedené požadavky, 2) odkaz na internetové stránky ministerstva věnované štítu na ochranu soukromí, 3) vysvětlení, že jejich služby v oblasti řešení sporů v rámci štítu na ochranu soukromí jsou bezplatné, 4) popis způsobu podání stížnosti v souvislosti se štítem na ochranu soukromí, 5) časovou lhůtu na vyřízení stížností v souvislosti se štítem na ochranu soukromí a 6) popis nabídky potenciálních opravných prostředků.
- iii. Nezávislé odvolací orgány 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 v souvislosti se štítem na ochranu soukromí obdržených během sledovaného roku, 2) typy obdržených stížností, 3) měřítko kvality řešení sporů, jako je doba, za jakou jsou stížnosti vyřízeny, a 4) důsledky či efekty 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 organizace štítu na ochranu soukromí 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 ⁽¹⁾ nebo s tvrzeními, která se týkají odpovídající úrovně ochrany poskytované štítem na ochranu soukromí. V rámci této možnosti rozhodčího řízení má panel štítu na ochranu soukromí (*Privacy Shield 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 dotčené fyzické osoby) nezbytné k nápravě porušení těchto zásad pouze v souvislosti s dotčenou fyzickou osobou. Fyzické osoby a organizace štítu na ochranu soukromí se budou moci domáhat soudního přezkumu a výkonu rozhodčích nálezů podle práva Spojených států na základě federálního zákona o rozhodčím řízení (*Federal Arbitration Act*).

⁽¹⁾ Oddíl I bod 5 těchto zásad.

e. Opravné prostředky a sankce

Výsledkem využití opravných prostředků, které poskytuje orgán zabývající se řešením 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 orgánu zabývajícímu se řešením sporů přiměřeně reagovat na různě závažné případy nedodržení zásad. Sankce by měly zahrnovat jak zveřejnění zjištěných případů nedodržení zásad, tak za určitých okolností požadavek na vymazání údajů⁽¹⁾. Další sankce mohou zahrnovat pozastavení a odnětí možnosti prokazovat se pečeti, náhradu škody vzniklé fyzickým osobám v důsledku nedodržení zásad nebo předběžné opatření. Orgány zabývající se řešením sporů a samoregulační orgány soukromého sektoru musí oznamovat případy, kdy organizace štítu na ochranu soukromí nedodržují jejich rozhodnutí, příslušnému orgánu veřejné správy s rozhodovací pravomocí nebo soudům a informovat ministerstvo.

f. Činnost FTC

Federální obchodní komise se zavázala přednostně přezkoumávat věci týkající se údajného nedodržení těchto zásad postoupené: i) samoregulačními organizacemi na ochranu soukromí a jinými orgány zabývajícími se řešením sporů, ii) členskými státy EU a iii) ministerstvem, s cílem určit, zda byl porušen § 5 zákona o FTC, který zakazuje nekalé nebo klamavé jednání či praktiky v obchodě. Dojde-li FTC k závěru, že existuje důvodné podezření, že ustanovení § 5 byla porušena, může dosáhnout vydání úředního příkazu k zastavení činnosti, který zakáže sporné praktiky, nebo může podat žalobu u federálního okresového soudu, jenž – vyhoví-li žalobě – může vydat soudní příkaz se stejným účinkem. Patří sem nepravdivá tvrzení o dodržování zásad štítu na ochranu soukromí nebo o příslušnosti ke štítu ze strany organizací, které již nejsou na seznamu organizací štítu na ochranu soukromí či se u ministerstva nikdy neautocertifikovaly. FTC může uložit občanskoprávní sankce za porušení úředního příkazu k zastavení činnosti a může postupovat proti neuposlechnutí soudního příkazu federálního soudu občanskoprávní nebo trestněprávní cestou. FTC 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 štítu na ochranu soukromí.

g. Soustavné nedodržování zásad

- i. Jestliže organizace soustavně nedodržuje zásady štítu na ochranu soukromí, ztrácí nárok požívat výhod z něj plynoucích. Organizace, které soustavně nedodržují zásady štítu na ochranu soukromí, budou ministerstvem odstraněny ze seznamu organizací štítu na ochranu soukromí a musí osobní informace, jež získaly v rámci štítu, vrátit nebo smazat.
- ii. K soustavnému nedodržování dochází tehdy, když se organizace, která se u ministerstva autocertifikovala, odmítá podřídit konečnému rozhodnutí samoregulační organizace na ochranu soukromí nebo orgánu veřejné správy či když takový orgán rozhodne, že organizace nedodržuje zásady tak často, že již není věrohodné její tvrzení, že tak činí. V těchto případech musí organizace takové skutečnosti neprodleně oznámit ministerstvu. Nesplnění této povinnosti může být žalováno podle zákona o nepravdivých prohlášeních (18 U.S.C., § 1001). Odstoupení organizace od samoregulačního programu soukromého sektoru na ochranu soukromí nebo nezávislého mechanismu řešení sporů ji nezbavuje povinnosti dodržovat tyto zásady a představovalo by jejich soustavné nedodržování.
- iii. Ministerstvo odstraní organizaci ze seznamu organizací štítu na ochranu soukromí v reakci na každé oznámení o soustavném nedodržování zásad, ať již je obdrží od organizace samé, od samoregulačního orgánu pro ochranu soukromí, od jiného nezávislého orgánu zabývajícího se řešením sporů nebo od orgánu veřejné správy, avšak teprve po uplynutí lhůty 30 dnů poté, co organizaci, jež nedodržovala zásady,

⁽¹⁾ Orgány zabývající se řešením sporů rozhodují o okolnostech, za nichž tyto sankce použijí, podle vlastního uvážení. Jedním z faktorů, které je třeba při rozhodování o vymazání údajů brát v úvahu, je citlivost daných údajů a dále okolnost, zda organizace shromáždila, používala nebo zveřejnila informace v očividném rozporu se zásadami štítu na ochranu soukromí.

upozorní a poskytne jí možnost reagovat. Ze seznamu organizací štítu na ochranu soukromí vedeného ministerstvem je tedy zřejmé, které organizace mají a které již nemají zajištěny výhody plynoucí ze štítu na ochranu soukromí.

- iv. Organizace, která požádá o účast v samoregulačním orgánu za účelem opětovného splnění požadavků štítu na ochranu soukromí, musí tomuto orgánu poskytnout úplné informace o své předchozí přináležitosti ke štítu.

12. Možnost volby – načasování nesouhlasu

- a. Obecně je účelem zásady možnosti volby zajistit, aby byly osobní informace používány a předávány 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 *opt-out*. Ve Spojených státech mohou fyzické osoby vykonat tuto volbu také prostřednictvím využití centrálního *opt-out* programu, jako je např. program Mail Preference Service sdružení Direct Marketing Association. Organizace, jež se účastní programu Mail Preference Service sdružení Direct Marketing Association, by měly podporovat dostupnost této služby pro spotřebitele, kteří si nepřejí dostávat komerční informace. 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 lékařské péči, mohou být předávány organizacím nacházejícím se mimo EU v několika různých případech. Podle článku 26 směrnice lze předávat osobní údaje „do třetí země, která nezajišťuje odpovídající úroveň ochrany ve smyslu čl. 25 odst. 2“, pod podmínkou, že i) je to nezbytné pro poskytnutí služeb vyžádaných spotřebitelem nebo pro splnění podmínek smlouvy, jako je např. smlouva s pravidelným cestujícím, či ii) s tím spotřebitel nepochybně vyslovil souhlas. Organizace USA přijímající zásady štítu na ochranu soukromí poskytují odpovídající ochranu osobních údajů, a proto mohou přijímat údaje z EU, aniž by musely splňovat tyto podmínky nebo jiné podmínky uvedené v článku 26 směrnice. Protože zásady štítu na ochranu soukromí zahrnují zvláštní pravidla pro citlivé informace, mohou být takové informace (které někdy musí být shromažďovány, např. ve spojení s potřebou lékařské péče o zákazníka) zahrnuty v předání údajů organizacím účastnícím se štítu na ochranu soukromí. V každém případě však musí organizace, která předává informace, 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. Uplatňování zákonů členských států EU nebo zásad štítu na ochranu soukromí

Právní předpisy členského státu EU se uplatní na shromažďování osobních údajů a jejich zpracování uskutečněné před předáním do Spojených států. Zásady štítu na ochranu soukromí se uplatní na údaje po jejich předání do Spojených států. Údaje používané pro farmaceutický výzkum a další účely by měly být popřípadě anonymní.

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 náležející ke štítu na ochranu soukromí, 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 kterým dotčená fyzická osoba následně souhlasila, je nutno získat nový souhlas.

c. Odstoupení od klinického hodnocení

Účastníci se mohou kdykoli rozhodnout nebo být požádáni odstoupit od klinického hodnocení. 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

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 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 předání 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

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 zdravotnické prostředky, uplatňovat zásady štítu na ochranu soukromí 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 společnostem 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

Údaje určené pro výzkum jsou u zdroje zásadně kódovány hlavním zkoušejícím pomocí unikátního klíče tak, aby nebyla zřejmá totožnost konkrétních subjektů údajů. Farmaceutické společnosti financující takový výzkum klíč neobdrží. Kód k unikátnímu klíči má pouze výzkumný pracovník, který tak může za určitých okolností danou osobu identifikovat (např. je-li potřebný následný lékařský dohled). Předání takto kódovaných údajů z EU do Spojených států nepředstavuje předání osobních údajů, které podléhá zásadám štítu na ochranu soukromí.

15. Veřejné záznamy a veřejně přístupné informace

- a. Organizace musí na osobní údaje z veřejně dostupných zdrojů uplatňovat zásady štítu na ochranu soukromí týkající se bezpečnosti, integrity údajů, účelového omezení a odvolání, prosazování a odpovědnosti. Tyto zásady se použijí na osobní údaje shromážděné z veřejných záznamů, tj. z takových záznamů, které vedou vládní orgány nebo jiné 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 s těmito zásadami, takže tyto výjimky přinesly prospěch jí samé nebo jiným, přestane splňovat požadavky štítu na ochranu soukromí a ztratí výhody z něho plynoucí.
- d. Na informace z veřejných záznamů není nutné používat 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 nejsou veřejně dostupné. 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 organizaci, 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 organizace štítu na ochranu soukromí 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 organizacemi štítu na ochranu soukromí společně s informacemi zveřejněnými zpravodajskou komunitou a s dalšími informacemi mohou být použity jako podklad společného každoročního přezkumu fungování štítu na ochranu soukromí 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 štítu na ochranu soukromí 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 štít EU-USA na ochranu soukromí. 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 v rámci štítu na ochranu soukromí.

A. Oblast působnosti

V rozhodčím řízení, které mají fyzické osoby k dispozici, se u zbytkových nároků rozhodne, zda organizace štítu na ochranu soukromí 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⁽¹⁾ nebo s tvrzeními, která se týkají odpovídající úrovně ochrany poskytované štítem na ochranu soukromí.

B. Dostupné opravné prostředky

V rámci této možnosti rozhodčího řízení má panel štítu na ochranu soukromí (*Privacy Shield 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 dotýčné fyzické osoby) nezbytné k nápravě porušení těchto zásad pouze v souvislosti s dotčenou fyzickou osobou. To jsou jediné pravomoci rozhodčího panelu v souvislosti s opravnými prostředky. Při rozhodování o opravných prostředcích musí vzít rozhodčí panel v úvahu jiné opravné prostředky, které již uložily jiné orgány v rámci štítu na ochranu soukromí. K dispozici není náhrada škody, nákladů, poplatků ani jiné opravné prostředky. Každá strana nese své vlastní palmáře.

C. Požadavky před rozhodčím řízením

Fyzická osoba, která se rozhodne využít této možnosti rozhodčího řízení, musí před podáním žaloby učinit tyto kroky: 1) předložit údajné porušení přímo organizaci a poskytnout jí příležitost otázku vyřešit ve lhůtě stanovené v oddíle III bodě 11 písm. d) podbodě i) těchto zásad, 2) využít nezávislý bezplatný odvolací mechanismus podle těchto zásad a 3) předložit problém prostřednictvím svého orgánu pro ochranu údajů ministerstvu obchodu a poskytnout mu příležitost vynaložit maximální úsilí na bezplatné vyřešení otázky ve lhůtě stanovené v dopise odboru pro mezinárodní obchod ministerstva obchodu.

Této možnosti se nelze dovolávat, jestliže totéž údajné porušení těchto zásad žalované fyzickou osobou 1) již bylo předmětem závazného rozhodčího řízení, 2) bylo předmětem pravomocného rozsudku vynesného v soudním sporu, jehož byla fyzická osoba účastníkem, nebo 3) již bylo stranami urovnáno. Kromě toho se této možnosti nelze dovolávat, jestliže orgán pro ochranu údajů z EU 1) má pravomoc podle oddílu III bodů 5 nebo 9 těchto zásad či 2) je oprávněn řešit údajné porušení přímo s organizací. Pravomoc orgánu pro ochranu 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 orgánu pro ochranu 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 v jiné podobě 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.

⁽¹⁾ Oddíl I bod 5 těchto zásad.

E. Přezkum a prosazování

Fyzické osoby a organizace štítu na ochranu soukromí se budou moci domáhat soudního přezkumu a výkonu rozhodčích nálezů podle práva Spojených států na základě federálního zákona o rozhodčím řízení (*Federal Arbitration Act, FAA*) ⁽¹⁾. Veškeré tyto věci musí být předloženy federálnímu okrskovému soudu, který je územně příslušný pro hlavní místo podnikání organizace štítu na ochranu soukromí.

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 FTC.

F. Rozhodčí panel

Strany vyberou rozhodce ze seznamu rozhodců popsaného níže.

V souladu s použitelným právem zpracuje Ministerstvo obchodu Spojených států a Evropská komise seznam alespoň 20 rozhodců vybraných na základě nezávislosti, profesní bezúhonnosti a know-how. V souvislosti s tímto procesem platí následující:

Rozhodci:

- 1) zůstanou na seznamu po dobu 3 let, nenastanou-li výjimečné nebo odůvodněné okolnosti, přičemž toto období lze prodloužit o další 3 roky;
- 2) nepodléhají žádným pokynům žádné ze stran, žádné organizace štítu na ochranu soukromí, Spojených států, EU, žádného členského státu EU ani žádného vládního orgánu, 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 soukromé právo Spojených států a mít know-how právních předpisů EU o ochraně údajů.

G. Postupy pro rozhodčí řízení

V souladu s použitelným právem se ministerstvo obchodu a Evropská komise do 6 měsíců od přijetí rozhodnutí o odpovídající úrovni ochrany dohodnou na přijetí stávajícího zavedeného souboru postupů pro rozhodčí řízení (například organizací AAA nebo JAMS), kterými se budou řízení u panelu štítu na ochranu soukromí řídit 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 doručením 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.

⁽¹⁾ Kapitola 2 zákona 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. No. 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 nálezu uvedený v dotyčné [Newyorské] úmluvě“. Tamtéž § 207. Kapitola 2 dále stanoví, že „[p]ůvodně 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]ísenné 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.

2. Budou vypracovány postupy, které zajistí, aby u téhož porušení žalovaného fyzickou osobou nebyly uplatněny duplicitní opravné prostředky nebo postupy.
3. Souběžně s rozhodcím řízením může konat FTC.
4. Těchto rozhodčích řízení se nesmí účastnit žádný zástupce Spojených států, EU, žádného členského státu EU ani žádného vládního orgánu, orgánu veřejné moci nebo donucovacího orgánu za předpokladu, že na žádost fyzické osoby z EU mohou orgány pro ochranu údajů z EU 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, 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 rozhodcím 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 rozhodcím řízením.
9. Rozhodčí řízení by měla skončit do 90 dnů od doručení oznámení žalované organizaci, nedohodnou-li se strany jinak.

H. Náklady

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

V závislosti na použitelném právu usnadní ministerstvo obchodu po konzultaci s Evropskou komisí zřízení fondu, do kterého budou organizace štitu na ochranu soukromí muset hradit roční příspěvek založený částečně na jejich velikosti, jenž pokryje náklady na rozhodčího řízení, včetně poplatků pro rozhodce, a to do maximální stanovené výše (dále též „strop“). Fond bude spravovat třetí strana, která bude pravidelně předkládat zprávy o jeho fungování. Při každoročním přezkumu ministerstvo obchodu a Evropská komise přezkoumají fungování fondu, včetně nutnosti upravit výši příspěvků nebo stropů, a posoudí mj. počet rozhodčích řízení a jejich náklady a načasování, přičemž vzájemně chápou, že organizace štitu na ochranu soukromí nebudou nadměrně finančně zatíženy. Na základě tohoto ustanovení ani z žádného fondu podle tohoto ustanovení se nehradí palmáře.

PŘÍLOHA III

Dopis ministra zahraničí Spojených států Johna Kerryho

7. července 2016

Vážená paní komisařko Jourová,

těší mě, že jsme dosáhli porozumění ve věci štítu EU-USA na ochranu soukromí, který bude zahrnovat mechanismus ombudsmana, jehož prostřednictvím budou úřady v EU moci jménem fyzických osob z EU předkládat žádosti, které se týkají signálových zpravodajských postupů Spojených států.

Dne 17. ledna 2014 oznámil prezident Barack Obama významné reformy zpravodajských služeb uvedené v prezidentské směrnici 28 (Presidential Policy Directive 28, dále též „PPD-28“). Podle PPD-28 jsem jako naši kontaktní osobu pro cizí vlády, které chtějí vznést dotazy v souvislosti se signálovými zpravodajskými činnostmi Spojených států, určil tajemnici ministra Catherine A. Novelliovou, jež také působí jako vedoucí koordinátorka pro mezinárodní informační diplomacii. Na základě toho jsem v souladu s podmínkami stanovenými v příloze A, které byly aktualizovány od mého dopisu ze dne 22. února 2016, zřídil mechanismus ombudsmana ve věcech štítu na ochranu soukromí Výkonem této funkce jsem pověřil paní tajemnici Novelliovou. Paní tajemnice Novelliová je na zpravodajské komunitě Spojených států nezávislá a je podřízena přímo mně.

Narídl jsem svým zaměstnancům, aby věnovali potřebné prostředky na zavedení nového mechanismu ombudsmana, a jsem přesvědčen, že uvedený mechanismus bude účinným prostředkem řešení obav fyzických osob z EU.

S pozdravem
John F. Kerry

Příloha A

Mechanismus ombudsmana ve věcech štítu na ochranu soukromí v souvislosti se signálovým zpravodajstvím

Uznávajíc význam rámce štítu EU-USA na ochranu soukromí stanoví toto memorandum proces provádění nového mechanismu podle prezidentské směrnice 28 (PPD-28) v souvislosti se signálovým zpravodajstvím. ⁽¹⁾

Dne 17. ledna 2014 pronesl prezident Obama projev, ve kterém oznámil významné reformy zpravodajských služeb. V projevu uvedl, že „[n]aše úsilí pomáhá chránit nejen náš národ, ale také naše přátele a spojence. Naše úsilí bude smysluplné, pouze budou-li obyčejní občané v jiných zemích věřit, že Spojené státy respektují také jejich soukromí.“ Prezident Obama oznámil vydání nové prezidentské směrnice – PPD-28, která „zřetelně předepíše, co děláme a neděláme, pokud jde o naše sledování v zahraničí“.

Paragraf 4(d) PPD-28 nařizuje ministru zahraničí určit „vedoucího koordinátora pro mezinárodní informační diplomacii“ (dále též „vedoucí koordinátor“) „jako ... kontaktní osobu pro cizí vlády, které chtějí vznést dotazy v souvislosti se signálovými zpravodajskými činnostmi Spojených států“. Od ledna 2015 působí jako vedoucí koordinátorka tajemnice ministra C. Novelliová.

Toto memorandum popisuje nový mechanismus, jehož prostřednictvím vedoucí koordinátor usnadní zpracovávání žádostí, které se týkají přístupu k údajům pro účely národní bezpečnosti v případě údajů předaných z EU do Spojených států v rámci štítu na ochranu soukromí, standardních smluvních doložek, závazných podnikových pravidel, „odchylek“ ⁽²⁾ nebo „možných budoucích odchylek“ ⁽³⁾ zavedenými postupy podle platných zákonů a politiky Spojených států a odpovědí na uvedené žádosti.

- 1. Ombudsman ve věcech štítu na ochranu soukromí.** Jako ombudsman ve věcech štítu na ochranu soukromí bude působit vedoucí koordinátorka, jež určí další úředníky ministerstva zahraničí, kteří jí popřípadě budou pomáhat při plnění povinností rozepsaných v tomto memorandu. (Dále budou koordinátorka a veškerí úředníci vykonávající tyto povinnosti označovány též jako „ombudsman ve věcech štítu na ochranu soukromí“.) Ombudsman ve věcech štítu na ochranu soukromí bude úzce spolupracovat s příslušnými úředníky z jiných ministerstev a agentur, kteří jsou odpovědní za vyřizování žádostí v souladu s platným právem a politikou Spojených států. Ombudsman je nezávislý na zpravodajské komunitě. Je přímo podřízen ministru zahraničí, který zajistí, aby ombudsman vykonával svou funkci objektivně a nepodléhal nepatřičnému vlivu, jenž může mít účinek na odpověď, kterou má poskytnout.
- 2. Účelná koordinace.** Ombudsman ve věcech štítu na ochranu soukromí bude schopen účelně využívat a koordinovat orgány dohledu popsané níže s cílem zajistit, aby jeho odpověď na žádosti předkládajícího orgánu pro vyřizování

⁽¹⁾ Za předpokladu, že rozhodnutí Komise o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí bude platit pro Island, Lichtenštejnsko a Norsko, bude se soubor materiálů ke štítu na ochranu soukromí vztahovat jak na Evropskou unii, tak na tyto tři země. Odkazy na EU a její členské státy tedy zahrnují i Island, Lichtenštejnsko a Norsko.

⁽²⁾ „Odchylkami“ se v této souvislosti rozumí komerční předávání, ke kterému dochází pod podmínkou, že: a) subjekt údajů nepochybně udělil svůj souhlas s předpokládaným předáním, b) předání je nezbytné pro splnění smlouvy mezi subjektem údajů a správcem nebo pro splnění předmluvných opatření přijatých na žádost subjektu údajů, c) předání je nezbytné pro uzavření nebo plnění smlouvy, která byla uzavřena v zájmu subjektu údajů mezi správcem a třetí stranou, d) předání je nezbytné nebo se stává právně závazným pro zachování důležitého veřejného zájmu nebo pro zjištění, výkon nebo obranu právních nároků před soudem, e) předání je nezbytné pro ochranu životně důležitých zájmů subjektu údajů či f) k předání dochází z veřejného rejstříku, který je na základě právních předpisů určen pro informování veřejnosti a je přístupný veřejnosti nebo jakékoli osobě, která osvědčí svůj oprávněný zájem, pokud jsou v daném případě splněny právní podmínky tohoto přístupu.

⁽³⁾ „Možnými budoucími odchylkami“ se v této souvislosti rozumí komerční předávání, ke kterému dochází pod jednou z těchto podmínek, pokud uvedená podmínka představuje oprávněné důvody k předávání osobních údajů z EU do Spojených států: a) daný subjekt údajů byl informován o rizicích takového předání v důsledku absence rozhodnutí o odpovídající úrovni ochrany a vhodných záruk a následně k navrhovanému předání vydal svůj souhlas, b) předání je nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo jiné osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas, či c) v případě předání do třetí země nebo mezinárodní organizaci a v případě, kdy není použitelná žádná jiná odchylka ani možná budoucí odchylka, a pouze jestliže předání není opakované, týká se pouze omezeného počtu subjektů údajů, je nezbytné pro účely oprávněných zájmů správce, nad nimiž nepřevažují zájmy nebo práva a svobody subjektu údajů, a správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů.

stížností fyzických osob z EU vycházela z potřebných informací. Bude-li se žádost týkat slučitelnosti sledování s právem Spojených států, bude ombudsman ve věcech štítu na ochranu soukromí moci spolupracovat s jedním z nezávislých orgánů dohledu s vyšetřovacími pravomocemi.

- a. Ombudsman ve věcech štítu na ochranu soukromí bude úzce spolupracovat s dalšími vládními úředníky Spojených států, včetně příslušných nezávislých orgánů dohledu, s cílem zajistit, aby vyplněné žádosti byly zpracovány a vyřešeny v souladu s platnými zákony a postupy. Ombudsman ve věcech štítu na ochranu soukromí bude moci svou činnost úzce koordinovat s Úřadem ředitele národních zpravodajských služeb, ministerstvem spravedlnosti a dalšími příslušnými ministerstvy a agenturami, které se zabývají národní bezpečností Spojených států, s generálními inspektory, s úředníky pro zákon o svobodě informací a s úředníky pro občanské svobody a ochranu soukromí.
- b. Vláda Spojených států se bude opírat o mechanismy pro koordinaci záležitostí národní bezpečnosti napříč ministerstvy a agenturami a pro dohled nad nimi, které pomohou zajistit, aby ombudsman ve věcech štítu na ochranu soukromí dokázal odpovídat na vyplněné žádosti podle § 3(b) ve smyslu § 4(e).
- c. Ombudsman ve věcech štítu na ochranu soukromí může záležitosti spojené s žádostmi postoupit k posouzení Výboru pro dohled nad respektováním soukromí a občanských svobod.

3. Předkládání žádostí.

- a. Žádost se nejdříve předloží orgánům dohledu v členských státech, kterým přísluší dohled nad národními bezpečnostními službami a/nebo zpracováním osobních údajů orgány veřejné moci. Ombudsmanovi žádost předloží centralizovaný orgán EU (dále společně též „subjekt pro vyřizování stížností fyzických osob z EU“).
- b. Subjekt pro vyřizování stížností fyzických osob z EU prostřednictvím těchto úkonů zajistí úplnost žádosti:
 - i) Ověří totožnost fyzické osoby a skutečnost, že fyzická osoba jedná na vlastní účet, a nikoli jako zástupce vládní nebo mezivládní organizace.
 - ii) Zajistí, aby byla žádost písemná a aby obsahovala tyto základní informace:
 - veškeré informace, které tvoří východisko žádosti,
 - charakter požadovaných informací nebo opatření,
 - popřípadě údajně zúčastněné subjekty vlády Spojených států a
 - ostatní opatření využitá k získání požadovaných informací nebo opatření a odpověď obdrženou v rámci uvedených ostatních opatření.
 - iii) Ověří, že se žádost týká údajů, o kterých se lze přiměřeně domnívat, že byly předány z EU do Spojených států podle štítu na ochranu soukromí, standardních smluvních doložek, závazných podnikových pravidel, odchylek nebo možných budoucích odchylek.
 - iv) Předběžně rozhodne, že žádost je míněna vážně, není kverulantská a není předkládána ve zlém víře.
- c. Úplná žádost pro účely dalšího vyřízení ombudsmanem ve věcech štítu na ochranu soukromí podle tohoto memoranda nemusí prokázat, že vláda Spojených států skutečně získala přístup k údajům žadatele prostřednictvím signálových zpravodajských činností.

4. Závazky komunikovat s předkládajícím subjektem pro vyřizování stížností fyzických osob z EU.

- a. Ombudsman ve věcech štítu na ochranu soukromí předkládajícímu subjektu pro vyřizování stížností fyzických osob z EU potvrdí obdržení žádosti.
- b. Ombudsman ve věcech štítu na ochranu soukromí provede prvotní přezkum s cílem ověřit, že žádost byla vyplněna ve shodě s § 3(b). Zaznamená-li ombudsman ve věcech štítu na ochranu soukromí jakékoli nedostatky nebo bude-li mít k vyplnění žádosti jakékoli dotazy, obrátí se na předkládající subjekt pro vyřizování stížností fyzických osob z EU s cílem uvedené obavy vyřešit.

- c. Jestliže bude ombudsman ve věcech štítu na ochranu soukromí pro účely snazšího vhodného vyřízení žádosti potřebovat o žádosti více informací nebo jestliže bude muset fyzická osoba, která žádost původně předložila, přijmout zvláštní opatření, informuje o tom ombudsman ve věcech štítu na ochranu soukromí předkládající subjekt pro vyřizování stížností fyzických osob z EU.
 - d. Ombudsman ve věcech štítu na ochranu soukromí sleduje stav žádostí a příslušným způsobem poskytuje předkládajícímu subjektu pro vyřizování stížností fyzických osob z EU aktuální informace.
 - e. Jakmile bude žádost vyplněna tak, jak je popsáno v § 3 tohoto memoranda, ombudsman ve věcech štítu na ochranu soukromí předkládajícímu subjektu pro vyřizování stížností fyzických osob z EU včas poskytne příslušnou odpověď v závislosti na trvající povinnosti chránit informace podle platných zákonů a postupů. Ombudsman ve věcech štítu na ochranu soukromí poskytne předkládajícímu subjektu pro vyřizování stížností fyzických osob z EU odpověď, ve které potvrdí, i) že stížnost byla řádně prošetřena a ii) že právo, předpisy, vládní nařízení, prezidentské směrnice a postupy agentur Spojených států, jež stanoví omezení a ochranná opatření popsaná v dopise ODNI, byly dodrženy, nebo v případě, že nebyly dodrženy, že bylo toto nedodržení napraveno. Ombudsman ve věcech štítu na ochranu soukromí nepotvrdí ani nevyvrátí, zda byla fyzická osoba cílem sledování, ani nepotvrdí konkrétní opravný prostředek, který byl použit. Jak je dále vysvětleno v § 5, žádosti podle zákona o svobodě informací (*Freedom of Information Act*) budou vyřizovány, jak stanoví uvedený předpis a další platné předpisy.
 - f. Ombudsman ve věcech štítu na ochranu soukromí bude komunikovat přímo se subjektem pro vyřizování stížností fyzických osob z EU, který bude zase odpovědný za komunikaci s fyzickou osobou, jež žádost předložila. Bude-li přímá komunikace součástí jednoho ze základních procesů popsaných níže, bude probíhat v souladu se stávajícími postupy.
 - g. Závazky v tomto memorandu se nebudou vztahovat na obecná tvrzení, že štít EU-USA na ochranu soukromí není v souladu s požadavky Evropské unie na ochranu údajů. Závazky v tomto memorandu vycházejí z obecné shody mezi Evropskou komisí a vládou Spojených států na tom, že vzhledem k rozsahu závazků v rámci tohoto mechanismu může dojít k omezením prostředků, a to i v souvislosti s žádostmi podle zákona o svobodě informací. Pokud by výkon funkcí ombudsmana ve věcech štítu na ochranu soukromí překročil přiměřená omezení prostředků a bránil by v plnění těchto závazků, vláda Spojených států projedná s Evropskou komisí případné vhodné úpravy za účelem řešení situace.
5. **Žádosti o informace.** Žádosti o přístup k záznamům vlády Spojených států lze podávat a vyřizovat podle zákona o svobodě informací.
- a. Zákon o svobodě informací je prostředkem pro každého, kdo se domáhá přístupu ke stávajícím záznamům kterékoli federální agentury, bez ohledu na státní příslušnost žadatele. Tento předpis je kodifikován jako 5 U.S.C. § 552. Uvedený předpis, společně s dalšími informacemi o zákoně o svobodě informací, je dostupný na adrese www.FOIA.gov a <http://www.justice.gov/oip/foia-resources>. Každá agentura má vedoucího pro zákon o svobodě informací a informace o tom, jak předložit žádost podle uvedeného zákona, poskytla na svých veřejných internetových stránkách. Agentury mají procesy pro vzájemnou konzultaci o žádostech podle zákona o svobodě informací, které se týkají záznamů uchovávaných jinou agenturou.
 - b. Například:
 - i) Úřad ředitele národních zpravodajských služeb (ODNI) zřídil portál věnovaný zákonu o svobodě informací: <http://www.dni.gov/index.php/about-this-site/foia>. Tento portál poskytuje informace o předkládání žádostí, kontrole stavu stávající žádosti a přístupu k informacím uvolněným a zveřejněným Úřadem ředitele národních zpravodajských služeb podle zákona o svobodě informací. Portál ODNI věnovaný zákonu o svobodě informací obsahuje odkazy na další internetové stránky prvků zpravodajské komunity, které se týkají zákona o svobodě informací: <http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites>.
 - ii) Komplexní informace o zákonu o svobodě informací poskytuje kancelář pro informační politiku ministerstva spravedlnosti: <http://www.justice.gov/oip>. Uvedené internetové stránky nejen obsahují informace o předkládání žádostí podle zákona o svobodě informací ministerstvu spravedlnosti, ale také stanoví vládě Spojených států pokyny k výkladu a uplatňování požadavků podle dotyčného zákona.

- c. Podle zákona o svobodě informací podléhá přístup k vládním záznamům určitému počtu výjimek. Ty zahrnují omezení přístupu k utajovaným informacím o národní bezpečnosti, osobním informacím třetích stran a informacím, které se týkají vyšetřování vedených donucovacími orgány, a jsou srovnatelné s omezeními, jež ve svém vlastním zákoně o přístupu k informacím ukládá každý členský stát EU. Tato omezení platí stejnou měrou pro Američany i jiné státní příslušníky.
- d. Spory ohledně zveřejňování záznamů požadovaných podle zákona o svobodě informací lze řešit správní cestou a poté u federálního soudu. Soud musí nově rozhodnout, zda jsou záznamy odpírány dle předpisů (5 U.S.C. § 552 (a)(4)(B)), a může vládě nařídit jejich zpřístupnění. V některých případech soudy vyvrátily tvrzení vlády, že by informace měly být odepřeny jako utajované. Ačkoli nelze získat peněžitou náhradu škody, mohou soudy přiznat náhradu palmáře.
6. **Žádosti o další opatření.** Žádost, podle které údajně došlo k porušení zákona nebo jinému porušení úřední povinnosti, bude postoupena příslušnému orgánu vlády Spojených států, včetně nezávislých orgánů dohledu, s pravomocí uvedenou žádost prošetřit a vyřešit nedodržení předpisů, jak je popsáno níže.
- a. Generální inspektoři jsou ze zákona nezávislí, mají širokou pravomoc vést vyšetřování, audity a přezkumy programů, včetně podvodů a zneužívání nebo porušování zákona, a mohou doporučovat nápravná opatření.
- i) Zákon o generálních inspektorech (*Inspector General Act*) z roku 1978 v platném znění ustanovil nezávislémi a objektivními subjekty ve většině agentur federální generální inspektory, jejichž povinností je bojovat s plýtváním, podvody a zneužíváním v rámci programů a chodu příslušných agentur. Za tímto účelem je každý generální inspektor povinen provádět audity a vyšetřování, které se týkají programů a chodu jeho agentury. Kromě toho zajišťují generální inspektoři vedení a koordinaci a doporučují postupy, jejichž cílem je podporovat hospodárnost, efektivnost a účinnost, předcházet podvodům a zneužívání v rámci programů a chodu agentur a odhalovat je.
- ii) Každý prvek zpravodajské komunity má svou vlastní kancelář generálního inspektora odpovědnou mj. za dohled nad zahraničními zpravodajskými činnostmi. Byla zveřejněna řada zpráv generálních inspektorů o zpravodajských programech.
- iii) Například:
- Podle § 405 zákona o schválení zpravodajské činnosti za rozpočtový rok 2010 (*Intelligence Authorization Act of Fiscal Year 2010* – <http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf>) byla zřízena Kancelář generálního inspektora zpravodajské komunity (*Office of the Inspector General of the Intelligence Community*, dále též „IC IG“). Kancelář generálního inspektora zpravodajské komunity je povinna vést audity, vyšetřování, inspekce a přezkumy napříč zpravodajskou komunitou za účelem označení a řešení systémových rizik, zranitelných míst a nedostatků společných úkolům zpravodajských agentur s cílem příznivě ovlivnit úspory a efektivnost celé zpravodajské komunity. Kancelář generálního inspektora zpravodajské komunity je oprávněna vyšetřovat stížnosti nebo informace, které se týkají údajného porušení zákona, pravidel či předpisů, plýtvání, podvodů, zneužití pravomoci nebo významného či zvláštního ohrožení veřejného zdraví a bezpečnosti v souvislosti se zpravodajskými programy a činnostmi ODNI a/nebo zpravodajské komunity. IC IG poskytuje informace, jak předložit zprávu přímo IC IG: <http://www.dni.gov/index.php/about-this-site/contact-the-ig>.
- Kancelář generálního inspektora (*Office of the Inspector General*, dále též „OIG“ – <https://www.justice.gov>) na Ministerstvu spravedlnosti Spojených států (dále též „MS“) je zákonem zřízený nezávislý subjekt, jehož posláním je odhalovat plýtvání, podvody, zneužívání a porušování úřední povinnosti v programech a u personálu MS, odrazovat od nich a podporovat ekonomičnost a účelnost uvedených programů. OIG vyšetřuje údajná porušení trestního a občanského práva zaměstnanci MS a také provádí audity a inspekce programů MS. OIG má pravomoc nad všemi stížnostmi na porušení úřední povinnosti zaměstnanci ministerstva spravedlnosti, včetně Federálního úřadu pro vyšetřování, Úřadu pro boj proti drogám, Federální vězeňské služby, Justiční strážce Spojených států, Úřadu pro alkohol, tabák, střelné zbraně a výbušniny, úřadů státních zástupců Spojených států a zaměstnanců, kteří pracují v jiných odborech nebo kancelářích ministerstva spravedlnosti. (Jedinou výjimkou je, že údajné porušení úřední povinnosti

personálem státních zastupitelství nebo donucovacích orgánů ministerstva, které se týká výkonu pravomoci státních zástupců provádět vyšetřování, podávat žaloby či poskytovat právní poradenství, přísluší kanceláři pro profesní odpovědnost MS.) Kromě toho § 1001 zákona o vlastenectví (*USA Patriot Act*) schváleného dne 26. října 2001 nařizuje generálnímu inspektorovi přezkoumávat informace a přijímat stížnosti, které se týkají údajného zneužívání občanských práv a svobod zaměstnanci ministerstva spravedlnosti. OIG má veřejné internetové stránky – <https://www.oig.justice.gov>, kde je uvedena „horká linka“ pro podávání stížností – <https://www.oig.justice.gov/hotline/index.htm>.

b. Příslušné povinnosti mají také úřady a subjekty vlády Spojených států, které se zabývají ochranou soukromí a občanských svobod. Například:

- i) Paragraf 803 prováděcích doporučení zákona o Komisi pro 11. září (*Implementing Recommendations of the 9/11 Commission Act*) z roku 2007, kodifikovaných ve sbírce zákonů Spojených států (42 U.S.C. § 2000-ee1) zřizuje v rámci některých ministerstev a agentur (včetně ministerstva zahraničí, ministerstva spravedlnosti a ODNI) úředníky pro ochranu soukromí a občanských svobod. Paragraf 803 uvádí, že tyto úředníci pro ochranu soukromí a občanských svobod budou sloužit jako hlavní poradci, kteří mají mj. zajistit, aby v rámci příslušného ministerstva, agentury nebo prvku existovaly adekvátní postupy řešení stížností fyzických osob, jež tvrdí, že toto ministerstvo, agentura či prvek porušily ochranu jejich soukromí nebo občanské svobody.
- ii) Kancelář pro občanské svobody a ochranu soukromí Úřadu ředitele národních zpravodajských služeb (*ODNI's Civil Liberties and Privacy Office*, ODNI CLPO) vede úředník ODNI pro ochranu občanských svobod a ochranu soukromí, což je funkce zřízená zákonem o národní bezpečnosti (*National Security Act*) z roku 1948 v platném znění. K povinnostem ODNI CLPO patří zajišťovat, aby politiky a postupy prvků zpravodajské komunity zahrnovaly adekvátní ochranu soukromí a občanských svobod, a přezkoumávat a prošetřovat stížnosti na údajné zneužívání nebo porušování občanských svobod a ochrany soukromí v rámci programů a činnosti ODNI. ODNI CLPO poskytuje veřejnosti informace, včetně pokynů, jak podat stížnost, na svých internetových stránkách: www.dni.gov/clpo. Obdrží-li ODNI CLPO stížnost v souvislosti s ochranou soukromí a občanských svobod, která se týká programů a činností zpravodajské komunity, poradí se s ostatními prvky zpravodajské komunity, jak by uvedená stížnost měla být dále zpracována. Upozorňujeme, že kancelář pro občanské svobody a ochranu soukromí, která poskytuje informace o svých povinnostech na svých internetových stránkách – https://www.nsa.gov/civil_liberties/, má také Národní bezpečnostní agentura (*National Security Agency*, NSA). Naznačují-li informace, že kterákoli agentura nedodrжуje požadavky na ochranu soukromí (např. požadavek podle § 4 PPD-28), mají agentury mechanismy pro dodržování předpisů k přezkumu a nápravě nežádoucích příhody. Agentury musí hlásit nežádoucí příhody s dodržováním předpisů podle PPD-28 Úřadu ředitele národních zpravodajských služeb.
- iii) Při plnění povinností podporuje vedoucího pro ochranu soukromí a občanských svobod ministerstva spravedlnosti kancelář pro ochranu soukromí a občanských svobod (*Office of Privacy and Civil Liberties*, OPCL) ministerstva spravedlnosti. Hlavním posláním OPCL je chránit soukromí a občanské svobody amerických občanů přezkoumáváním činností ministerstva v oblasti ochrany soukromí, dohledem nad nimi a jejich koordinací. OPCL poskytuje složkám ministerstva právní poradenství a pokyny, zajišťuje dodržování předpisů o ochraně soukromí ministerstvem, včetně dodržování zákona o ochraně soukromí (*Privacy Act*) z roku 1974, ustanovení o ochraně soukromí uvedených v zákoně o elektronické veřejné správě (*E-Government Act*) z roku 2002 a federálním zákoně o řízení informační bezpečnosti (*Federal Information Security Management Act*) a směrnic o správních postupech vydaných na podporu uvedených zákonů, rozvíjí a zajišťuje odbornou přípravu ministerstva v oblasti ochrany soukromí, pomáhá vedoucímu pro ochranu soukromí a občanských svobod zpracovávat politiku ministerstva na ochranu soukromí, připravuje zprávy o ochraně soukromí pro prezidenta a Kongres a přezkoumává postupy ministerstva pro nakládání s informacemi s cílem zajistit, aby tyto postupy byly v souladu s ochranou soukromí a občanských svobod. OPCL poskytuje veřejnosti informace o svých povinnostech na adrese <http://www.justice.gov/opcl>.
- iv) Podle 42 U.S.C. § 2000ee a násl. Výbor pro dohled nad respektováním soukromí a občanských svobod průběžně přezkoumává i) politiky a postupy ministerstev, agentur a výkonných složek, které se týkají snahy chránit občany před terorismem, a jejich provádění s cílem zajistit ochranu soukromí a občanských svobod a ii) další opatření exekutivy, jež souvisejí s tímto úsilím, s cílem určit, zda tato opatření patřičně chrání soukromí a občanské svobody a jsou v souladu s rozhodnými právními a správními předpisy a postupy, jež se týkají ochrany soukromí a občanských svobod. Získává a přezkoumává zprávy a jiné informace od úředníků pro ochranu soukromí a občanských svobod a popřípadě jim poskytuje doporučení k jejich činnostem. Paragraf 803 prováděcích doporučení zákona o Komisi pro 11. září z roku 2007, kodifikovaných ve sbírce zákonů Spojených států (42 U.S.C. § 2000ee-1), nařizuje úředníkům pro ochranu soukromí a občanských svobod osmi federálními agenturami (včetně ministra obrany, ministra vnitra, ředitele národních zpravodajských služeb a ředitele Ústřední zpravodajské služby) i veškerých dalších agentur označených radou předkládat Výboru pro dohled nad respektováním soukromí a občanských svobod pravidelné zprávy, které uvádějí mj.

počet, charakter a vyřízení stížností na údajná porušení předpisů obdržených příslušnou agenturou. Předpis zmocňující Výbor pro dohled nad respektováním soukromí a občanských svobod radě nařizuje přijímat tyto zprávy a popřípadě poskytovat úředníkům pro ochranu soukromí a občanských svobod doporučení k jejich činnosti.

PŘÍLOHA IV

Dopis předsedkyně Federální obchodní komise Edith Ramirezové

7. července 2016

Elektronickou poštou

Věra Jourová
Komisařka pro spravedlnost, spotřebitele a rovnost žen a mužů
Evropská komise
Rue de la Loi/Wetstraat 200
1049 Brusel
Belgie

Vážená paní komisařko Jourová,

Federální obchodní komise Spojených států (*Federal Trade Commission*, FTC) si váží příležitosti popsat, jak prosazuje nový rámec štítu EU-USA na ochranu soukromí (dále též „rámec štítu na ochranu soukromí“ nebo „rámec“). Jsme přesvědčeni, že rámec bude hrát životně důležitou úlohu při usnadňování obchodních transakcí chránících soukromí v čím dál tím propojenějším světě. Umožní podnikům provádět významné operace v rámci celosvětového hospodářství a zároveň zajistí důležitou ochranu soukromí spotřebitelů v EU. Federální obchodní komise se přeshraniční ochraně soukromí věnuje již dlouho a prosazování rámce pro ni bude prvořadou prioritou. Níže vysvětlujeme historicky důrazné obecné prosazování ochrany soukromí Federální obchodní komisí, včetně prosazování původního programu „bezpečného přístavu“, i přístup FTC k prosazování nového rámce.

Federální obchodní komise svůj závazek prosazovat program „bezpečného přístavu“ poprvé veřejně vyjádřila v roce 2000. V té době tehdejší předseda FTC Robert Pitofsky zaslal Evropské komisi dopis, ve kterém nastínil závazek FTC důrazně prosazovat zásady „bezpečného přístavu“ pro ochranu soukromí. Federální obchodní komise tento závazek potvrdila téměř 40 donucovacími opatřeními, řadou dalších vyšetřování a spoluprací s jednotlivými evropskými orgány pro ochranu údajů (dále též „orgány pro ochranu údajů z EU“) na záležitostech vzájemného zájmu.

Poté, co Evropská komise v listopadu 2013 vznesla obavy ohledně správy a prosazování programu „bezpečného přístavu“, zahájili jsme my a Ministerstvo obchodu Spojených států konzultace s úředníky Evropské komise s cílem prozkoumat způsoby, jak tuto záležitost napravit. Zatímco uvedené konzultace pokračovaly, vydal Soudní dvůr dne 6. října 2015 rozhodnutí ve věci *Schrems*, které mj. zrušilo platnost rozhodnutí Evropské komise o odpovídající úrovni ochrany programu „bezpečného přístavu“. Po vydání uvedeného rozhodnutí jsme nadále úzce spolupracovali s ministerstvem obchodu a Evropskou komisí ve snaze posílit ochranu soukromí poskytovanou fyzickým osobám z EU. Výsledkem těchto průběžných konzultací je rámec štítu na ochranu soukromí. Stejně jako v případě programu „bezpečného přístavu“ se FTC tímto zavazuje nový rámec důrazně prosazovat. Dokladem uvedeného závazku je tento dopis.

Zejména potvrzujeme svůj závazek ve čtyřech klíčových oblastech: 1) upřednostňování a vyšetřování záležitostí předložených k přezkoumání, 2) řešení nepravdivých nebo klamavých tvrzení o přináležitosti ke štítu na ochranu soukromí, 3) průběžné sledování dodržování usnesení a 4) lepší zapojování orgánů pro ochranu údajů z EU a spolupráce s nimi na prosazování rámce. Níže uvádíme podrobné informace o každém z těchto závazků, příslušné souvislosti, které se týkají úlohy FTC při ochraně soukromí spotřebitelů a prosazování „bezpečného přístavu“, a obecnější situaci v oblasti ochrany soukromí ve Spojených státech ⁽¹⁾.

I. SOUVISLOSTI**A. Činnost FTC v souvislosti s prosazováním a politikou v oblasti ochrany soukromí**

FTC má širokou pravomoc prosazovat občanské právo s cílem podporovat ochranu spotřebitele a hospodářskou soutěž v oblasti obchodu. V rámci svého mandátu chránit spotřebitele prosazuje FTC širokou paletu zákonů o ochraně soukromí a bezpečnosti údajů o spotřebitelích. Hlavní zákon prosazovaný FTC, zákon o FTC, zakazuje „nekalé“ nebo

⁽¹⁾ Další informace o federálních a státních zákonech Spojených států na ochranu soukromí uvádíme v příloze A. Shrnutí nedávných opatření na prosazování ochrany soukromí a bezpečnosti je pak dostupné na internetových stránkách FTC na adrese <https://www.ftc.gov/reports/privacy-data-security-update-2015>.

„klamavé“ jednání či praktiky v obchodě nebo související s obchodem ⁽¹⁾. Prohlášení, opomenutí nebo praktika jsou klamavé, jestliže jsou významné a mohou spotřebitele, kteří za daných okolností jednají přiměřeně, uvést v omyl ⁽²⁾. Jednání či praktiky jsou nekalé, jestliže způsobí nebo je pravděpodobné, že způsobí značné škody, kterým se spotřebitelé nemohou rozumně vyhnout či které nejsou vyváženy odpovídajícími výhodami pro spotřebitele nebo hospodářskou soutěž ⁽³⁾. 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.

Pravomoc FTC podle zákona o FTC se vztahuje na záležitosti „v obchodě nebo související s obchodem“. FTC nemá pravomoc prosazovat trestní právo ani se zabývat záležitostmi národní bezpečnosti. FTC nemůže dosáhnout ani na většinu jiných vládních opatření. Kromě toho existují výjimky z pravomoci FTC nad obchodními aktivitami, a to mj. v souvislosti s bankami, leteckými dopravci, pojišťovnictvím a běžnými přenosovými činnostmi poskytovatelů telekomunikačních služeb. FTC také nemá pravomoc nad většinou neziskových organizací, ale má pravomoc nad fiktivními dobročinnými organizacemi nebo jinými neziskovými organizacemi, jejichž cílem je ve skutečnosti zisk. FTC má také pravomoc nad neziskovými organizacemi, jejichž cílem je zisk jejich ziskových členů, a proto jim mj. poskytují podstatné hospodářské výhody.⁵ V některých případech se příslušnost FTC překrývá s příslušností jiných donucovacích orgánů ⁽⁴⁾. V některých případech se příslušnost FTC 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.

Prosazování předpisů je základním pilířem přístupu FTC k ochraně soukromí. Federální obchodní komise dosud předložila k projednání více než 500 věcí, které se týkaly ochrany soukromí a bezpečnosti informací o spotřebitelích. Tento soubor věcí se týká off-line i on-line informací a zahrnuje donucovací opatření vůči velkým i malým společnostem, které údajně řádně nezacházely s citlivými údaji o spotřebitelích, nezabezpečily osobní informace spotřebitelů, klamavě sledovaly spotřebitele on-line, zasílaly spotřebitelům nevyžádanou poštu, instalovaly do počítačů spotřebitelů špionážní nebo jiný škodlivý software, porušily pravidlo zákazu telefonátů a další telemarketingová pravidla a nepatřičně sbíraly a sdílely informace o spotřebitelích v mobilních zařízeních. Donucovací opatření FTC – ve fyzickém i digitálním světě – vysílají společnostem významný vzkaz o nutnosti chránit soukromí spotřebitelů.

Federální obchodní komise také vyvinula řadu politických iniciativ zaměřených na zlepšení ochrany soukromí spotřebitelů, které formují její činnost v oblasti prosazování předpisů. FTC pořádá pracovní setkání a vydává zprávy, které doporučují osvědčené postupy zaměřené mj. na zlepšení ochrany soukromí v mobilním ekosystému, zvýšení transparentnosti v odvětví zprostředkovatelů údajů, maximalizaci výhod dat velkého objemu při současném zmírňování jejich rizik, zejména pro spotřebitele s nízkými příjmy a nedostatečnou dostupností služeb, a upozorňování na důsledky rozpoznávání tváří a internetu věcí pro ochranu soukromí a bezpečnost.

FTC se také zabývá osvětou spotřebitelů a podniků s cílem zvýšit dopad svých iniciativ v oblasti prosazování a vypracovávání postupů. FTC využívá k poskytování osvětových materiálů na celou řadu témat, včetně mobilních aplikací, ochrany soukromí dětí a zabezpečení údajů, různé nástroje – publikace, on-line zdroje, pracovní setkání a sociální média. Nejnověji zahájila komise svou iniciativu Začni s bezpečností (Start with Security), která zahrnuje nové pokyny pro podniky, jež čerpají z poučení z věcí komise, které se týkaly zabezpečení údajů, i řadu pracovních setkání po celé zemi. Kromě toho je FTC dlouho čelním představitelem osvěty spotřebitelů v oblasti základní výpočetní bezpečnosti. Loni si naši stránku On-line na stráž (OnGuard Online) a její mutaci ve španělštině, Alerta en Linea, zobrazilo více než 5 milionů návštěvníků.

B. Právní ochrana poskytovaná Spojenými státy ve prospěch spotřebitelů z EU

Rámec bude fungovat v širším prostředí ochrany soukromí zajišťované Spojenými státy, které chrání spotřebitele z EU řadou způsobů.

⁽¹⁾ 15 U.S.C. § 45(a).

⁽²⁾ Viz dokument FTC Policy Statement on Deception, appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), ke stažení <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

⁽³⁾ See 15 U.S.C. § 45(n); Dokument FTC Policy Statement on Unfairness, appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), ke stažení <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

⁽⁴⁾ Viz věc California Dental Ass'n v. FTC, 526 U.S. 756 (1999).

Zákaz nekalého nebo klamavého jednání či praktik uvedený v zákoně o FTC se neomezuje na ochranu spotřebitelů ve Spojených státech před společnostmi ze Spojených států, jelikož se vztahuje na praktiky, které 1) způsobují nebo je pravděpodobné, že způsobí přiměřeně předvídatelné škody ve Spojených státech, či 2) zahrnují závažné jednání ve Spojených státech. Dále může FTC využít při ochraně zahraničních spotřebitelů všechny opravné prostředky, včetně náhrady, které má k dispozici na ochranu domácích spotřebitelů.

Činnost FTC v oblasti prosazování předpisů tedy výrazně prospívá spotřebitelům ve Spojených státech i zahraničním spotřebitelům. Například ve věcech prosazování § 5 zákona o FTC chráníme soukromí jak spotřebitelů ve Spojených státech, tak zahraničních spotřebitelů. Ve věci proti zprostředkovateli informací Accusearch byl prodej důvěrných telefonních záznamů společností třetím stranám bez vědomí nebo souhlasu spotřebitelů podle FTC nekalou praktikou v rozporu s § 5 zákona o FTC. Společnost Accusearch prodala informace, které se týkaly jak spotřebitelů ve Spojených státech, tak zahraničních spotřebitelů⁽¹⁾. Soud na základě žaloby zdržovací zakázal společnosti Accusearch mj. uvádění na trh nebo prodej osobních informací spotřebitelů bez písemného souhlasu, nebyly-li získány zákonným způsobem z veřejně dostupných informací, a nařídil zaplacení téměř 200 000 USD⁽²⁾.

Dalším příkladem je vyrovnaní FTC s organizací TRUSTe. Zajišťuje, že se spotřebitelé, včetně spotřebitelů v Evropské unii, mohou opírat o prohlášení celosvětového orgánu stavovské samosprávy o jeho přezkumu a certifikaci domácích i zahraničních on-line služeb⁽³⁾. Je důležité, že naše opatření vůči organizaci TRUSTe také více posiluje samoregulační systém ochrany soukromí, neboť zajišťuje odpovědnost subjektů, které hrají v samoregulačních programech, včetně přeshraničních rámců na ochranu soukromí, významnou úlohu.

FTC také prosazuje jiné cílené zákony, jejichž ochrana se vztahuje na spotřebitele mimo Spojené státy, například zákon o ochraně soukromí dětí na internetu (*Children's Online Privacy Protection Act*, COPPA). 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 13 let, rodiče uvědomili a získali jejich ověřitelný souhlas. Zákon o ochraně soukromí dětí na internetu 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 o ochraně soukromí dětí na internetu 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 FTC mohou další výhody spotřebitelům z EU poskytovat i některé jiné federální a státní zákony o ochraně spotřebitelů a soukromí.

C. Prosazování zásad „bezpečného přístavu“

V rámci svého programu prosazování ochrany soukromí a bezpečnosti se FTC také snaží chránit spotřebitele z EU donucovacími opatřeními, která se týkají porušování zásad „bezpečného přístavu“. Federální obchodní komise uložila v souvislosti s prosazováním zásad „bezpečného přístavu“ 39 opatření: 36 se týkalo údajných nepravdivých tvrzení o certifikaci a tři věci – proti společnostem Google, Facebook a Myspace – se týkaly údajných porušení zásad ochrany soukromí v rámci „bezpečného přístavu“⁽⁴⁾. Tyto věci dokládají vykonatelnost certifikací a následky nedodržování předpisů. Dvacetiletý soudní smír vyžaduje, aby společnosti Google, Facebook a Myspace zavedly komplexní programy ochrany soukromí, které musí být přiměřeně navrženy tak, aby řešily rizika, jež pro ochranu soukromí představuje vývoj a řízení nových i stávajících produktů a služeb, a chránily soukromí a důvěrnost osobních informací. Komplexní programy na ochranu soukromí, které tato usnesení vyžadují, musí označovat významná předvídatelná rizika a zahrnovat kontrolní mechanismy k jejich řešení. Společnosti musí také FTC předkládat průběžná nezávislá posouzení svých programů ochrany soukromí. Usnesení také těmto společnostem zakazují zkreslená prohlášení o jejich postupech ochrany soukromí a jejich účasti v jakémkoli programu týkajícím se ochrany soukromí nebo bezpečnosti. Tento zákaz

⁽¹⁾ Viz Úřad kanadského komisaře pro ochranu soukromí, stížnost podle zákona o ochraně osobních informací a o elektronických dokumentech (*Personal Information Protection and Electronic Documents Act*, PIPEDA) proti společnosti Accusearch, Inc., podnikající pod názvem Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Úřad kanadského komisaře pro ochranu soukromí předložil v rámci opravného prostředku proti opatření FTC stanovisko *amicus curiae* a provedl vlastní vyšetřování, ve kterém dospěl k závěru, že praktiky společnosti Accusearch také porušovaly kanadské právo.

⁽²⁾ Viz věc *FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

⁽³⁾ Viz dokument *In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (decision and order), *dostupné zde* <https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf>.

⁽⁴⁾ Viz dokument *In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13 2011) (decision and order), *dostupné zde* <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>; Dokument *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (decision and order), *k dispozici zde* <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>; Dokument *In the Matter of Myspace LLC* No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), *dostupné zde* <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace>.

by se také vztahoval na jednání a praktiky společností podle nového rámce štítu na ochranu soukromí. FTC může tato usnesení prosazovat občanskoprávními sankcemi. A společnost Google v roce 2012 za porušení usnesení FTC skutečně zaplatila v rámci občanskoprávní sankce rekordních 22,5 milionu USD. Tato usnesení FTC tedy pomáhají chránit více než miliardu spotřebitelů po celém světě, přičemž stamiliony z nich pobývají v Evropě.

Věci FTC se také zaměřovaly na nepravdivá, klamavá nebo zavádějící tvrzení o účasti na „bezpečném přístavu“. FTC bere tato tvrzení vážně. Například ve věci *FTC v. Karnani* podala Federální obchodní komise v roce 2011 žalobu proti muži ve Spojených státech zabývajícímu se internetovým marketingem, podle které on a jeho společnost lstí přiměli britské spotřebitele domnívat se, že společnost sídlí ve Spojeném království, neboť mj. používali doménová jména s koncovkou .uk a odkazovali na britskou měnu a poštovní systém Spojeného království⁽¹⁾. Po obdržení výrobků však spotřebitelé zjistili, že musí hradit nečekaná dovozní cla, že záruky ve Spojeném království neplatí a že získání náhrady je spojeno s poplatky. Federální obchodní komise také žalované obvinila z klamání spotřebitelů v souvislosti s jejich účastí v programu „bezpečný přístav“. Stojí za povšimnutí, že všechny oběti byly ve Spojeném království.

Mnoho našich jiných případů prosazování zásad „bezpečného přístavu“ se týkalo organizací, které se připojily k programu „bezpečný přístav“, ale neobnovily svou každoroční certifikaci, a přitom nadále vystupovaly jako platní členové. Jak dále uvádíme níže, Federální obchodní komise se také zavázala zabývat se nepravdivými tvrzeními o přináležitosti k rámci štítu na ochranu soukromí. Toto strategické prosazování doplní zvyšující se počet opatření ministerstva obchodu za účelem ověřování dodržování požadavků programu na certifikaci a recertifikaci, sledování účinného dodržování předpisů, a to i pomocí dotazníků rozesílaných účastníkům rámce, a zvýšené úsilí ministerstva zjišťovat nepravdivá tvrzení o přináležitosti k rámci a zneužití certifikační ochranné známky rámce⁽²⁾.

II. UPŘEDNOSTŇOVÁNÍ A VYŠETŘOVÁNÍ VĚCÍ PŘEDLOŽENÝCH K PŘEZKOUMÁNÍ

Stejně jako u programu „bezpečný přístav“ se FTC zavazuje dát věcem předloženým členskými státy EU k přezkoumání FTC přednost. Budeme také upřednostňovat věci nedodržování samoregulačních pokynů, které se týkají rámce štítu na ochranu soukromí, předložené k přezkoumání samoregulačními organizacemi na ochranu soukromí a jinými nezávislými orgány zabývajícími se řešením sporů.

S cílem usnadnit předkládání věcí členskými státy EU k přezkoumání podle rámce vytváří FTC normalizovaný proces předkládání věcí k přezkoumání a poskytuje členským státům EU pokyny k typu informací, které by FTC při vyšetřování věcí předložených k přezkoumání nejlépe pomohly. V rámci tohoto úsilí určí FTC kontaktní osobu pro věci předložené členskými státy EU k přezkoumání. Nejužitečnější je, když předkládající orgán údajné porušení vyšetří a bude při vyšetřování spolupracovat s FTC.

Po obdržení věci předložené členským státem EU nebo orgánem stavovské samosprávy k přezkoumání může FTC přijmout za účelem řešení vznesených otázek řadu opatření. Můžeme například přezkoumat opatření dané společností na ochranu soukromí, získat další informace přímo od dané společnosti nebo od třetích stran, 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 pomohla osvěta spotřebitelů a podniků, a popřípadě zahájit donucovací řízení.

FTC se také zavazuje vyměňovat si s předkládajícími donucovacími orgány informace o věcech předložených k přezkoumání, včetně stavu uvedených věcí, v závislosti na zákonech a omezeních, které se týkají zachování 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 FTC. FTC předkládajícímu orgánu také poskytne zpětnou vazbu k typům věcí předložených k přezkoumání s cílem zefektivnit úsilí o řešení protiprávního jednání. Požádá-li předkládající

⁽¹⁾ Viz věc *FTC v. Karnani*, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (stipulated final order), dostupné zde <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf>; viz dále Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, <https://www.ftc.gov/blog/2011/06/around-world-shady-ways> (9. června 2011).

⁽²⁾ Dopis Kena Hyatta, tajemníka ministra obchodu pro mezinárodní obchod, odbor pro mezinárodní obchod Věře Jourové, komisařce pro spravedlnost, spotřebitele a rovnost žen a mužů.

donucovací orgán pro účely vlastního donucovacího řízení o informace o stavu konkrétní věci předložené k přezkoumání, FTC odpoví s ohledem na počet posuzovaných věcí předložených k přezkoumání a v závislosti na zákonných požadavcích na zachování důvěrnosti a jiných zákonných požadavcích.

FTC bude také úzce spolupracovat s orgány pro ochranu 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 FTC opravňuje pomáhat cizím donucovacím orgánům, prosazují-li zákony, jež zakazují postupy, které se významně podobají postupům zakázaným zákony prosazovanými FTC ⁽¹⁾. V rámci této pomoci může FTC v závislosti na požadavcích zákona Spojených států o bezpečném internetu (*U. S. SAFE WEB Act*) sdílet informace získané v souvislosti se svým vyšetřováním, zahájit jménem orgánu pro ochranu údajů z EU, který provádí vlastní vyšetřování, donucovací proces a vyslechnout v souvislosti s donucovacím řízením orgánu pro ochranu údajů svědky nebo žalované. Federální obchodní komise tuto pravomoc pravidelně využívá, aby pomohla jiným orgánům po celém světě ve věcech ochrany soukromí a spotřebitele ⁽²⁾.

Kromě upřednostňování věcí předložených členskými státy EU a samoregulačními organizacemi na ochranu soukromí k přezkoumání v rámci štítu na ochranu soukromí ⁽³⁾ se FTC zavazuje v příslušných případech prošetřovat možná porušení rámce z vlastního podnětu pomocí řady nástrojů.

Déle než deset let má FTC robustní program vyšetřování problémů s ochranou soukromí a bezpečností, které se týkají obchodních organizací. V rámci těchto vyšetřování Federální obchodní komise běžně zkoumala, zda dotýčný subjekt činí prohlášení o „bezpečném přístavu“. Jestliže subjekt tato prohlášení činil a vyšetřování odhalilo zjevné porušování zásad ochrany soukromí v rámci „bezpečného přístavu“, zařadila Federální obchodní komise do svých donucovacích opatření obvinění z porušování uvedených zásad. V tomto proaktivním přístupu budeme pokračovat i podle nového rámce. Je důležité uvést, že FTC provádí mnohem více vyšetřování, než kolik jich v konečném důsledku vede k veřejným donucovacím opatřením. Mnoho vyšetřování FTC je uzavřeno, protože zaměstnanci nezjistí zjevné porušení zákona. Protože vyšetřování FTC jsou neveřejná a důvěrná, uzavření vyšetřování se často nezveřejňuje.

Téměř 40 donucovacích opatření iniciovaných FTC ve věci programu „bezpečný přístav“ je dokladem závazku agentury proaktivně prosazovat přeshraniční programy ochrany soukromí. FTC bude hledat potenciální porušení rámce při vyšetřování ve věcech ochrany soukromí a bezpečnostních šetřeních, která pravidelně provádíme.

III. ŘEŠENÍ NEPRAVDIVÝCH NEBO KLAMAVÝCH TVRZENÍ O PŘÍNÁLEŽITOSTI KE ŠTÍTU NA OCHRANU SOUKROMÍ

Jak je uvedeno výše, přijme FTC opatření vůči subjektům, které uvádějí v omyl, pokud jde o jejich účast na rámci. FTC přednostně posoudí věci předložené k přezkoumání ministerstvem obchodu, které se budou týkat organizací označených za organizace, jež nepatřičně tvrdí, že jsou platnými členy rámce, nebo bez povolení užívají jakoukoli certifikační ochrannou známku rámce.

Kromě toho konstatujeme, že jestliže politika určité organizace na ochranu soukromí tvrdí, že organizace dodržuje zásady štítu na ochranu soukromí, a uvedená organizace se nezaregistruje u ministerstva obchodu nebo svou registraci neprodlouží, tato skutečnost ji nezpůsobí prosazování uvedených závazků podle rámce ze strany FTC.

⁽¹⁾ Při určování toho, zda uplatnit svou pravomoc podle zákona *U.S. SAFE WEB Act*, FTC 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.

⁽²⁾ Například v rozpočtových letech 2012–2015 využila FTC svou pravomoc sdílet informace podle zákona *U.S. SAFE WEB Act* v reakci téměř na 60 žádostí cizích agentur a vydala téměř 60 občanskoprávních výzev k podání vysvětlení nebo vydání podkladů (které se rovnají správním předvoláním), aby pomohla při 25 zahraničních vyšetřováních.

⁽³⁾ Ačkoli FTC neřeší stížnosti jednotlivých spotřebitelů ani v nich nevstupuje jako mediátor, potvrzuje, že upřednostní věci předložené k přezkoumání v rámci štítu na ochranu soukromí orgány pro ochranu údajů z EU. Kromě toho využívá FTC 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 FTC využít tentýž systém podávání stížností, který mají k dispozici občané Spojených států, na adrese www.ftc.gov/complaint. V případě individuálních stížností v rámci štítu na ochranu soukromí však může být pro občany EU nejužitečnější předkládat stížnosti orgánu svého členského státu pro ochranu údajů nebo poskytovateli alternativního řešení sporů.

IV. SLEDOVÁNÍ USNESENÍ

FTC také potvrzuje svůj závazek sledovat výkon usnesení o zajištění dodržování rámce štítu na ochranu soukromí.

V budoucích usneseních FTC podle rámce budeme požadovat dodržování rámce prostřednictvím různých vhodných předběžných opatření. Ta zahrnují zákaz zkrácených prohlášení o rámci a jiných programech ochrany soukromí, bude-li toto jednání důvodem základního opatření FTC.

Věci FTC, které se týkaly prosazování původního programu „bezpečný přístav“, jsou poučné. V 36 věcech nesprávných nebo klamavých tvrzení o certifikaci podle zásad „bezpečného přístavu“ každé usnesení zakazuje žalovanému zkrácená prohlášení o jeho účasti na programu „bezpečný přístav“ či jakémkoli jiném programu v oblasti ochrany soukromí nebo bezpečnosti a požaduje, aby daná společnost poskytla FTC zprávy o dodržování předpisů. Ve věcech porušení zásad ochrany soukromí v rámci „bezpečného přístavu“ byly společnosti požádány, aby zavedly komplexní programy ochrany soukromí a po dobu dvaceti let každé dva roky získaly od třetí strany posouzení uvedených programů, která musí poskytnout Federální obchodní komisi.

Porušování správních usnesení FTC může vést k občanskoprávním sankcím ve výši až 16 000 USD za každé porušení nebo 16 000 USD za každý den trvajícího porušování⁽¹⁾, 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 usnesení vztahuje, musí po určený počet let uchovávat dokumenty, které dokládají, že dodržují předpisy. Usnesení musí být také rozeslána zaměstnancům odpovědným za zajištění jejich dodržování.

FTC dodržování usnesení podle zásad „bezpečného přístavu“ systematicky sleduje tak jako u všech svých usnesení. FTC bere prosazování svých usnesení ve věcech ochrany soukromí a zabezpečení údajů vážně a v případě potřeby podává žaloby na jejich výkon. Například jak je uvedeno výše, společnost Google zaplatila na základě obvinění, že porušila usnesení FTC, občanskoprávní sankci ve výši 22,5 milionu USD. Je důležité, že usnesení FTC budou nadále chránit všechny spotřebitele po celém světě, kteří vstoupí s určitým podnikem do interakce, nejen spotřebitele, již podali stížnosti.

FTC v neposlední řadě nadále povede on-line seznam společností, které podléhají usnesením vyneseným v souvislosti s prosazováním programu „bezpečný přístav“ i nového štítu na ochranu soukromí⁽²⁾. Kromě toho zásady štítu na ochranu soukromí nyní vyžadují, aby společnosti, které jsou předmětem usnesení FTC nebo soudu z důvodu nedodržení zásad, zveřejnily veškeré příslušné části případné zprávy o dodržování předpisů či hodnotící zprávy předložené Federální obchodní komisi, které se týkají rámce, a to v rozsahu odpovídajícím právním a správním předpisům o zachování důvěrnosti.

V. SOUČINNOST S ORGÁNY PRO OCHRANU ÚDAJŮ Z EU A SPOLUPRÁCE NA PROSAZOVÁNÍ PŘEDPISŮ

FTC uznává významnou úlohu, kterou orgány pro ochranu údajů z EU v souvislosti s dodržováním rámce hrají, a vybízí k intenzivnějším konzultacím a spolupráci na prosazování předpisů. Kromě případných konzultací s předkládajícími orgány pro ochranu údajů o konkrétních záležitostech se FTC zavazuje účastnit se pravidelných schůzí s určenými zástupci pracovní skupiny zřízené podle článku 29, kde se bude obecně projednávat, jak zlepšit spolupráci na prosazování rámce. FTC se také spolu s ministerstvem obchodu, Evropskou komisí a pracovní skupinou zřízenou podle článku 29 bude účastnit každoročního přezkumu rámce s cílem projednat jeho provádění.

FTC také podporuje vývoj nástrojů, které zlepší spolupráci na prosazování předpisů s orgány pro ochranu údajů z EU i s jinými orgány pro prosazování ochrany soukromí ve světě. Konkrétně FTC spolu s donucovacími partnery v Evropské unii i ve světě spustila loni v rámci Globální sítě pro prosazování práva na ochranu soukromí systém varování pro sdílení informací o vyšetřováních a pro podporu koordinace prosazování předpisů. Tento nástroj varování by mohl být zvláště užitečný v souvislosti s rámcem štítu na ochranu soukromí. FTC a orgány pro ochranu údajů z EU by jej mohly využívat ke koordinaci vyšetřování v souvislosti s rámcem i jiných vyšetřování v oblasti ochrany soukromí, a to i jako výchozí bod pro sdílení informací, aby mohly spotřebitelům poskytovat koordinovanější a účinnější ochranu

⁽¹⁾ 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

⁽²⁾ Viz FTC, Business Center, Legal Resources, <https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251>.

soukromí. Těšíme se na pokračování spolupráce se zúčastněnými orgány EU na širším využívání systému varování v rámci Globální sítě pro prosazování práva na ochranu soukromí a na vývoji dalších nástrojů na zlepšení spolupráce na prosazování předpisů ve věcech ochrany soukromí, včetně věcí podle rámce štítu.

FTC s radostí potvrzuje svůj závazek prosazovat nový rámec štítu na ochranu soukromí. Těšíme se také na další spolupráci s našimi kolegy z EU na ochraně soukromí spotřebitelů na obou stranách Atlantiku.

S pozdravem

Edith Ramirez

předsedkyně

Příloha A

Rámec štítu EU-USA na ochranu soukromí v souvislostech: Přehled situace v oblasti ochrany a zabezpečení soukromí ve Spojených státech

Ochrana poskytovaná rámcem štítu EU-USA na ochranu soukromí (dále též „rámec“) existuje v souvislosti s širší ochranou soukromí poskytovanou v kontextu právního systému Spojených států jako celku. Zaprvé, Federální obchodní komise Spojených států (*Federal Trade Commission*, FTC) má robustní program ochrany soukromí a zabezpečení údajů pro obchodní praktiky ve Spojených státech, který chrání spotřebitele po celém světě. Zadruhé, situace v oblasti ochrany a zabezpečení soukromí spotřebitelů ve Spojených státech zaznamenala od roku 2000, kdy byl přijat původní program Spojených států a EU „bezpečný přístav“, značný vývoj. Od té doby bylo schváleno mnoho federálních i státních zákonů o ochraně soukromí a bezpečnosti a značně se zvýšil počet veřejnoprávních i soukromoprávních sporů v oblasti prosazování práv na ochranu soukromí. Široká působnost právní ochrany a zabezpečení soukromí spotřebitelů ve Spojených státech platné pro obchodní praktiky v oblasti osobních údajů doplňuje ochranu, kterou fyzickým osobám z EU poskytuje nový rámec.

I. OBECNÝ PROGRAM FTC V OBLASTI PROSAZOVÁNÍ OCHRANY A ZABEZPEČENÍ SOUKROMÍ

FTC je přední agenturou Spojených států na ochranu spotřebitelů zaměřenou na ochranu soukromí v komerčním sektoru. Má pravomoc stíhat nekalé nebo klamavé jednání či praktiky, které narušují soukromí spotřebitelů, jakož i prosazovat cílenější zákony o ochraně soukromí, jež chrání některé finanční informace, informace o zdravotním stavu a dětech a informace využívané k určitým rozhodnutím o způsobilosti spotřebitelů.

Federální obchodní komise má bezpříkladnou zkušenost s prosazováním ochrany soukromí spotřebitelů. Její donucovací opatření řešila protiprávní postupy na internetu i mimo něj. Federální obchodní komise například uplatnila donucovací opatření vůči dobře známým společnostem, jako je Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC a Snapchat, i vůči společnostem méně známým. Žalovala podniky, které údajně zasílaly spotřebitelům nevyžádanou poštu, instalovaly do počítačů špionážní software, nezabezpečily osobní informace spotřebitelů, klamavě sledovaly spotřebitele on-line, narušily soukromí dětí, protiprávně sbíraly informace v mobilních zařízeních spotřebitelů a nezabezpečily zařízení připojená k internetu využívaná k uchovávání osobních informací. Výsledná usnesení obvykle stanovila průběžné sledování Federální obchodní komisí po dobu dvaceti let, zakázala další porušování zákona a uložila podnikům značné finanční sankce za porušení usnesení⁽¹⁾. Důležité je, že usnesení FTC nechrání jen fyzické osoby, které si stěžovaly na problém, ale všechny spotřebitele, neboť se zabývají dalším směřováním podniků. V přeshraničním kontextu má FTC pravomoc chránit spotřebitele po celém světě před postupy uskutečňovanými ve Spojených státech⁽²⁾.

Dosud Federální obchodní komise předložila k projednání více než 130 věcí nevyžádané pošty a špionážního softwaru, více než 120 věcí porušení telemarketingového pravidla „Do Not Call“, více než 100 žalob podle zákona o spravedlivém informování o úvěrové spolehlivosti (*Fair Credit Reporting Act*), téměř 60 věcí zabezpečení údajů, více než 50 žalob ve věci obecné ochrany soukromí, téměř 30 věcí porušení zákona *Gramm-Leach-Bliley Act* a více než 20 žalob podle zákona o ochraně soukromí dětí na internetu (*Children's Online Privacy Protection Act*, COPPA)⁽³⁾. Kromě těchto případů Federální obchodní komise také odeslala a zveřejnila varovné dopisy⁽⁴⁾.

⁽¹⁾ Každému subjektu, který nedodrží usnesení FTC, hrozí občanskoprávní sankce ve výši až 16 000 USD za každé porušení nebo 16 000 USD za každý den trvajícího porušování. Viz 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

⁽²⁾ Kongres výslovně potvrdil pravomoc FTC vymáhat zákonné opravné prostředky, včetně náhrady, v případě jakéhokoli jednání či praktik v zahraničním obchodě, které 1) způsobují nebo je pravděpodobné, že způsobí přiměřeně předvídatelné škody ve Spojených státech, či 2) zahrnují závažné jednání ve Spojených státech. Viz 15 U.S.C. § 45(a)(4).

⁽³⁾ V některých případech ve věcech ochrany soukromí a zabezpečení údajů daná společnost podle komise údajně uplatňovala jak klamavé, tak nekalé praktiky; tyto věci se také někdy týkají údajného porušování více předpisů, například zákona o spravedlivém informování o úvěrové spolehlivosti, zákona Gramma, Leache a Blileyho a zákona o ochraně soukromí dětí na internetu.

⁽⁴⁾ Viz např. Press Release, Fed. Trade Comm'n, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (Dec. 22, 2014), <https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa>; Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), <https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations>; Press Release, Fed. Trade Comm'n, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 3, 2013), <https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may>.

V rámci důrazného prosazování ochrany soukromí v minulosti Federální obchodní komise také pravidelně hledala potenciální porušení programu „bezpečný přístav“. Od přijetí programu provedla Federální obchodní komise řadu vyšetřování ve věci dodržování zásad „bezpečného přístavu“ z vlastního podnětu a předložila k projednání 39 věcí porušování uvedených zásad společnostmi ze Spojených států. FTC učiní z prosazování nového rámce svou prioritu, a bude tak v tomto proaktivním přístupu pokračovat.

II. FEDERÁLNÍ A STÁTNÍ OCHRANA SOUKROMÍ SPOTŘEBITELŮ

Přehled prosazování zásad „bezpečného přístavu“, který je přílohou rozhodnutí Evropské komise o odpovídající úrovni ochrany uvedených zásad, poskytuje shrnutí mnoha federálních i státních zákonů o ochraně soukromí zavedených v době přijetí programu „bezpečný přístav“ v roce 2000 ⁽¹⁾. V té době regulovalo komerční sběr a využívání osobních informací kromě § 5 zákona o FTC mnoho federálních předpisů, např. zákon o politice v kabelových komunikacích (*Cable Communications Policy Act*), zákon o ochraně soukromí řidičů (*Driver's Privacy Protection Act*), zákon o ochraně údajů v elektronických komunikacích (*Electronic Communications Privacy Act*), zákon o elektronických převodech finančních prostředků (*Electronic Funds Transfer Act*), zákon o spravedlivém informování o úvěrové spolehlivosti (*Fair Credit Reporting Act*), zákon *Gramm-Leach-Bliley Act*, zákon o právu na ochranu finančních údajů (*Right to Financial Privacy Act*), zákon o ochraně spotřebitelů v oblasti telefonních služeb (*Telephone Consumer Protection Act*) a zákon o ochraně soukromí v souvislosti s videozáznamy (*Video Privacy Protection Act*). Obdobné zákony v těchto oblastech měly také mnohé státy USA.

Od roku 2000 došlo na federální i státní úrovni ke značnému vývoji, který poskytuje další ochranu soukromí spotřebitelů ⁽²⁾. Například na federální úrovni novelizovala Federální obchodní komise v roce 2013 prováděcí pravidlo k zákonu COPPA, a stanovila tak řadu dalších ochranných opatření pro osobní informace dětí. Federální obchodní komise také vydala dvě pravidla, kterými se provádí zákon *Gramma, Leache a Blileyho* – pravidlo o ochraně soukromí a pravidlo o ochranných opatřeních –, podle nichž finanční instituce ⁽³⁾ musí zveřejňovat své postupy sdílení informací a zavést komplexní program zabezpečení informací na ochranu informací o spotřebitelích ⁽⁴⁾. Obdobně zákon o spravedlivých a přesných úvěrových transakcích (*Fair and Accurate Credit Transactions Act*, FACTA) schválený v roce 2003 doplňuje starší zákony USA o úvěrech a stanoví požadavky na zaslepení, sdílení a likvidaci určitých citlivých finančních údajů. Federální obchodní komise schválila podle zákona FACTA řadu pravidel, která se týkají mj. práva spotřebitelů na bezplatný roční úvěrový výpis, požadavků na bezpečnou likvidaci informací ve zprávách o spotřebiteli, práva spotřebitelů vyslovit nesouhlas se zasíláním určitých nabídek úvěrů a pojištění, práva spotřebitelů odmítnout využívání poskytnutých informací přidruženým podnikem k uvádění jeho výrobků a služeb na trh a požadavků na provádění programů odhalování krádeží totožnosti a jejich předcházení finančními institucemi a věřiteli ⁽⁵⁾. Kromě toho byla v roce 2013 zrevidována pravidla schválená podle zákona o přenositelnosti zdravotního pojištění a o související odpovědnosti (*Health Insurance Portability and Accountability Act*), když to nich byla doplněna další opatření na ochranu soukromí a zabezpečení osobních zdravotních informací ⁽⁶⁾. Účinku nabyla také pravidla na ochranu spotřebitelů před nevyžádanými telemarketingovými telefonáty, robotickými telefonáty a nevyžádanou poštou. Kongres kromě toho schválil zákony, které od některých společností, jež sbírají informace o zdravotním stavu, vyžadují, aby spotřebitele v případě porušení uvědomily ⁽⁷⁾.

Velmi aktivní ve schvalování zákonů o ochraně a zabezpečení soukromí jsou i jednotlivé státy USA. Od roku 2000 schválilo zákony, které vyžadují, aby podniky uvědomily fyzické osoby o narušení bezpečnosti osobních informací,

⁽¹⁾ Viz dokument U.S. Dep't of Commerce, Safe Harbor Enforcement Overview, https://build.export.gov/main/safeharbor/eu/eg_main_018476.

⁽²⁾ V případě zájmu o komplexnější shrnutí právní ochrany ve Spojených státech viz Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015).

⁽³⁾ Zákon *Gramm-Leach-Bliley Act* velmi široce vymezuje finanční instituce, kterými se rozumí mj. všechny podniky, jež se „výrazně zabývají“ poskytováním finančních produktů nebo služeb. Patří sem například podniky proplácející šeky, poskytovatelé mikroúvěrů, zprostředkovatelé hypotečních úvěrů, nebankovní věřitelé, odhadci majetku nebo nemovitostí a odborní daňoví poradci.

⁽⁴⁾ Podle hlavy X zákona o ochraně spotřebitelů na finančním trhu (*Consumer Financial Protection Act*, CFPA), Pub. L. 111-203, 124 Stat. 1955 (July 21, 2010) (znám také jako *Dodd-Frank Wall Street Reform and Consumer Protection Act*) byla většina pravomocí FTC vytvářet pravidla podle zákona *Gramm-Leach-Bliley Act* převedena na Kancelář pro ochranu spotřebitelů na finančním trhu (*Consumer Financial Protection Bureau*, CFPB). FTC si ponechává donucovací pravomoc podle zákona *Gramm-Leach-Bliley Act* i pravomoc vytvářet pravidla v souvislosti s pravidlem o ochranných opatřeních a omezenou pravomoc vytvářet pravidla v rámci pravidla o ochraně soukromí v souvislosti s obchodníky s automobily.

⁽⁵⁾ Podle zákona CFPA sdílí komise svou úlohu v oblasti prosazování zákona FCRA s kanceláří CFPB, až na pravomoc vytvářet pravidla předanou z velké části CFPB (s výjimkou pravidel o varovných signálech a likvidaci, *Red Flags and Disposal Rules*).

⁽⁶⁾ Viz 45 C.F.R. pts. 160, 162, 164.

⁽⁷⁾ Viz např. *American Recovery & Reinvestment Act of 2009*, Pub. L. No. 111-5, 123 Stat. 115 (2009) a příslušné vyhlášky, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

čtyřicet sedm států, District of Columbia, Guam, Portoriko a Panenské ostrovy ⁽¹⁾. Alespoň třicet dva států a Portoriko má zákony o likvidaci údajů, které stanoví požadavky na zničení nebo likvidaci osobních informací ⁽²⁾. Několik států také schválilo obecné zákony o zabezpečení údajů. Kromě toho schválila různé zákony na ochranu soukromí Kalifornie, včetně zákona, který vyžaduje, aby společnosti měly opatření na ochranu soukromí a zveřejňovaly své postupy pro nesledování spotřebitelů (*Do Not Track*) ⁽³⁾, zákona „*Shine the Light*“, jenž požaduje transparentnost zprostředkovatelů údajů ⁽⁴⁾, a zákona, který stanoví „mazací tlačítko“, jež nezletilým osobám umožní požádat o vymazání některých informací v sociálních médiích ⁽⁵⁾. Na základě těchto zákonů a dalších pravomocí uložily federální a státní vládní instituce společně, které neochránily soukromí a nezabezpečily osobní informace spotřebitelů, značné pokuty ⁽⁶⁾.

K úspěšným rozsudkům a vyrovnáním, které poskytují spotřebitelům další ochranu soukromí a zabezpečení údajů, vedly také soukromoprávní soudní spory. Například v roce 2015 společnost Target souhlasila s úhradou 10 milionů USD v rámci vyrovnání se zákazníky, podle kterých byly ohroženy jejich osobní finanční informace všeobecným porušováním ochrany osobních údajů. V roce 2013 souhlasila společnost AOL s úhradou vyrovnání ve výši 5 milionů USD v rámci hromadné žaloby, která se týkala údajné neodpovídající anonymizace spojené se zveřejněním vyhledávacích dotazů stovek tisíc členů AOL. Kromě toho schválil federální soud úhradu 9 milionů USD společností Netflix za to, že údajně vedla záznamy o historii výpůjček v rozporu se zákonem o ochraně soukromí v souvislosti s videozáznamy z roku 1988. Federální soudy v Kalifornii schválily dvě samostatná vyrovnání s podnikem Facebook, jedno ve výši 20 milionů USD a druhé ve výši 9,5 milionu USD, která se týkala sběru, využívání a sdílení osobních informací uživatelů společnosti. A v roce 2008 schválil kalifornský státní soud vyrovnání ve výši 20 milionů USD se společností LensCrafters za protiprávní zveřejnění lékařských informací o spotřebitelích.

Stručně řečeno, jak toto shrnutí dokládá, poskytují Spojené státy soukromí a zabezpečení údajů spotřebitelů výraznou právní ochranu. Nový rámec štítu na ochranu soukromí, který fyzickým osobám z EU zajišťuje smysluplná ochranná opatření, bude působit v tomto širším kontextu, v němž je ochrana soukromí a zabezpečení údajů spotřebitelů nadále významnou prioritou.

⁽¹⁾ Viz např. National Conference of State Legislatures (NCSL), *State Security Breach Notification Laws* (Jan. 4, 2016), dostupné zde <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

⁽²⁾ NCSL, *Data Disposal Laws* (Jan. 12, 2016), dostupné zde <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>.

⁽³⁾ Cal. Bus. & Professional Code §§ 22575-22579.

⁽⁴⁾ Cal. Civ. Code §§ 1798.80-1798.84.

⁽⁵⁾ Cal. Bus. & Professional Code § 22580-22582.

⁽⁶⁾ Viz Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (Feb. 17, 2014), k dispozici zde <http://www.computerworld.com/s/article/9246393/jay-cline-u.s.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1>.

PŘÍLOHA V

Dopis ministra dopravy Spojených států Anthonyho Foxxe

19. února 2016

Komisařka Věra Jourová
Evropská komise
Rue de la Loi/Wetstraat 200
1 049 1 049 Brusel
Belgie

Věc: Rámec štítu EU-USA na ochranu soukromí

Vážená paní komisařko Jourová,

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

MD poprvé veřejně vyjádřilo svůj závazek prosazovat rámec „bezpečného přístavu“ v dopise zasláném Evropské komisi před 15 lety. V uvedeném dopise se MD zavázalo důsledně prosazovat zásady ochrany soukromí v rámci „bezpečného přístavu“. MD tento závazek stále dodržuje a tento dopis je toho důkazem.

MD zejména obnovuje svůj závazek v těchto klíčových oblastech: 1) upřednostňování vyšetřování údajných porušení štítu na ochranu soukromí, 2) vhodná donucovací opatření vůči subjektům, které se dopustí nepravdivých nebo klamavých tvrzení o certifikaci v souvislosti se štítem na ochranu soukromí, a 3) sledování a zveřejňování výkonu usnesení o porušení štítu na ochranu soukromí. Poskytujeme informace o každém z těchto závazků a pro účely potřebných souvislostí nezbytné základní informace o úloze MD při ochraně soukromí spotřebitelů a prosazování štítu na ochranu soukromí.

I. SOUVISLOSTI

A. Právomoc MD v oblasti ochrany soukromí

Ministerstvo je pevně odhodláno zajistit ochranu soukromí informací poskytovaných spotřebiteli leteckým dopravcům a prodejcům letenek. Právomoc MD přijímat opatření v této oblasti je zakotvena v předpisu 49 U.S.C. § 41712, který zakazuje, aby se letecký dopravce nebo prodejce letenek při prodeji letenek dopouštěl „nekalých či klamavých praktik nebo používal nekalé soutěžní metody“, které působí nebo by mohly způsobit spotřebiteli újmu. Vzorem pro § 41712 je § 5 zákona o Federální obchodní komisi (*Federal Trade Commission Act*) (15 U.S.C. § 45). Podle našeho výkladu předpis o nekalých nebo klamavých praktikách leteckým dopravcům či prodejcům letenek zakazuje: 1) porušovat podmínky jejich politiky ochrany soukromí nebo 2) shromažďovat či sdělovat soukromé informace způsobem, který narušuje veřejný pořádek, je nemravný nebo způsobuje spotřebiteli značnou újmu, jež není vykompenzována odpovídajícími výhodami. Podle našeho výkladu § 41712 také zakazuje dopravcům a prodejcům letenek: 1) porušovat jakákoli pravidla vydaná ministerstvem, která označují konkrétní praktiky v oblasti ochrany soukromí za nekalé nebo klamavé, či 2) porušovat zákon o ochraně soukromí dětí na internetu (*Children's Online Privacy Protection Act*, COPPA) nebo pravidla Federální obchodní komise (*Federal Trade Commission*, FTC), jimiž se COPPA provádí. Podle federálního práva má MD výlučnou pravomoc regulovat postupy leteckých dopravců v oblasti ochrany soukromí a pravomoc sdílenou s FTC nad postupy prodejců letenek v oblasti ochrany soukromí.

Jakmile se tedy letecký dopravce nebo prodejce letenek veřejně zaváže dodržovat zásady ochrany soukromí podle rámce štítu na ochranu soukromí, může ministerstvo využívat své zákonné pravomoci uvedené v § 41712, aby zajistilo dodržování uvedených zásad. Jakmile tedy cestující poskytne informace leteckému dopravci nebo prodejci letenek, který se zavázal ctít zásady ochrany soukromí podle rámce štítu na ochranu soukromí, 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 pro prosazování předpisů a řízení v letectví (dále též „úřad pro prosazování předpisů v letectví“). Zákonný zákaz nekalých a klamavých praktik stanovený v § 41712 prosazuje převážně jednáním, přípravou příkazů ke zdržení se konání a zpracováváním usnesení o vyměření občansko-právních sankcí. O potenciálních porušeních předpisů se úřad většinou dozvídá ze stížností, které obdrží od fyzických osob, cestovních agentur, leteckých dopravců a amerických a cizích vládních agentur. K podávání stížností ve věci ochrany soukromí na letecké dopravce a prodejce letenek mohou spotřebitelé využít internetové stránky MD ⁽¹⁾.

Není-li věc přiměřeně a vhodně urovnána, má úřad pro prosazování předpisů v letectví 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 27 500 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 pro prosazování předpisů v letectví 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 štítu na ochranu soukromí, vyžadají-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 ministerstvo dopravy obdrželo poměrně málo stížností na údajné porušení ochrany soukromí prodejci letenek nebo leteckými dopravci. Vystanou-li stížnosti, jsou vyšetřeny podle zásad stanovených výše.

C. Právní ochrana poskytovaná MD 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.

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. 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 13 let, uvědomili rodiče a získali jejich ověřitelný souhlas. Zákon o ochraně soukromí dětí na internetu 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 o ochraně soukromí dětí na internetu 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 o ochraně soukromí dětí na internetu poruší, má MD pravomoc přijmout donucovací opatření.

II. PROSAZOVÁNÍ ŠTÍTU NA OCHRANU SOUKROMÍ

Jestliže se letecký dopravce nebo prodejce letenek rozhodne účastnit se rámce štítu na ochranu soukromí a ministerstvo obdrží stížnost, že tento letecký dopravce či prodejce letenek rámec údajně porušil, podnikne za účelem důsledného prosazování rámce tyto kroky.

⁽¹⁾ <http://www.transportation.gov/airconsumer/privacy-complaints>

A. Přednostní vyšetřování údajných porušení

Úřad ministerstva pro prosazování předpisů v letectví vyšetří každou stížnost na údajné porušení štítu na ochranu soukromí (včetně stížností obdržенých od orgánů pro ochranu údajů z EU), a budou-li existovat důkazy o porušení, přijme donucovací opatření. Úřad pro prosazování předpisů v letectví bude dále spolupracovat s FTC a ministerstvem obchodu a přednostně posoudí tvrzení, že regulované subjekty nedodržují závazky chránit soukromí učiněné v rámci štítu na ochranu soukromí.

Po obdržení oznámení o údajném porušení rámce štítu na ochranu soukromí může úřad ministerstva pro prosazování předpisů v letectví přijmout v rámci svého vyšetřování řadu opatření. Může například přezkoumat opatření prodejce letenek nebo leteckého dopravce na ochranu soukromí, 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 FTC, posoudil, zda by pomohla osvěta spotřebitelů a podniků, a popřípadě zahájil donucovací řízení.

Dozví-li se ministerstvo o potenciálních porušeních štítu na ochranu soukromí prodejci letenek, koordinuje svůj postup s FTC. Rovněž budeme o výsledku případného donucovacího opatření ve věci štítu na ochranu soukromí informovat FTC a ministerstvo obchodu.

B. Řešení nepravdivých nebo klamavých tvrzení o členství

Ministerstvo zůstává odhodláno vyšetřovat porušení štítu na ochranu soukromí, včetně nepravdivých nebo klamavých tvrzení o členství v programu štítu. Přednostně posoudíme věci předložené k přezkoumání ministerstvem obchodu, které se budou týkat organizací označených za organizace, jež nepatřičně tvrdí, že jsou platnými členy štítu na ochranu soukromí, nebo bez povolení užívají certifikační ochrannou známku rámce štítu.

Kromě toho oznamujeme, že jestliže politika určité organizace na ochranu soukromí tvrdí, že organizace dodržuje hmotněprávní zásady štítu na ochranu soukromí, a uvedená organizace se nezaregistruje u ministerstva obchodu nebo svou registraci neprodlouží, tato skutečnost ji nezbaví prosazování uvedených závazků ministerstvem dopravy.

C. Sledování a zveřejňování výkonu usnesení o porušeních štítu na ochranu soukromí

Úřad ministerstva pro prosazování předpisů v letectví také zůstává odhodlán sledovat podle potřeby výkon usnesení s cílem zajistit dodržování programu štítu na ochranu soukromí. Konkrétně vydá-li úřad příkaz, aby se letecký dopravce nebo prodejce letenek v budoucnu zdržel porušování štítu na ochranu soukromí a § 41712, bude sledovat, zda subjekt ustanovení o zdržení se konání uvedené v příkazu dodržuje. Kromě toho úřad zajistí, aby usnesení ve věcech štítu na ochranu soukromí byla dostupná na jeho internetové stránce.

Těšíme se na pokračování naší spolupráce se svými federálními partnery i zúčastněnými subjekty v EU ve věcech štítu na ochranu soukromí.

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

S pozdravem

Anthony R. Foxx

ministr dopravy

PŘÍLOHA VI

**Dopis generálního rady Roberta Litta
Úřad ředitele národních zpravodajských služeb**

22. února 2016

Justin S. Antonipillai
Rada
Ministerstvo obchodu Spojených států amerických
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Zástupce náměstka ministryně
Odbor pro mezinárodní obchod
1401 Constitution Ave., NW
Washington, DC 20230

Vážený pane Antonipillai, vážený pane Deane,

v souvislosti s vyjednáváním o štítu EU-USA na ochranu soukromí poskytly Spojené státy v průběhu posledních dvou a půl let podstatné informace o fungování činností shromažďování informací zpravodajskou komunitou Spojených států prostřednictvím signálového zpravodajství. Součástí byly i informace o platném právním rámci, víceúrovňovém dohledu nad těmito činnostmi, rozsáhlém zprůhledňování těchto činností a o celkové ochraně soukromí a občanských svobod s cílem pomoci Evropské komisi rozhodnout o odpovídající úrovni uvedených ochranných opatření, neboť se týkají výjimky ze zásad štítu na ochranu soukromí pro národní bezpečnost. V tomto dokumentu jsou poskytnuté informace shrnuty.

I. PREZIDENTSKÁ SMĚRNICE 28 A SIGNÁLOVÁ ZPRAVODAJSKÁ ČINNOST SPOJENÝCH STÁTŮ

Zpravodajská komunita Spojených států shromažďuje zahraniční zpravodajské informace způsobem, který je pečlivě kontrolován, je v přísném souladu se zákony Spojených států a podléhá několika úrovním dohledu; zaměřuje se na důležité priority v oblasti zahraničního zpravodajství a národní bezpečnosti. Shromažďování informací prostřednictvím signálových zpravodajských služeb Spojených států upravuje mozaika zákonů a postupů, mimo jiné Ústava Spojených států amerických, zákon o zabezpečování informací o činnostech cizí moci (*Foreign Intelligence Surveillance Act*, FISA, 50 U.S.C. § 1801 a násl.), výkonný dekret 12333 a jeho prováděcí pravidla, prezidentské pokyny a četné postupy a pokyny, které byly schváleny Soudem pro uplatňování zákona FISA a ministrem spravedlnosti a které stanovují dodatečná pravidla pro omezení shromažďování, uchovávání, používání a šíření informací zahraničního zpravodajství ⁽¹⁾.

a. Přehled prezidentské směrnice 28

V lednu 2014 přednesl prezident Obama řeč, v níž nastínil několik reforem signálových zpravodajských činností Spojených států, a vydal k těmto činnostem prezidentskou směrnici 28 (*Presidential Policy Directive 28*, PPD-28) ⁽²⁾. Prezident zdůraznil, že signálové zpravodajské činnosti Spojených států pomáhají zajistit bezpečnost nejen naší země a našich svobod, ale také bezpečnost a svobody jiných zemí, včetně členských států EU, které se při ochraně svých občanů spoléhají na informace získané zpravodajskými agenturami Spojených států.

Ve směrnici PPD-28 je stanovena řada zásad a požadavků, které se vztahují na všechny signálové zpravodajské činnosti Spojených států a na všechny osoby, bez ohledu na státní příslušnost nebo místo, kde se nacházejí. Zejména stanovuje určité požadavky na postupy pro řešení shromažďování, uchovávání a šíření osobních informací o osobách, které nejsou osobami USA, získaných signálovým zpravodajstvím Spojených států. Tyto požadavky jsou níže rozebrány podrobněji, lze je však shrnout takto:

— PPD znovu opakuje, že Spojené státy shromažďují informace prostřednictvím signálového zpravodajství pouze tak, jak je povoleno zákonem, výkonným dekretem nebo jinými prezidentskými směrnicemi.

⁽¹⁾ Další informace o zahraničních zpravodajských činnostech Spojených států jsou veřejně dostupné on-line na stránce IC on the Record (www.icontherecord.tumblr.com), což je veřejná stránka ODNI, která usiluje o vyšší transparentnost zpravodajských činností vlády.

⁽²⁾ Dostupné zde <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

- PPD stanovuje postupy pro zajištění toho, že se signálové zpravodajské činnosti provádějí pouze za účelem plnění zákonných a povolených cílů národní bezpečnosti.
- PPD rovněž vyžaduje, aby ochrana soukromí a občanských svobod tvořila nedílnou součást plánování shromažďování informací prostřednictvím signálových zpravodajských činností. Spojené státy především neshromažďují zpravodajské informace proto, aby potlačovaly nebo obtěžovaly osoby, které je kritizují či s nimi nesouhlasí, ani proto, aby znevýhodňovaly osoby na základě jejich etnické příslušnosti, rasy, pohlaví, sexuální orientace nebo náboženství, a ani proto, aby poskytovaly konkurenční obchodní výhody společností a podnikatelskému odvětví ze Spojených států.
- PPD nařizuje, aby bylo shromažďování informací prostřednictvím signálových zpravodajských činností v nejvyšší možné míře uzpůsobeno na míru a aby se hromadné informace shromažďované prostřednictvím signálových zpravodajských služeb využívaly pouze ke konkrétně vyjmenovaným účelům.
- PPD nařizuje, aby zpravodajská komunita přijala postupy, které jsou „přiměřeně navrženy tak, aby minimalizovaly šíření a uchovávání osobních informací shromážděných prostřednictvím signálových zpravodajských činností,“ a zejména rozšiřuje určitou ochranu osobních informací, které požívali pouze osoby USA, i na osoby, které nejsou osobami USA.
- Agentury přijaly a zveřejnily postupy provádějící směrnici PPD-28.

Je zjevné, že se tyto stanovené postupy a ochranná opatření vztahují i na štít na ochranu soukromí. Jsou-li údaje předány podnikům ve Spojených státech v souladu se štítem na ochranu soukromí nebo jakýmkoli jiným způsobem, mohou si je zpravodajské agentury Spojených států od uvedených podniků vyžádat pouze v případě, že je jejich žádost v souladu se zákonem FISA nebo je předložena v souladu se zákonnými ustanoveními pro příkaz k vydání informací z důvodu národní bezpečnosti (*National Security Letter*), o nichž se hovoří dále (¹). Navíc aniž by se tímto potvrzovaly nebo vyvracely zprávy médií, podle kterých zpravodajská komunita Spojených států údajně shromažďuje údaje přenášené transatlantickými kabely do Spojených států, pokud by zpravodajská komunita Spojených států skutečně údaje z transatlantických kabelů shromažďovala, činila by tak v souladu s omezeními a ochrannými opatřeními zde uvedenými, včetně požadavků směrnice PPD-28.

b. Omezení shromažďování informací

PPD-28 stanovuje několik důležitých obecných zásad, kterými se shromažďování informací prostřednictvím signálového zpravodajství řídí:

- Shromažďování informací prostřednictvím signálového zpravodajství musí být povoleno zákonem nebo prezidentským povolením a musí se provádět v souladu s ústavou a právem.
- Ochrana soukromí a občanských svobod musí tvořit nedílnou součást plánování signálových zpravodajských činností.
- Signálové zpravodajství shromažďuje informace pouze v případě, kdy k tomu existují oprávněné důvody z hlediska zpravodajských služeb v zahraničí nebo kontrarozvědky.
- Spojené státy nebudou shromažďovat informace prostřednictvím signálového zpravodajství proto, aby potlačovaly nebo obtěžovaly osoby, které je kritizují či s nimi nesouhlasí.
- Spojené státy nebudou shromažďovat informace prostřednictvím signálového zpravodajství proto, aby znevýhodňovaly osoby na základě jejich etnické příslušnosti, rasy, pohlaví, sexuální orientace nebo náboženství.
- Spojené státy nebudou shromažďovat informace prostřednictvím signálového zpravodajství proto, aby poskytovaly konkurenční obchodní výhody společností a podnikatelskému odvětví ze Spojených států.
- Signálové zpravodajské činnosti Spojených států musí být vždy v nejvyšší možné míře uzpůsobeny na míru a musí zohledňovat dostupnost jiných zdrojů informací. To mimo jiné znamená, že kdykoli je to možné, provádí se shromažďování informací prostřednictvím signálové zpravodajské činnosti cíleně, a nikoli hromadně.

Požadavek, aby byly signálové zpravodajské činnosti „v nejvyšší možné míře uzpůsobeny na míru“, se vztahuje na způsob shromažďování informací, ale i na to, co se skutečně shromažďuje. Například při stanovování toho, zda

(¹) Donucovací orgány nebo regulační agentury mohou od společností požadovat informace pro účely vyšetřování ve Spojených státech na základě jiných trestněprávních, občanskoprávních a regulačních pravomocí, které stojí mimo oblast působnosti tohoto dokumentu, jenž se omezuje na pravomoci na poli národní bezpečnosti.

shromažďovat informace prostřednictvím signálových zpravodajských činností, musí zpravodajská komunita zvážit dostupnost jiných informací, včetně diplomatických nebo veřejných zdrojů, a dát přednost těmto prostředkům, pokud je to vhodné a proveditelné. Postupy prvků zpravodajské komunity by měly navíc vyžadovat, aby se, pokud je to možné, shromažďování zaměřilo na konkrétní cíle nebo témata zahraničního zpravodajství, a to prostřednictvím využití diskriminantů (např. konkrétní prostředky, selekční termíny a identifikátory).

Je důležité nahlížet na informace poskytnuté Komisi jako na celek. Rozhodnutí o tom, co je „možné“ nebo „proveditelné“, není na uvážení fyzických osob, ale podléhá postupům, které agentury vydaly v souladu se směrnicí PPD-28 a které byly zpřístupněny veřejnosti, i dalším postupům popsáním v uvedené směrnici ⁽¹⁾. Ve směrnici PPD-28 se uvádí, že hromadným shromažďováním informací prostřednictvím signálových zpravodajských služeb je shromažďování, které „se z technických či provozních důvodů provádí bez využití diskriminantů (např. specifické identifikátory, selekční termíny atd.)“. Směrnice PPD-28 v tomto ohledu uznává, že prvky zpravodajské komunity za určitých okolností musí prostřednictvím signálového zpravodajství shromažďovat hromadné informace, aby mohly stanovit nová nebo vznikající nebezpečí a další informace životně důležité pro národní bezpečnost, které jsou často skryty v rozsáhlém a složitém systému moderních celosvětových komunikací. Rovněž uznává obavy týkající se soukromí a občanských svobod při shromažďování hromadných informací ze signálového zpravodajství. Směrnice PPD-28 tudíž vede zpravodajskou komunitu k tomu, aby upřednostňovala jiné možnosti, které by umožnily provádět cílené, nikoli hromadné signálové zpravodajství. V souladu s tím by měly prvky zpravodajské komunity vždy, když je to možné, provádět zacílené, nikoli hromadné signálové zpravodajské činnosti. ⁽²⁾ Tyto zásady zajistí, aby se z výjimečného hromadného shromažďování nestalo obecné pravidlo.

Pojem „přiměřenost“ je základní zásadou práva Spojených států. Znamená, že po prvcích zpravodajské komunity nebude vyžadováno, aby přijaly opatření, jež jsou možná teoreticky, ale že své úsilí o ochranu oprávněných zájmů v oblasti soukromí a občanských svobod budou muset vyvažovat s praktickými potřebami signálových zpravodajských činností. I zde jsou k dispozici postupy agentur, které mohou zajistit, aby formulace „přiměřeně navrženy tak, aby minimalizovaly šíření a uchovávání osobních informací“ nepodřývala obecné pravidlo.

PPD-28 taktéž stanoví, že informace hromadně shromažďované prostřednictvím signálového zpravodajství lze využívat pouze k šesti konkrétním účelům: ke zjišťování určitých činností cizích mocností a k boji proti těmto činnostem, k boji proti terorismu, k boji proti šíření zbraní hromadného ničení, k zajištění kybernetické bezpečnosti, ke zjišťování ohrožení ozbrojených sil Spojených států nebo spojenců a k boji proti těmto nebezpečím a k boji proti hrozbám mezinárodní trestné činnosti, včetně vyhýbání se postihům. Poradce prezidenta pro národní bezpečnost po konzultaci s ředitelem národních zpravodajských služeb tato přijatelná využití informací shromažďovaných hromadně prostřednictvím signálového zpravodajství každoročně přezkoumá, aby se zjistilo, zda by se neměla změnit. Ředitel národních zpravodajských služeb tento seznam v nejvyšší možné míře zveřejní v souladu s národní bezpečností. To představuje významné a transparentní omezení využití informací shromažďovaných hromadně prostřednictvím signálového zpravodajství.

Navíc prvky zpravodajské komunity, které provádějí směrnici PPD-28, posílily stávající analytické postupy a normy pro dotazování v nevyhodnocených informacích ze signálového zpravodajství ⁽³⁾. Analytici musí své dotazování nebo jiné termíny a techniky vyhledávání strukturovat, aby zajistili, že jsou vhodné pro určení zpravodajských informací relevantních pro oprávněné úkoly v rámci činností zahraničního zpravodajství či prosazování práva. Za tímto účelem musí prvky zpravodajské komunity zaměřit své dotazování ohledně osob na kategorie informací ze signálového zpravodajství, které přísluší požadavkům zahraničního zpravodajství nebo prosazování práva, tak aby se předešlo využívání osobních informací, jež jejich požadavkům nepřísluší.

Je důležité zdůraznit, že veškeré činnosti hromadného shromažďování informací týkající se internetové komunikace, které zpravodajská komunita Spojených států vykonává prostřednictvím signálového zpravodajství, probíhají v malé části internetu. Navíc zacílené dotazování, jak je popsáno výše, zajišťuje, že analytikům jsou ke zkoumání vždy předloženy pouze informace, které jsou potenciálně zpravodajsky hodnotné. Účelem těchto omezení je chránit soukromí a občanské svobody všech osob bez ohledu na jejich státní příslušnost nebo místo pobytu.

⁽¹⁾ Dostupné zde www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Těmito postupy se pojetí zacíleného a na míru uzpůsobeného shromažďování informací, o nichž se hovoří v tomto dopise, provádí způsobem, který je specifický pro jednotlivé prvky zpravodajské komunity.

⁽²⁾ Jako jeden příklad za všechny lze citovat postupy NSA, kterými se provádí směrnice PPD-28 a ve kterých se uvádí: „Kdykoli je to možné, provádí se sběr informací prostřednictvím využití jednoho nebo více selekčních termínů, aby se bylo možno soustředit na konkrétní cíle zahraničního zpravodajství (např. konkrétního známého mezinárodního teroristu či teroristickou skupinu) nebo konkrétní témata zahraničního zpravodajství (např. šíření zbraní hromadného ničení cizí mocností či jejími agenty).“

⁽³⁾ Dostupné zde http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Spojené státy mají propracované postupy pro zajištění toho, že se signálové zpravodajské činnosti provádějí pouze za účelem plnění přiměřených cílů národní bezpečnosti. Po rozsáhlém formálním meziagenturním postupu stanovuje prezident každý rok nejvyšší státní priority pro shromažďování zahraničních zpravodajských informací. Ředitel národních zpravodajských služeb zodpovídá za to, aby tyto zpravodajské priority byly převedeny do rámce národních zpravodajských priorit (*National Intelligence Priorities Framework*, NIPF). Směrnice PPD-28 posílila a vylepšila meziagenturní postup tak, aby se zajistil přezkum a schválení všech zpravodajských priorit zpravodajské komunity tvůrci politik na vysoké úrovni. Další pokyny k rámci národních zpravodajských priorit stanoví směrnice 204 o zpravodajské komunitě, která byla v lednu 2015 aktualizována tak, aby zahrnovala požadavky směrnice PPD-28⁽¹⁾. Ačkoli je rámec národních zpravodajských priorit důvěrný, informace týkající se konkrétních priorit činností zahraničního zpravodajství Spojených států se každoročně promítají do neutajovaného dokumentu ředitele národních zpravodajských služeb s názvem Posouzení celosvětových hrozeb (*Worldwide Threat Assessment*), který je také k dispozici na internetových stránkách ODNI.

Priority jsou v rámci národních zpravodajských priorit uvedeny poměrně vysoce obecně. Zahrnují témata, jako je sledování kapacit jaderných a balistických střel konkrétních zahraničních protivníků, účinky korupce drogových kartelů a porušování lidských práv v konkrétních zemích. A nevztahují se jen na signálové zpravodajství, ale na veškeré zpravodajské činnosti. Organizace, která zodpovídá za to, aby se priority rámce národních zpravodajských priorit promítly do skutečného shromažďování informací prostřednictvím signálového zpravodajství, se nazývá Výbor pro národní signálové zpravodajství (*National Signals Intelligence Committee*, SIGCOM). Působí pod záštitou ředitele Národní bezpečnostní agentury (*National Security Agency*, NSA), který je pověřen výkonným dekretem 12333 jako „funkční manažer pro signálové zpravodajství“ a pod dohledem ministra obrany a ředitele národních zpravodajských služeb zodpovídá za dohled nad signálovým zpravodajstvím napříč zpravodajskou komunitou a za jeho koordinaci. Ve Výboru pro národní signálové zpravodajství jsou zastoupeny všechny prvky zpravodajské komunity, a až Spojené státy provedou směrnici PPD-28 v plném rozsahu, budou v něm zastoupena také další ministerstva a agentury se zájmem na politice týkající se signálového zpravodajství.

Všechny ministerstva a agentury Spojených států, které čerpají z činností zahraničního zpravodajství, předkládají své žádosti o shromažďování informací Výboru pro národní signálové zpravodajství. Výbor tyto žádosti přezkoumá, zajistí, aby byly v souladu s rámcem národních zpravodajských priorit, a udělí jim prioritu na základě například těchto kritérií:

- Může signálové zpravodajství poskytnout v tomto případě užitečné informace, nebo pro splnění daného požadavku existují lepší či hospodárnější zdroje informací, jako satelitní snímky nebo informace z otevřených zdrojů?
- Do jaké míry jsou tyto informace nezbytně nutné? Jde-li o vysokou prioritu v rámci národních zpravodajských priorit, nejčastěji půjde také o vysokou prioritu v signálovém zpravodajství.
- Jaký druh signálového zpravodajství by mohl být využit?
- Je shromažďování informací co nejvíce uzpůsobeno na míru? Měla by zde existovat časová, zeměpisná nebo jiná omezení?

Postup Spojených států pro vyřizování požadavků na signálové zpravodajství také vyžaduje výslovné zvážení dalších faktorů, jmenovitě:

- Jsou cíl nebo metodika shromažďování informací obzvláště citlivé? Pokud ano, bude zapotřebí přezkum vysoce postavenými tvůrci politik.
- Bude shromažďování informací představovat bezdůvodné ohrožení soukromí a občanských svobod, bez ohledu na státní příslušnost?
- Jsou zapotřebí dodatečná ochranná opatření proti šíření a uchovávání informací, aby se ochránilo soukromí nebo zájmy národní bezpečnosti?

Nakonec na závěr postupu školený personál NSA na základě priorit ověřených Výborem pro národní signálové zpravodajství vyhledá a určí konkrétní selekční termíny, jako jsou například telefonní čísla nebo e-mailové adresy, u nichž se předpokládá, že se jejich prostřednictvím získají zahraniční zpravodajské informace odpovídající těmto prioritám. Všechny zvolené termíny musí být před zadáním do systémů Národní bezpečnostní agentury pro shromažďování informací přezkoumány a schváleny. I poté však to, zda a kdy se shromažďování opravdu uskuteční, bude částečně

⁽¹⁾ Dostupné zde <http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf>.

záviset na dalších faktorech, jako je například dostupnost vhodných zdrojů pro shromažďování. Tento postup zajišťuje, že cíle shromažďování informací prostřednictvím signálového zpravodajství ze strany Spojených států odrážejí oprávněné a důležité potřeby zahraničního zpravodajství. A samozřejmě, pokud se shromažďování provádí podle zákona FISA, musí NSA a další agentury dodržovat dodatečná omezení schválená Soudem pro uplatňování zákona FISA. Stručně řečeno, ani Národní bezpečnostní agentura, ani žádná jiná zpravodajská agentura Spojených států o tom, co shromažďuje, nerozhoduje sama.

Tento postup zajišťuje, že všechny zpravodajské priority Spojených států jsou stanovovány vysoce postavenými tvůrci politik, kteří dokáží nejlépe určit požadavky pro zahraniční zpravodajské činnosti Spojených států a kteří zohledňují nejen potenciální hodnotu shromážděných zpravodajských informací, ale také rizika související s tímto shromažďováním, včetně ohrožení soukromí, národohospodářských zájmů a zahraničních vztahů.

Pokud jde o údaje předávané do Spojených států v souladu se štítem na ochranu soukromí, pak přesto, že Spojené státy nemohou potvrdit ani vyvrátit konkrétní zpravodajské metody nebo operace, vztahují se požadavky směrnice PPD-28 na veškeré signálové zpravodajské operace prováděné Spojenými státy, bez ohledu na typ či zdroj shromažďovaných údajů. Dále omezení a ochranná opatření vztahující se na shromažďování informací prostřednictvím signálového zpravodajství se týkají informací shromažďovaných signálovým zpravodajstvím pro jakékoli povolené účely, včetně účelů jak zahraniční, tak vnitrostátní bezpečnosti.

Postupy popsané výše ukazují jasné odhodlání předcházet svévolnému a nahodilému shromažďování informací prostřednictvím signálového zpravodajství a naplňovat – od nejvyšších úrovní naší vlády – zásadu přiměřenosti. Směrnice PPD-28 a prováděcí postupy agentur vyjasňují nová i stávající omezení a konkrétněji popisují účel, pro nějž Spojené státy shromažďují a využívají informace ze signálového zpravodajství. Měly by tak dále ujistit, že činnosti signálového zpravodajství jsou a nadále budou prováděny pouze pro oprávněné účely zahraničních zpravodajských činností.

c. Omezení uchovávání a šíření informací

Paragraf 4 směrnice PPD-28 vyžaduje, aby každý prvek zpravodajské komunity měl výslovná omezení pro uchovávání a šíření osobních informací o osobách, které nejsou osobami USA, shromážděných prostřednictvím signálového zpravodajství, která jsou srovnatelná s omezeními pro státní příslušníky Spojených států. Tato pravidla jsou začleněna do postupů pro jednotlivé zpravodajské agentury, které byly vydány v únoru 2015 a jsou veřejně dostupné. Aby bylo možné osobní informace získané prostřednictvím zahraniční zpravodajské činnosti uchovávat či šířit, musely být získány na základě schváleného zpravodajského požadavku, jak stanoví výše popsáný postup podle NIPF, musí existovat důvodné podezření, že jde o důkaz trestného činu, nebo musí splňovat jednu z dalších norem pro uchovávání informací o osobách USA, které jsou uvedeny v § 2.3 výkonného dekretu 12333.

Informace, pro které nic z toho neplatí, nemohou být uchovávány déle než 5 let, pokud ředitel národních zpravodajských služeb výslovně neuvede, že je jejich další uchovávání v zájmu národní bezpečnosti Spojených států. Prvky zpravodajské komunity tudíž musí informace shromážděné o osobách, které nejsou osobami USA, prostřednictvím signálového zpravodajství vymazat pět let po jejich shromáždění, pokud například nebylo stanoveno, že jde o informaci důležitou pro schválený požadavek na činnost zahraničního zpravodajství, nebo pokud ředitel národních zpravodajských služeb po zvážení stanoviska úředníka ODNI pro ochranu občanských svobod a pracovníků dalších agentur pro ochranu soukromí a občanských svobod nestanoví, že je jejich další uchovávání v zájmu národní bezpečnosti.

Navíc všechny postupy agentur, kterými se provádí směrnice PPD-28, nyní výslovně vyžadují, že informace o osobách nesmějí být šířeny pouze na základě toho, že jde o osobu, která není osobou USA, a Úřad ředitele národních zpravodajských služeb vydal směrnici pro všechny prvky zpravodajské komunity⁽¹⁾, aby tento požadavek zohlednily. Po pracovnících zpravodajské komunity se výslovně požaduje, aby při vypracovávání a šíření zpravodajských zpráv brali v potaz zájmy ochrany soukromí osob, které nejsou osobami USA. Zejména informace shromážděné prostřednictvím signálového zpravodajství o pravidelných činnostech cizího státního příslušníka by se sama o sobě nepovažovala za zahraniční zpravodajství, které by bylo možno šířit nebo trvale uchovávat, jestliže jinak neodpovídá schválenému požadavku na činnost zahraničního zpravodajství. To představuje uznání významného omezení a odpověď na obavy Evropské komise ohledně širší vymezení činností zahraničního zpravodajství, jak je stanoveno ve výkonném dekretu 12333.

⁽¹⁾ Intelligence Community Directive (ICD) 203, dostupné zde <http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf>.

d. Soulad s předpisy a dohled

Systém dohledu nad zahraničním zpravodajstvím Spojených států poskytuje přísný víceúrovňový dohled, aby se zajistilo dodržování příslušných zákonů a postupů, včetně těch, které se týkají shromažďování, uchovávání a šíření informací o osobách, které nejsou osobami USA, získaných prostřednictvím signálového zpravodajství, jak je stanoveno ve směrnici PPD-28. Pokud jde o systém dohledu:

- Zpravodajská komunita zaměstnává stovky pracovníků dohledu. Jen samotná NSA má více než 300 lidí, kteří se věnují souladu s předpisy, a jiné prvky také mají kanceláře dohledu. Rozsáhlý dohled nad zpravodajskými činnostmi navíc zajišťuje ministerstvo spravedlnosti a určitý dohled zajišťuje i ministerstvo obrany.
- Každý prvek zpravodajské komunity má svou vlastní kancelář generálního inspektora odpovědnou mj. za dohled nad zahraničními zpravodajskými činnostmi. Generální inspektoři jsou ze zákona nezávislí, mají širokou pravomoc vést vyšetřování, audity a přezkumy programů, včetně podvodů a zneužívání nebo porušování zákona, a mohou doporučovat nápravná opatření. Doporučení generálního inspektora jsou sice nezávazná, jeho zprávy se však často zveřejňují a v každém případě se předkládají Kongresu, což zahrnuje následné zprávy, pokud nápravné kroky doporučené v předchozích zprávách dosud nebyly dokončeny. Kongres je tudíž informován o všech případech nesouladu a může vyvíjet tlak, a to i prostřednictvím rozpočtových opatření, aby dosáhl nápravných kroků. Byla zveřejněna řada zpráv generálních inspektorů o zpravodajských programech ⁽¹⁾.
- Kancelář ODNI pro občanské svobody a ochranu soukromí (CLPO) je pověřena zajišťováním toho, aby zpravodajská komunita fungovala tak, aby pomáhala národní bezpečnosti a zároveň chránila občanské svobody a práva na soukromí. ⁽²⁾ Ostatní prvky zpravodajské komunity mají své vlastní úředníky pro ochranu soukromí.
- Výbor pro dohled nad respektováním soukromí a občanských svobod (*Privacy and Civil Liberties Oversight Board*, PCLOB) je nezávislý zákonem zřízený orgán, který je pověřen analyzováním a přezkoumáváním protiteroristických programů a politik, včetně využívání signálového zpravodajství, aby se zajistilo, že odpovídajícím způsobem chrání soukromí a občanské svobody. Vydal několik veřejných zpráv o zpravodajských činnostech.
- Jak je podrobněji uvedeno níže, Soud pro uplatňování zákona FISA, který tvoří nezávislí federální soudci, zodpovídá za dohled nad veškerými činnostmi shromažďování informací prostřednictvím signálového zpravodajství prováděnými podle zákona FISA a za jejich soulad s uvedeným zákonem.
- A konečně Kongres Spojených států, přesněji řečeno výbory pro zpravodajství a pro soudnictví Sněmovny a Senátu, mají významné dohledové pravomoci, co se týče všech zahraničních zpravodajských činností Spojených států, včetně signálového zpravodajství Spojených států.

Vedle těchto formálních mechanismů dohledu má zpravodajská komunita zavedeno množství mechanismů pro zajištění svého souladu s omezeními shromažďování, jak je popsáno výše. Například:

- Každý rok musí jejich požadavky na signálové zpravodajství potvrzovat vládní úředníci.
- NSA kontroluje cíle signálového zpravodajství v průběhu celého postupu shromažďování, aby stanovila, zda skutečně poskytují zahraničnímu zpravodajství hodnotné informace, které odpovídají prioritám, a pokud je nepřinášejí, jejich sledování zastaví. Další postupy zaručují, aby byly selekční termíny pravidelně přezkoumávány.

⁽¹⁾ Viz např. dokument U.S. Department of Justice Inspector General Report „A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008“ (September 2012), k dispozici zde <https://oig.justice.gov/reports/2016/o1601a.pdf>.

⁽²⁾ Viz www.dni.gov/clpo.

- Na základě doporučení nezávislé přezkumné skupiny jmenované prezidentem Obamou stanovil ředitel národních zpravodajských služeb nový mechanismus pro sledování shromažďování a šíření informací ze signálového zpravodajství, jejichž cíl nebo způsob shromažďování je obzvláště citlivý, aby se zajistilo, že jsou v souladu s tím, co stanovili tvůrci politik.
- A konečně ODNI každoročně přezkoumává přidělení zdrojů zpravodajské komunity ve srovnání s prioritami rámce národních zpravodajských priorit a posílání zpravodajství jako celku. Tento přezkum zahrnuje posouzení hodnoty všech druhů shromažďování zpravodajských informací, včetně signálového zpravodajství, a hledí jak do minulosti – jak úspěšně se zpravodajská komunita zhostila svých úkolů? –, tak do budoucnosti – co bude zpravodajská komunita potřebovat v budoucnosti? To zaručí, že se zdroje signálového zpravodajství využijí pro nejvýznamnější národní priority.

Jak dokazuje tento komplexní přehled, zpravodajská komunita sama nerozhoduje o tom, které konverzace má odposlouchávat, nesnaží se shromažďovat veškeré informace ani nepůsobí bez dohledu. Jejich činnosti se zaměřují na priority stanovené tvůrci politik, a to prostřednictvím postupu, který zahrnuje vstupy napříč vládou a nad kterým je vykonáván dohled jak v rámci NSA, tak ze strany ODNI, ministerstva spravedlnosti a ministerstva obrany.

Směrnice PPD-28 také obsahuje mnoho dalších ustanovení pro zajištění toho, že osobní informace shromažďované prostřednictvím signálového zpravodajství jsou chráněny, bez ohledu na státní příslušnost. Směrnice PPD-28 například upravuje postupy pro zabezpečení údajů, pro přístup k nim a pro jejich kvalitu, aby byly osobní informace shromažďované prostřednictvím signálového zpravodajství chráněny, a ukládá také povinnou odbornou přípravu, aby se zajistilo, že personál chápe odpovědnost chránit osobní informace bez ohledu na státní příslušnost. PPD také upravuje mechanismy dodatečného dohledu a souladu s předpisy. Ty zahrnují pravidelný audit a přezkumy příslušnými úředníky pro dohled a soulad, pokud jde o postupy na ochranu osobních informací obsažených v signálovém zpravodajství. Přezkumy také musí zkoumat soulad agentur s postupy na ochranu takových informací.

Směrnice PPD-28 navíc stanoví, že významné otázky souladu s předpisy týkající se osob, které nejsou osobami USA, budou řešeny na vysoké vládní úrovni. Pokud vyvstane významný problém ohledně souladu týkající se osobních informací jakékoli osoby, které byly shromažďovány v důsledku činností signálového zpravodajství, musí být takový problém kromě splnění již existujících požadavků na předkládání zpráv také okamžitě nahlášen řediteli národních zpravodajských služeb. Týká-li se problém osobních informací osoby, která není osobou USA, pak ředitel národních zpravodajských služeb po konzultaci s ministrem zahraničí a s ředitelem příslušného prvku zpravodajské komunity stanoví, zda by měly být učiněny kroky pro informování příslušné cizí vlády, při dodržení ochrany zdrojů a metod a personálu Spojených států. Navíc, jak nařizuje směrnice PPD-28, ministr zahraničí určil vysoce postaveného úředníka, tajemnici ministra Catherine Novelliovou, která slouží jako kontaktní osoba pro cizí vlády, jež chtějí vznést dotazy v souvislosti se signálovými zpravodajskými činnostmi Spojených států. Tento závazek k zapojení na vysoké úrovni dokládá úsilí vynaložené vládou Spojených států v několika uplynulých letech na získání důvěry v četná a překrývající se opatření zavedená na ochranu informací o osobách USA i i osobách, které nejsou osobami USA.

e. Shrnutí

Postupy Spojených států pro shromažďování, uchovávání a šíření informací získaných zahraniční zpravodajskou činností poskytují důležitou ochranu soukromí pro osobní informace o všech osobách, bez ohledu na státní příslušnost. Tyto postupy zejména zajišťují, že se naše zpravodajská komunita zaměřuje na své poslání chránit národní bezpečnost, jak jí povolují příslušné zákony, výkonné dekrety a prezidentské směrnice, že ochraňuje informace před nepovoleným přístupem, použitím a zveřejněním, a že své činnosti vykonává pod několika úrovněmi přezkumu a dohledu, včetně přezkumu a dohledu vykonávaného dohledovými výbory Kongresu. Směrnice PPD-28 a její prováděcí postupy představují naše úsilí o rozšíření určité minimalizace a dalších podstatných zásad ochrany údajů na osobní informace všech osob bez ohledu na jejich státní příslušnost. Osobní informace získané shromažďováním informací prostřednictvím signálového zpravodajství Spojených států podléhají zásadám a požadavkům zákonů a prezidentských směrnic Spojených států, včetně ochranných opatření stanovených ve směrnici PPD-28. Tyto zásady a požadavky zajišťují, aby bylo se všemi osobami zacházeno důstojně a s respektem, bez ohledu na jejich státní příslušnost nebo místo pobytu, a uznávají, že všechny osoby mají oprávněný zájem na ochraně svého soukromí, když se nakládá s jejich osobními údaji.

II. ZÁKON O DOHLEDU NAD ZAHRANIČNÍMI ZPRAVODAJSKÝMI ČINNOSTMI – § 702

Shromažďování podle § 702 zákona o dohledu nad zahraničními zpravodajskými činnostmi ⁽¹⁾ není „masivní a nahodilé“, nýbrž je úzce zaměřené na shromažďování zahraničního zpravodajství od jednotlivě stanovených oprávněných cílů, je jednoznačně schváleno povolením vydaným na základě výslovné zákonné pravomoci a podléhá jak nezávislému soudnímu dohledu, tak podstatnému přezkumu a dohledu ze strany výkonné moci a Kongresu. Sběr údajů podle § 702 se považuje za signálové zpravodajství podléhající požadavkům směrnice PPD-28 ⁽²⁾.

Shromažďování podle § 702 je jedním z nejcennějších zpravodajských zdrojů, který chrání jak Spojené státy, tak naše evropské partnery. Rozsáhlé informace o fungování a dohledu podle § 702 jsou veřejně dostupné. Četná soudní podání, soudní rozhodnutí a zprávy o dohledu týkající se programu byly odtajněny a zveřejněny na internetových stránkách ODN: www.icontherecord.tumblr.com. Paragraf 702 byl navíc komplexně analyzován ve zprávě PCLOB, která je k dispozici na adrese <https://www.pclob.gov/library/702-Report.pdf> ⁽³⁾.

Paragraf 702 byl po rozsáhlé veřejné rozpravě v Kongresu přijat jako součást zákona *FISA Amendments Act of 2008* ⁽⁴⁾. Povoluje se jím získávání zahraničních zpravodajských informací prostřednictvím zacílení na osoby, které nejsou osobami USA a jsou mimo území Spojených států, s povinnou pomocí poskytovatelů elektronických komunikačních služeb ze Spojených států. Podle § 702 ministr spravedlnosti a ředitel národních zpravodajských služeb – dva představitelé na vládní úrovni jmenovaní prezidentem a potvrzení Senátem – předkládají každoročně Soudu pro uplatňování zákona FISA certifikace ⁽⁵⁾. V těchto certifikacích jsou specifikovány kategorie zahraničních zpravodajských informací, které mají být shromažďovány, jako například zpravodajství týkající se boje proti terorismu nebo zbraní hromadného ničení, jež musí patřit do kategorií definovaných v zákonu FISA ⁽⁶⁾. Jak uvedl výbor PCLOB, „[t]ato omezení neumožňují neomezené shromažďování informací o cizincích“ ⁽⁷⁾.

Certifikace také musí zahrnovat postupy pro „cílení“ a „minimalizaci“, které musí Soud pro uplatňování zákona FISA přezkoumat a schválit ⁽⁸⁾. Postupy pro zacílení mají zajišťovat, aby shromažďování probíhalo pouze tak, jak je povoleno zákonem, a aby spadalo do rozsahu certifikací; postupy pro minimalizaci mají omezovat získávání, šíření a uchovávání informací o osobách USA, obsahují však také ustanovení, která rovněž poskytují podstatnou ochranu informací o osobách, které nejsou osobami USA, jak je popsáno níže. Navíc, jak je popsáno výše, prezident ve směrnici PPD-28 nařídil, aby zpravodajská komunita poskytovala dodatečnou ochranu osobním informacím osob, které nejsou osobami USA, a tato ochrana se vztahuje na informace shromažďované podle § 702.

Jakmile soud postupy pro zacílení a minimalizaci schválí, neprobíhá shromažďování podle § 702 hromadně nebo nahodile, nýbrž „spočívá zcela v sledování konkrétních osob, o kterých bylo učiněno individualizované zjištění“, jak prohlásil výbor PCLOB ⁽⁹⁾. Shromažďování je zacíleno prostřednictvím využití individuálních selekčních termínů, jako

⁽¹⁾ 50 U.S.C. § 1881a.

⁽²⁾ Spojené státy mohou také v souladu s jinými ustanoveními zákona FISA získat soudní příkaz k předložení údajů, včetně údajů předaných podle štítu na ochranu soukromí. Viz 50 U.S.C. § 1801 a násl. Ustanovení hlavy I, která povoluje elektronické sledování, a hlavy III, jež povoluje fyzické prohlídky, zákona FISA vyžadují soudní příkaz (s výjimkou mimořádných okolností) a vždy požadují důvodné podezření k tomu, aby se bylo možno domnívat, že cílem je cizí mocnost nebo agent cizí mocnosti. Hlava IV zákona FISA 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*) povoluje na základě soudního příkazu (s výjimkou mimořádných okolností) ve schválených vyšetřováních v oblasti zahraničního zpravodajství, kontrarozvědky či boje proti terorismu. Hlava V zákona FISA povoluje, aby úřad FBI v souladu se soudním příkazem (s výjimkou mimořádných okolností) získával obchodní záznamy, které jsou důležité pro vyšetřování v oblasti zahraničního zpravodajství, kontrarozvědky nebo boje proti terorismu. Jak je uvedeno níže, zákon *USA FREEDOM Act* výslovně zakazuje využívat zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení nebo příkazy k hromadnému shromažďování informací z obchodních záznamů podle zákona FISA pro hromadné shromažďování informací a ukládá požadavek na „konkrétní selekční termíny“, aby se zajistilo cílené využívání povolení.

⁽³⁾ Privacy and Civil Liberties Board, „Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act“ (July 2, 2014) („PCLOB Report“).

⁽⁴⁾ Viz Pub. L. No. 110-261, 122 Stat. 2436 (2008).

⁽⁵⁾ Viz 50 U.S.C. § 1881a(a) and (b).

⁽⁶⁾ Viz *tamtéž* § 1801(e).

⁽⁷⁾ Viz PCLOB Report, s. 99.

⁽⁸⁾ Viz 50 U.S.C. § 1881a(d), (e).

⁽⁹⁾ Viz PCLOB Report, s. 111.

jsou e-mailové adresy nebo telefonní čísla, u nichž pracovníci zpravodajských služeb Spojených států stanovili, že jsou pravděpodobně využívány pro sdělování zahraničních zpravodajských informací typu, na který se vztahuje certifikace předložená soudu⁽¹⁾. Základ pro selekci cíle musí být podložen dokumenty a dokumentace pro každý zvolený termín je následně přezkoumána ministerstvem spravedlnosti⁽²⁾. Vláda USA zveřejnila informace, které ukazují, že v roce 2014 bylo podle § 702 zacíleno přibližně 90 000 osob, což je nepatrný zlomek z více než 3 miliard uživatelů internetu na celém světě⁽³⁾.

Informace shromážděné podle § 702 podléhají soudem schváleným postupům pro minimalizaci, které poskytují ochranu osobám, které nejsou osobami USA, i osobám USA a které byly zveřejněny⁽⁴⁾. Komunikace získaná podle § 702 se například uchovává v databázích s přísnou kontrolou přístupu, bez ohledu na to, zda se týká osob USA nebo osob, které nejsou osobami USA. Mohou ji zkoumat pouze zpravodajští pracovníci, kteří prošli odbornou přípravou ohledně postupů pro minimalizaci týkající se ochrany soukromí a kterým byl přístup schválen specificky pro plnění jejich povolených funkcí⁽⁵⁾. Využití údajů se omezuje na stanovení zahraničních zpravodajských informací nebo důkazů trestného činu⁽⁶⁾. V souladu se směrnicí PPD-28 lze tyto informace šířit, pouze pokud je k tomu oprávněný důvod zahraničního zpravodajství nebo prosazování práva; skutečnost, že jednou ze stran komunikace není osoba USA, není sama o sobě dostačující⁽⁷⁾. A postupy pro minimalizaci a směrnice PPD-28 také stanovují lhůty pro uchovávání údajů získaných podle § 702⁽⁸⁾.

Dohled podle § 702 je rozsáhlý a provádějí jej všechny tři složky moci v našem státě. Agentury, které tento předpis provádějí, mají několik úrovní interních přezkumů, včetně přezkumu nezávislými generálními inspektory a technologických kontrol nad přístupem k údajům. Ministerstvo spravedlnosti a ODNI důkladně zkoumají a kontrolují použití § 702, aby ověřily soulad s právními pravidly; agentury rovněž mají nezávislou povinnost informovat o možných případech nesouladu. Tyto případy jsou vyšetřovány a všechny nežádoucí příhody s dodržováním předpisů jsou nahlášený Soudem pro uplatňování zákona FISA, prezidentově Výboru pro dohled nad zpravodajstvím a Kongresu a jsou příslušným způsobem napraveny⁽⁹⁾. Dosud k žádným případům záměrných pokusů o porušení zákona nebo obcházení zákonných požadavků nedošlo⁽¹⁰⁾.

Významnou roli hraje při provádění § 702 Soud pro uplatňování zákona FISA. Je tvořen nezávislými federálními soudci, kteří jako všichni ostatní federální soudci vykonávají funkci soudce doživotně, ale u tohoto soudu působí pouze po dobu sedmi let. Jak je uvedeno výše, soud musí přezkoumávat, zda jsou každoroční certifikace a postupy pro zacílení a minimalizaci v souladu se zákonem. Navíc, jak je také uvedeno výše, musí vláda soud neprodleně uvědomit o problémech s dodržováním⁽¹¹⁾; již bylo odtajněno a zveřejněno několik stanovisek soudu, která ukazují mimořádnou úroveň soudní kontroly a nezávislosti při přezkumu takových případů.

Bývalý předsedající soudce soudu popsal náročné postupy v dopise Kongresu, který byl zveřejněn⁽¹²⁾. V důsledku zákona USA FREEDOM Act, jak je uvedeno níže, má nyní soud výslovné oprávnění jmenovat externího právníka nezávislým advokátem pro ochranu soukromí v případech, kdy vyvstávají nové nebo významné právní otázky⁽¹³⁾. Takový stupeň zapojení nezávislého soudnictví země do zahraničních zpravodajských činností zaměřených na osoby, které nejsou občany dané země ani se v ní nenacházejí, je neobvyklý, ne-li bezprecedentní a pomáhá zajistit, aby se shromažďování informací podle § 702 uskutečňovalo v příslušných zákonných mezích.

⁽¹⁾ Tamtéž.

⁽²⁾ Tamtéž 8; 50 U.S.C. § 1881a(l); viz také NSA Director of Civil Liberties and Privacy Report, „NSA's Implementation of Foreign Intelligence Surveillance Act Section 702“ (hereinafter „NSA Report“) s. 4, dostupné zde <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

⁽³⁾ Director of National Intelligence 2014 Transparency Report, dostupná zde http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

⁽⁴⁾ Postupy pro minimalizaci jsou dostupné na adrese: <http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf> („NSA Minimization Procedures“); <http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf>; a <http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf>.

⁽⁵⁾ Viz NSA Report s. 4.

⁽⁶⁾ Viz např. NSA Minimization Procedures, s. 6.

⁽⁷⁾ Postupy zpravodajských agentur podle směrnice PPD-28 dostupné zde <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

⁽⁸⁾ Viz NSA Minimization Procedures; § 4 směrnice PPD-28.

⁽⁹⁾ Viz 50 U.S.C. § 1881(l); viz také PCLOB Report, s. 66-76.

⁽¹⁰⁾ Viz Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, s. 2-3, dostupné zde <http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf>

⁽¹¹⁾ Pravidlo 13 Soudu pro uplatňování zákona FISA, dostupné zde <http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

⁽¹²⁾ Dopis Reggie B. Waltona Patricku J. Leahymu ze dne 29. července 2013, s. 2-3. k dispozici zde <http://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

⁽¹³⁾ Viz § 401 USA FREEDOM Act, P.L. 114-23.

Kongres vykonává dohled prostřednictvím ze zákona vyžadovaných zpráv předkládaných výboru pro zpravodajství a výboru pro soudnictví a častých informačních schůzek a slyšení. Ty zahrnují pololetní zprávu ministra spravedlnosti, která dokumentuje použití § 702 a veškeré nežádoucí příhody s dodržováním předpisů ⁽¹⁾, samostatné pololetní posouzení předkládané ministrem spravedlnosti a ředitelem pro národní zpravodajské služby, jež dokládá soulad s postupy pro zacílení a minimalizaci, včetně souladu s postupy vytvořenými pro zajištění toho, aby byly informace shromažďovány pouze v případě, kdy k tomu existují oprávněné důvody z hlediska zahraničních zpravodajských činností ⁽²⁾, a výroční zprávu vedoucích představitelů prvků zpravodajských služeb, která zahrnuje certifikaci, že shromažďování podle § 702 nadále poskytuje zahraniční zpravodajské informace ⁽³⁾.

Krátce řečeno, shromažďování podle § 702 je povoleno zákonem, podléhá několika úrovním přezkumu, soudního dozoru a dohledu, a jak Soud pro uplatňování zákona FISA uvedl v nedávno odtajněném stanovisku, „neprovádí se hromadně nebo nahodile“, nýbrž „prostřednictvím ... samostatných rozhodnutí o zacílení pro jednotlivé [komunikační] prostředky“ ⁽⁴⁾.

III. ZÁKON USA FREEDOM ACT

Zákon *USA FREEDOM Act*, uzákoněný podpisem v červnu 2015, významným způsobem pozměnil dohled Spojených států a další národní bezpečnostní pravomoci a veřejně zprůhladnil užívání těchto pravomocí a rozhodnutí Soudu pro uplatňování zákona FISA, jak je uvedeno níže ⁽⁵⁾. Tento zákon zajišťuje, aby naši pracovníci v oblasti zpravodajství a prosazování práva měli pravomoci, jaké k ochraně národa potřebují, a zároveň aby se dále zajistila řádná ochrana soukromí fyzických osob při uplatňování těchto pravomocí. Posiluje ochranu soukromí a občanských svobod a zvyšuje transparentnost.

Zákon zakazuje hromadné shromažďování jakýchkoli záznamů, včetně záznamů jak o osobách USA, tak o osobách, které nejsou osobami USA, v souladu s několika ustanoveními zákona FISA nebo prostřednictvím *National Security Letter*, což je forma zákonem povoleného správního předvolání ⁽⁶⁾. Tento zákaz výslovně zahrnuje telefonní metadata týkající se hovorů mezi osobami uvnitř Spojených států a osobami mimo Spojené státy a zahrnoval by také shromažďování informací v rámci štítu na ochranu soukromí na základě těchto pravomocí. Zákon vyžaduje, aby vláda každou žádost o záznamy na základě uvedených pravomocí zakládala na „specifickém zvoleném termínu“ – na takovém termínu, který konkrétně identifikuje určitou osobu, účet, adresu nebo osobní zařízení tak, že se tím v co nejvyšší možné přiměřené míře omezí rozsah požadovaných informací ⁽⁷⁾. Toto dále zajistí, aby bylo shromažďování informací pro zpravodajské účely přesně zaměřeno a zacíleno.

Zákon také přinesl významné změny řízení u Soudu pro uplatňování zákona FISA, které jednak zvyšují transparentnost, jednak poskytují dodatečné zajištění ochrany soukromí. Jak je uvedeno výše, povolil vytvoření stálého panelu právníků s bezpečnostní prověrkou, kteří mají zkušenosti v oblasti ochrany soukromí a občanských svobod, shromažďování zpravodajských informací, komunikačních technologií nebo dalších souvisejících oblastí, již mohou být jmenováni pro vystupování před soudem jako *amicus curiae* v případech, které zahrnují významné či novátorské výklady práva. Tito právníci jsou oprávněni přednášet právní argumenty ve prospěch ochrany soukromí a občanských svobod fyzických osob a budou mít přístup k veškerým informacím, včetně utajených informací, které soud uzná za nutné pro výkon jejich služby ⁽⁸⁾.

Tento zákon také staví na bezprecedentní transparentnosti vlády Spojených států ohledně zpravodajských činností tím, že požaduje, aby ředitel národních zpravodajských služeb po konzultaci s ministrem spravedlnosti buď odtajnil všechna rozhodnutí, příkazy nebo stanoviska vydaná Soudem pro uplatňování zákona FISA či přezkumným soudem pro dohled nad zahraničními zpravodajskými činnostmi, která obsahují významné konstrukce nebo výklady jakýchkoli právních ustanovení, či aby zveřejnil jejich neutajovaná shrnutí.

⁽¹⁾ Viz 50 U.S.C. § 1881f.

⁽²⁾ Viz *tamtéž* § 1881a(l)(1).

⁽³⁾ Viz *tamtéž* § 1881a(l)(3). Některé z těchto zpráv jsou tajné.

⁽⁴⁾ Mem. Opinion and Order, s. 26 (FISC 2014), available at <http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

⁽⁵⁾ Viz *USA FREEDOM Act of 2015*, Pub. L. No. 114-23, § 401, 129 Stat. 268.

⁽⁶⁾ Viz *tamtéž* §§ 103, 201, 501. *National Security Letters* jsou povoleny několika zákony a umožňují úřadu FBI získávat informace obsažené v úvěrových zprávách, finančních záznamech, elektronickém odběru a transakčních záznamech určitých druhů společností, a to pouze z důvodu ochrany před mezinárodním terorismem nebo nezákonnými zpravodajskými činnostmi. Viz 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. *National Security Letters* obvykle využívá úřad FBI ke shromažďování kritických informací netýkajících se obsahu v raných fázích vyšetřování v oblasti boje proti terorismu a kontrarozvědky – jde například o totožnost odběratele účtu, který mohl komunikovat s agenty teroristických skupin jako ISIL. Příjemci *National Security Letter* mají právo jej napadnout u soudu. Viz 18 U.S.C. § 3511.

⁽⁷⁾ Viz *tamtéž*.

⁽⁸⁾ Viz *tamtéž* § 401.

Zákon navíc umožňuje rozsáhlá zveřejňování ohledně shromažďování informací podle zákona FISA a žádostí podle *National Security Letters*. Spojené státy musí Kongresu a veřejnosti každý rok mimo jiné informace odhalit také počet požadovaných a získaných příkazů a certifikací podle zákona FISA, odhadované počty osob USA a osob, které nejsou osobami USA, zacílených a dotčených sledováním a počet pověření *amici curiae* ⁽¹⁾. Zákon rovněž vyžaduje, aby vláda navíc veřejně informovala o počtu žádostí na základě *National Security Letter* jak pro osoby USA, tak pro osoby, které nejsou osobami USA ⁽²⁾.

Pokud jde o transparentnost obchodních společností, poskytuje jim zákon řadu možností, jak veřejně informovat o souhrnných počtech příkazů a směrnic podle zákona FISA nebo *National Security Letter*, které obdrží od vlády, jakož i o počtu zákaznických účtů zacílených těmito příkazy ⁽³⁾. Několik společností již tyto informace zveřejnilo a odhalilo tak, že tyto záznamy byly požadovány pouze u omezeného počtu zákazníků.

Tato transparentní hlášení společností dokazují, že se žádosti zpravodajských služeb Spojených států dotýkají pouze nepatrného zlomku údajů. Nedávná zpráva o transparentnosti jedné významné společnosti například ukazuje, že se žádosti z důvodu národní bezpečnosti (na základě zákona FISA nebo *National Security Letter*), které obdržela, týkaly méně než 20 000 jejích účtů v době, kdy měla více než 400 milionů odběratelů. Jinými slovy, všechny požadavky Spojených států z důvodu národní bezpečnosti, které tato společnost uvedla ve zprávě, se dotýkaly méně než 0,005 % jejích odběratelů. Je zřejmé, že i kdyby se všechny tyto požadavky týkaly údajů „bezpečného přístavu“, což tak samozřejmě není, jsou to požadavky zacílené, mají přiměřený rozsah a nejsou hromadné ani nahodilé.

Zákony, kterými se povolují *National Security Letters*, již sice omezovaly okolnosti, za nichž mohlo být adresátovi takového příkazu zakázáno jeho zveřejnění, zákon však dále stanovil, že takový požadavek na nezveřejňování musí být pravidelně přezkoumán; také ukládá, aby adresáti *National Security Letters* byli uvědomeni v případě, kdy skutečnosti již nebudou zavdávat příčinu k požadavku na nezveřejňování, a kodifikuje postupy, jimiž mohou adresáti požadavky na nezveřejnění napadnout. a kodifikuje postupy, jimiž mohou adresáti požadavky na nezveřejnění napadnout ⁽⁴⁾.

Souhrnně řečeno, významné změny v pravomocích zpravodajských služeb Spojených států, které přinesl zákon USA o svobodě, jasně dokazují rozsáhlé úsilí Spojených států přenést ochranu osobních informací, soukromí a občanských svobod a transparentnost do popředí všech zpravodajských postupů Spojených států.

IV. TRANSPARENTNOST

Navíc k transparentnosti požadované zákonem USA o svobodě zpravodajská komunita Spojených států poskytuje veřejnosti mnohé dodatečné informace a ve zprůhledňování svých zpravodajských činností je velmi dobrým příkladem. Zpravodajská komunita zveřejnila mnohé své politiky, postupy, rozhodnutí soudu pro dohled nad zahraničními zpravodajskými činnostmi a další odtajněné materiály, čímž svou činnost výjimečným způsobem zprůhlednila. Zpravodajská komunita navíc podstatně zvýšila zveřejňování statistik ohledně vládního využívání pravomocí pro shromažďování informací z důvodu národní bezpečnosti. Dne 22. dubna 2015 zpravodajská komunita vydala druhou výroční zprávu, v níž předkládá statistiky o tom, jak často vláda tyto významné pravomoci využívá. ODNI na svých internetových stránkách a na stránkách *IC On the Record* také zveřejnil soubor konkrétních zásad transparentnosti ⁽⁵⁾ a prováděcí plán, kterým se zásady převádějí do konkrétních, měřitelných iniciativ ⁽⁶⁾. V říjnu 2015 ředitel národních zpravodajských služeb nařídil, aby každá zpravodajská agentura pověřila v rámci svého vedení úředníka pro transparentnost zpravodajských služeb, který bude podporovat transparentnost a povede iniciativy pro transparentnost ⁽⁷⁾. Úředník pro transparentnost bude úzce spolupracovat s úředníky pro ochranu soukromí a občanských svobod z jednotlivých zpravodajských agentur, aby se zajistilo, že transparentnost a ochrana soukromí a občanských svobod zůstávají i nadále hlavními prioritami.

⁽¹⁾ Viz *tamtéž* § 602.

⁽²⁾ Viz *tamtéž*.

⁽³⁾ Viz *tamtéž* § 603.

⁽⁴⁾ Viz *tamtéž* §§ 502(f)–503.

⁽⁵⁾ Dostupné na adrese <http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles>.

⁽⁶⁾ Dostupné na adrese <http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf>.

⁽⁷⁾ Viz *tamtéž*.

Jako příklad tohoto úsilí lze uvést, že hlavní úředník NSA pro ochranu soukromí a občanských svobod zveřejnil v průběhu posledních let několik neutajovaných zpráv, včetně zpráv o činnostech podle § 702, výkonného dekretu 12333 a zákona USA FREEDOM Act ⁽¹⁾. Zpravodajská komunita navíc úzce spolupracuje s Výborem pro dohled nad respektováním soukromí a občanských svobod, Kongresem a advokáty v oblasti ochrany soukromí ve Spojených státech, aby mohla zpravodajské činnosti Spojených států, kdykoli je to možné a je to v souladu s ochranou citlivých zdrojů a metod zpravodajství, dále zprůhledňovat. Celkově jsou zpravodajské činnosti Spojených států stejně transparentní, či dokonce ještě transparentnější než zpravodajské činnosti kteréhokoli jiného státu na světě a jsou tak transparentní, jak jen je to při dodržení potřeby chránit citlivé zdroje a metody možné.

Shrnutí rozsáhlé transparentnosti zpravodajských činností Spojených států:

- Zpravodajská komunita uvolnila a zveřejnila on-line tisíce stránek stanovisek soudů a postupů agentur, které nastiňují specifické postupy a požadavky našich zpravodajských činností. Rovněž jsme zveřejnili zprávy o souladu zpravodajských agentur s příslušnými omezeními.
- Vysoce postavení zpravodajští úředníci pravidelně hovoří na veřejnosti o úlohách a činnostech svých organizací, včetně popisů režimů pro soulad s předpisy a ochranných opatření, kterými se jejich práce řídí.
- Zpravodajská komunita zveřejnila dodatečné dokumenty o zpravodajských činnostech podle zákona o svobodě informací.
- Prezident vydal směrnici PPD-28, v níž se veřejně stanovují omezení našich zpravodajských činností, a Úřad ředitele národních zpravodajských služeb vydal dvě veřejné zprávy o provádění těchto omezení.
- Zpravodajská komunita nyní musí ze zákona zveřejňovat významná právní stanoviska vydaná Soudem pro uplatňování zákona FISA nebo jejich shrnutí.
- Vláda musí každoročně předkládat zprávu o tom, v jakém rozsahu využívá určité pravomoci v oblasti národní bezpečnosti, a společnosti jsou oprávněny činit totéž.
- Výbor pro dohled nad respektováním soukromí a občanských svobod vydala několik podrobných veřejných zpráv o zpravodajských činnostech a bude tak činit i nadále.
- Zpravodajská komunita poskytuje rozsáhlé utajené informace dohledovým výborům Kongresu.
- Ředitel národních zpravodajských služeb vydal zásady transparentnosti, jimiž se mají činnosti zpravodajské komunity řídit.

Toto rozsáhlé zprůhledňování půjde stále dál. Veškeré informace, které budou uvolněny pro veřejnost, budou samozřejmě k dispozici jak ministerstvu obchodu, tak Evropské komisi. Každoroční přezkum ze strany ministerstva obchodu a Evropské komise týkající se provádění štítu na ochranu soukromí poskytne Evropské komisi příležitost prodiskutovat jakékoli otázky, které vyvstaly na základě zveřejnění jakýchkoli nových informací, jakož i jakékoli jiné záležitosti týkající se štítu na ochranu soukromí a jeho fungování a chápeme, že ministerstvo si může k účasti na tomto přezkumu přizvat dle vlastního uvážení zástupce dalších agentur, včetně zpravodajské komunity. Podle mechanismů PPD-28 členské státy EU samozřejmě mohou své dotazy týkající se sledování předkládat také pověřenému úředníkovi ministerstva zahraničí.

V. NÁPRAVNÁ OPATŘENÍ

Právo Spojených států poskytuje fyzickým osobám, které byly předmětem nezákonného elektronického sledování pro účely národní bezpečnosti, několik způsobů nápravy. Podle zákona FISA se právo usilovat o nápravu u soudu Spojených států neomezuje na osoby USA. Fyzická osoba, která může prokázat oprávněnost svého nároku, aby mohla podat

⁽¹⁾ Dostupné na adrese https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

soudní žalobu, by podle zákona FISA měla k dispozici nápravná opatření pro napadení nezákonného elektronického sledování. Zákon FISA například osobám vystaveným nezákonnému elektronickému sledování umožňuje žalovat vládní úředníky Spojených států jako soukromé osoby o náhradu peněžní škody, včetně punitivní náhrady škody a odměny pro právního zástupce. Viz 50 U.S.C. § 1810. Fyzické osoby, které mohou prokázat oprávněnost svého nároku, mohou také podat občanskoprávní žalobu o náhradu peněžní škody, včetně nákladů řízení, proti Spojeným státům, pokud informace o nich získané prostřednictvím elektronického sledování podle zákona FISA byly nezákonně a úmyslně použity nebo zveřejněny. Viz 18 U.S.C. § 2712. V případě, že vláda má v úmyslu jakékoli informace získané prostřednictvím elektronického sledování nebo z něj odvozené o jakékoli dotčené osobě podle zákona FISA proti této osobě použít či zveřejnit v soudním nebo správním řízení ve Spojených státech, musí předem na svůj záměr upozornit tribunál a dotčenou osobu, která poté může napadnout zákonnost sledování a usilovat o zadržení takových informací. Viz 50 U.S.C. § 1806. Zákon FISA také upravuje trestní sankce pro fyzické osoby, které se záměrně zapojují do nezákonného elektronického sledování z titulu výkonu své funkce v soudnictví nebo prosazování práva či které záměrně využijí nebo zveřejní informace získané nezákonným sledováním. Viz 50 U.S.C. § 1809.

Občané EU mají jiné způsoby, jak se domáhat právní nápravy proti úředníkům Spojených států za nezákonné využití údajů nebo nezákonný přístup k nim ze strany vlády, včetně vládních úředníků, kteří poruší zákon nezákonným přístupem k informacím či jejich použitím pro údajné účely národní bezpečnosti. Zákon o počítačových podvodech a zneužití (*Computer Fraud and Abuse Act*) zakazuje úmyslný nezákonný přístup (nebo překročení zákonného přístupu) pro získání informací z finančních institucí, počítačového systému vlády Spojených států či počítače prostřednictvím internetového přístupu, stejně jako vyhrožování poškozením chráněných počítačů pro účely vydírání nebo podvodu. Viz 18 U.S.C. § 1030. Jakákoli osoba kterékoli státní příslušnosti, která utrpí škodu nebo ztrátu z důvodu porušení tohoto zákona, může na porušitele (včetně vládního úředníka) podat žalobu o náhradu škody a zdržovací žalobu nebo žádost o soudní zákaz podle § 1030(g), bez ohledu na to, zda došlo k trestnímu stíhání, a to za předpokladu, že jednání zahrnuje nejméně jednu z okolností stanovených v zákoně. Zákon o ochraně údajů v elektronických komunikacích (*Electronic Communications Privacy Act*, ECPA) upravuje vládní přístup k uchovávaným elektronickým komunikacím a transakčním záznamům a informacím o odběratelích drženým třetími stranami poskytujícími komunikační služby. Viz 18 U.S.C. §§ 2701-2712. Zákon ECPA povoluje poškozeným fyzickým osobám žalovat vládní úředníky za úmyslný nezákonný přístup k uchovávaným údajům. Vztahuje se na všechny osoby bez ohledu na jejich státní příslušnost a poškozené osoby mohou získat náhradu škody a náhradu palmáře. Zákon o právu na ochranu finančních údajů (*Right to Financial Privacy Act*, RFPA) omezuje přístup vlády Spojených států k záznamům bank a makléřů-obchodníků s cennými papíry o jednotlivých zákaznících. Viz 12 U.S.C. §§ 3401-3422. Podle zákona RFPA může zákazník banky nebo makléře-obchodníka s cennými papíry žalovat vládu Spojených států o zákonnou, skutečnou a punitivní náhradu škody za protiprávní získání přístupu k jeho záznamům; pokud je shledáno, že takový protiprávní přístup byl úmyslný, automaticky bude zahájeno vyšetřování s možným disciplinárním postihem příslušných zaměstnanců vlády. Viz 12 U.S.C. § 3417.

A konečně zákon o svobodě informací (*Freedom of Information Act*, FOIA) stanoví prostředky k tomu, aby se kterákoli osoba domáhala přístupu k existujícím záznamům federálních agentur na jakékoli téma v závislosti na určitých kategoriích výjimek. Viz 5 U.S.C. § 552(b). Tyto kategorie zahrnují omezení přístupu k utajovaným informacím o národní bezpečnosti, k osobním informacím jiných fyzických osob a k informacím o vyšetřováních vedených donucovacími orgány a jsou srovnatelné s omezeními, jež ve svých vlastních zákonech o přístupu k informacím ukládají jiné státy. Tato omezení platí stejnou měrou pro Američany i jiné státní příslušníky. Spory ohledně zveřejňování záznamů požadovaných podle zákona o svobodě informací lze řešit správní cestou a poté u federálního soudu. Soud musí nově rozhodnout, zda jsou záznamy odpírány dle předpisů (5 U.S.C. § 552(a)(4)(B)), a může vládě nařídít jejich zpřístupnění. V některých případech soudy vyvrátily tvrzení vlády, že by informace měly být odepřeny jako utajované ⁽¹⁾. Ačkoli nelze získat peněžitou náhradu škody, mohou soudy přiznat náhradu palmáře.

VI. ZÁVĚR

Spojené státy uznávají, že naše signálové i jiné zpravodajské činnosti musejí zohledňovat skutečnost, že by se se všemi osobami mělo zacházet důstojně a s respektem, bez ohledu na jejich státní příslušnost nebo místo pobytu, a že všechny osoby mají při nakládání s jejich osobními informacemi oprávněný zájem na ochraně svého soukromí. Spojené státy využívají signálové zpravodajství pouze pro prosazování zájmů národní bezpečnosti a zahraniční politiky a pro ochranu svých občanů a občanů svých spojenců a partnerů před újmou. Zkráceně řečeno, zpravodajská komunita neprovádí nahodilé sledování kohokoli, včetně běžných evropských občanů. Shromažďování informací prostřednictvím signálového zpravodajství se uskutečňuje pouze v řádně povolených případech, a to způsobem, který je v přísném souladu s těmito

⁽¹⁾ Viz např. *New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

omezeními, po zvážení dostupnosti alternativních zdrojů, včetně diplomatických a veřejných zdrojů, a způsobem, jenž upřednostňuje vhodné a proveditelné alternativy. A kdykoli je to možné, uskutečňuje se signálové zpravodajství pouze prostřednictvím shromažďování zacíleného pomocí diskriminantů na konkrétní zahraničnězpravodajské cíle nebo témata.

Politika Spojených států byla v tomto ohledu potvrzena směrnicí PPD-28. V tomto rámci nemají zpravodajské agentury Spojených států zákonnou pravomoc, zdroje, technickou kapacitu ani touhu zachycovat veškeré světové komunikace. Tyto agentury nečtou e-maily všech lidí ve Spojených státech ani všech lidí na celém světě. V souladu se směrnicí PPD-28 poskytují Spojené státy robustní ochranu osobních informací osob, které nejsou osobami USA, jež jsou shromažďovány prostřednictvím signálových zpravodajských činností. To v nejvyšší možné míře proveditelné v souladu s národní bezpečností zahrnuje politiky a postupy pro minimalizaci uchovávání a šíření osobních informací o osobách, které nejsou osobami USA, a to v rozsahu srovnatelném s ochranou poskytovanou státním příslušníkům Spojených států. Jak je navíc uvedeno výše, komplexní režim dohledu nad cílenými pravomocemi podle § 702 zákona FISA nemá obdoby. A konečně významné změny práva Spojených států v oblasti zpravodajské komunity zavedené zákonem USA o svobodě a iniciativami vedenými Úřadem ředitele národních zpravodajských služeb za účelem zprůhlednění zpravodajské komunity velice podporují ochranu soukromí a občanských svobod každé fyzické osoby bez ohledu na její státní příslušnost.

S pozdravem

Robert S. Litt

21. června 2016

Justin S. Antonipillai
Rada
Ministerstvo obchodu Spojených států amerických
1401 Constitution Avenue, N.W.
Washington, DC 20230

Ted Dean
Zástupce náměstka ministryně
Odbor pro mezinárodní obchod
1401 Constitution Avenue, N.W.
Washington, DC 20230

Vážený pane Antonipillai, vážený pane Deane,

píši Vám, abych Vám poskytl další informace o tom, jak Spojené státy provádějí hromadné shromažďování informací prostřednictvím signálových zpravodajských služeb. Jak vysvětluje poznámka pod čarou 5 v prezidentské směrnicí 28 (*Presidential Policy Directive 28*, PPD-28), „hromadným“ shromažďováním se rozumí získávání poměrně velkého objemu signálových zpravodajských informací nebo údajů za okolností, kdy zpravodajská komunita nemůže k soustředěnému shromažďování použít identifikátor spojený s konkrétním cílem (například e-mailovou adresu či telefonní číslo cíle). To však neznamená, že takovéto shromažďování je „masivní“ nebo „nahodilé“. Podle směrnice PPD-28 totiž „[s]ignálové zpravodajské činnosti musí být v nejvyšší možné míře uzpůsobeny na míru“. S cílem podpořit tento mandát přijímá zpravodajská komunita kroky, aby zajistila, že i když nebudeme moci použít zvláštní identifikátory k cílenému shromažďování, budou údaje, které mají být shromážděny, pravděpodobně obsahovat zahraniční zpravodajské informace, jež odpovídají požadavkům formulovaným tvůrci politiky Spojených států, a to postupem vysvětleným v mém dřívějším dopise, a minimalizuje objem irelevantních shromážděných informací.

Zpravodajská komunita může být například požádána o získání signálových zpravodajských informací o aktivitách teroristické skupiny, která působí v některém z regionů jedné blízkovýchodní země a o které se má za to, že plánuje útoky proti západoevropským zemím; zpravodajská komunita však nemusí znát jména, telefonní čísla, e-mailové adresy ani žádné jiné zvláštní identifikátory fyzických osob spojovaných s touto teroristickou skupinou. Můžeme se rozhodnout skupinu zaměřit shromažďováním komunikace směřující do a z uvedeného regionu k dalšímu přezkumu a rozboru, abychom určili komunikaci, která se týká uvedené skupiny. Při tom by se zpravodajská komunita snažila shromažďování co nejvíce zúžit. To by se považovalo za „hromadné“ shromažďování, protože není proveditelné využití diskriminantů, nikoli však za shromažďování „masivní“ nebo „nahodilé“, naopak by bylo zaměřeno co nejpřesněji.

I když tedy není možné zacílení pomocí konkrétních zvolených termínů, Spojené státy neshromažďují veškerou komunikaci ze všech komunikačních prostředků z celého světa, ale používají filtry a jiné technické nástroje, aby se shromažďování soustředilo na zařízení, která pravděpodobně obsahují komunikaci významnou pro zahraniční zpravodajství. Při tom se činnosti signálového zpravodajství Spojených států dotýkají pouze zlomku komunikace odehrávající se prostřednictvím internetu.

Navíc jak jsem uvedl ve svém dřívějším dopise, protože „hromadné“ shromažďování s sebou nese větší riziko shromažďování irelevantní komunikace, omezuje PPD-28 využití signálových zpravodajských činností zpravodajskou komunitou shromážděných hromadně na šest stanovených účelů. PPD-28 a postupy agentur, kterými se PPD-28 provádí, také omezují uchovávání a šíření osobních informací získaných signálovým zpravodajstvím bez ohledu na to, zda byly informace získány hromadně nebo cíleně, a bez ohledu na státní příslušnost fyzické osoby.

„Hromadné“ shromažďování informací zpravodajskou komunitou tedy není „masivní“ ani „nahodilé“, ale používá metody a nástroje k filtrovanému shromažďování s cílem soustředit se na materiál, který bude odpovídat požadavkům na zahraniční zpravodajství formulovaným tvůrci politiky, a zároveň minimalizovat shromažďování irelevantních informací; při tom se zpravodajská komunita řídí přísnými pravidly na ochranu irelevantních informací, jež mohou být získány.

Politiky a postupy popsané v tomto dopise se vztahují na veškeré hromadné shromažďování informací prostřednictvím signálového zpravodajství, včetně veškerého hromadného shromažďování komunikace do a z Evropy, aniž bychom potvrdovali nebo vyvraceli, zda k tomuto shromažďování dochází.

Žádali jste také o více informací o Výboru pro dohled nad respektováním soukromí a občanských svobod (PCLOB) a generálních inspektorech a jejich pravomocích. PCLOB je nezávislá agentura v rámci moci výkonné. Pěticečlennou radu složenou ze zástupců obou hlavních politických stran jmenuje prezident a potvrzuje Senát ⁽¹⁾. Každý člen rady je jmenován na šestileté funkční období. Členové rady a zaměstnanci musí získat příslušnou bezpečnostní prověrku, aby mohli vykonávat své zákonné povinnosti a odpovědnost v plném rozsahu ⁽²⁾.

Posláním PCLOB je zajistit, aby úsilí federální vlády předcházet terorismu bylo v rovnováze s potřebou chránit soukromí a občanské svobody. Rada má dvě základní povinnosti – dohlížet a poskytovat rady. PCLOB si stanoví vlastní pořad jednání a určuje, jaké dohledové nebo poradenské činnosti bude vykonávat.

V rámci svých *dohledových* činností PCLOB přezkouvá a analyzuje opatření přijímaná mocí výkonnou na ochranu národa před terorismem s tím, že nutnost těchto opatření musí být v rovnováze s nutností chránit soukromí a občanské svobody ⁽³⁾. Nejnovější dohledový přezkum, který PCLOB dokončil, se zaměřoval na programy sledování provozované podle § 702 zákona FISA ⁽⁴⁾. V současnosti přezkouvá zpravodajské činnosti provozované podle výkonného dekretu 12333 ⁽⁵⁾.

V rámci své *poradní* úlohy PCLOB zajišťuje, aby se při vypracovávání a provádění zákonů, předpisů a postupů spojených se snahou chránit národ před terorismem náležitě braly v úvahu obavy o svobodu ⁽⁶⁾.

Aby mohl výbor plnit své poslání, je ze zákona oprávněn nahlížet do všech příslušných záznamů, zpráv, auditů, přezkumů, dokladů, dokumentů, doporučení a veškerých dalších příslušných materiálů, včetně utajovaných informací v souladu se zákonem ⁽⁷⁾. Kromě toho se výbor může dotazovat jakéhokoli vládního úředníka či zaměstnance nebo jej vyslýchat, a to i veřejně ⁽⁸⁾. Navíc může rada písemně požádat ministra spravedlnosti o vydání předvolání jménem rady subjektům mimo moc výkonnou, která jim nařídí poskytnout příslušné informace ⁽⁹⁾.

A konečně je výbor ze zákona povinen vystupovat transparentně vůči veřejnosti. V rámci toho veřejnost informuje o svých činnostech pořádáním veřejných slyšení a zpřístupňováním svých zpráv veřejnosti v maximální možné míře v souladu s ochranou utajovaných informací ⁽¹⁰⁾. Kromě toho musí výbor PCLOB hlásit, odmítne-li se vládní agentura řídit jejím doporučením.

Generální inspektoři ve zpravodajské komunitě provádějí audity, inspekce a přezkumy programů a činností ve zpravodajské komunitě s cílem označit a řešit systémová rizika, zranitelná místa a nedostatky. Kromě toho generální inspektoři vyšetřují podněty nebo informace o údajném porušování zákonů, pravidel či předpisů nebo špatném

⁽¹⁾ 42 U.S.C. 2000ee(a), (h).

⁽²⁾ 42 U.S.C. 2000ee(k).

⁽³⁾ 42 U.S.C. 2000ee(d)(2).

⁽⁴⁾ Obecně viz <https://www.pclob.gov/library.html#oversightreports>.

⁽⁵⁾ Obecně viz <https://www.pclob.gov/events/2015/may13.html>.

⁽⁶⁾ 42 U.S.C. 2000ee(d)(1); viz také dokument PCLOB Advisory Function Policy and Procedure, Policy 2015-004, dostupný na adrese https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.

⁽⁷⁾ 42 U.S.C. 2000ee(g)(1)(A).

⁽⁸⁾ 42 U.S.C. 2000ee(g)(1)(B).

⁽⁹⁾ 42 U.S.C. 2000ee(g)(1)(D).

⁽¹⁰⁾ 42 U.S.C. 2000ee(f).

hospodaření, závažné plýtvání finančními prostředky, zneužití pravomoci či podstatné a konkrétní ohrožení veřejného zdraví a bezpečnosti v rámci programů a činností zpravodajské komunity. Životně důležitou složkou objektivitu a integrity každé zprávy, zjištění a doporučení, které generální inspektor vydá, je jeho nezávislost. K nejzásadnějším faktorům zachování nezávislosti generálních inspektorů patří proces jejich jmenování a odvolání, samostatné provozní, rozpočtové a personální pravomoci a požadavek předkládat zprávy jak vedoucím vládních agentur, tak Kongresu.

Kongres ustavil nezávislou kancelář generálního inspektora v každé vládní agentuře, včetně každého prvku zpravodajské komunity ⁽¹⁾. Po schválení zákona o schválení zpravodajské činnosti za rozpočtový rok 2015 (*Intelligence Authorization Act for Fiscal Year 2015*) téměř všechny generální inspektory dohlížející na prvky zpravodajské komunity jmenuje prezident a potvrzuje Senát, včetně generálních inspektorů na ministerstvu spravedlnosti, v Ústřední zpravodajské agentuře, Národní bezpečnostní agentuře a ve zpravodajské komunitě ⁽²⁾. Kromě toho jsou tito generální inspektori stálí nestranní činitelé, které může odvolat pouze prezident. I když podle ústavy Spojených států má prezident pravomoc odvolávat generální inspektory, byla uvedená pravomoc uplatněna jen zřídka a v takovém případě musí prezident poskytnout Kongresu 30 dní před odvoláním generálního inspektora písemné odůvodnění ⁽³⁾. Tento proces jmenování generálních inspektorů zajišťuje, aby výběr, jmenování nebo odvolání generálního inspektora nepatříčně neovlivňovali vládní činitelé.

Zadruhé, generální inspektori mají významné zákonné pravomoci provádět audity, vyšetřování a přezkumy vládních programů a operací. Mimo dohledové vyšetřování a přezkumy vyžadované zákonem mají generální inspektori značně volné uvážení vykonávat dohledovou pravomoc za účelem přezkumu programů a činností podle svého výběru ⁽⁴⁾. V rámci výkonu této pravomoci zákon zajišťuje, aby generální inspektori měli k plnění svých povinností nezávislé prostředky, včetně pravomoci přijímat vlastní zaměstnance a samostatně dokumentovat své rozpočtové žádosti pro Kongres ⁽⁵⁾. Zákon zajišťuje, aby generální inspektori měli přístup k informacím potřebným k výkonu jejich povinností. Sem patří pravomoc mít přímý přístup ke všem záznamům a informacím agentur, které podrobně rozepisují programy a operace dané agentury bez ohledu na utajení, pravomoc předvolávat za účelem poskytnutí informací a dokumentů a pravomoc přijímat přísahy ⁽⁶⁾. V omezených případech může vedoucí vládní agentury činnost generálního inspektora zakázat, pokud by například jeho audit nebo vyšetřování významně poškodily národní bezpečnostní zájmy Spojených států. Uplatnění této pravomoci je opět krajně neobvyklé a vedoucí agentury musí Kongresu do 30 dnů oznámit důvody jejího uplatnění ⁽⁷⁾. Ředitel národních zpravodajských služeb tuto pravomoc omezit jakékoli činnosti generálního inspektora ve skutečnosti nikdy neuplatnil.

Zatřetí, generální inspektori jsou povinni poskytovat vedoucím vládních agentur a Kongresu úplné a aktuální informace prostřednictvím zpráv o podvodech a jiných vážných problémech, zneužívání a nedostacích v souvislosti s vládními programy a činnostmi ⁽⁸⁾. Dvojí podávání zpráv posiluje nezávislost generálních inspektorů, neboť zprůhledňuje jejich dohledový proces a vedoucím agentur poskytuje příležitost provést doporučení generálních inspektorů, než Kongres přijme legislativní opatření. Generální inspektori jsou například ze zákona povinni zpracovávat pololetní zprávy, které popisují tyto problémy i nápravná opatření, jež byla dosud přijata ⁽⁹⁾. Vládní agentury berou zjištění a doporučení generálních inspektorů vážně a generální inspektori mohou často zařadit souhlas agentur s jejich doporučeními a jejich

⁽¹⁾ § 2, 4 zákona o generálních inspektorech (*Inspector General Act of 1978*), ve znění pozdějších předpisů; § 103H(b), (e) zákona o národní bezpečnosti (*National Security Act of 1947*), ve znění pozdějších předpisů; § 17(a) zákon o Ústřední zpravodajské službě (*Central Intelligence Act*) (dále též „zákon o CIA“).

⁽²⁾ Viz Pub. L. No. 113-293, 128 Stat. 3990, (Dec. 19, 2014). Prezident nejmenuje pouze generální inspektory *Defense Intelligence Agency* a *National Geospatial-Intelligence Agency*; nad těmito agenturami však má současně pravomoc generální inspektor ministerstva obrany a generální inspektor zpravodajské komunity.

⁽³⁾ § 3 zákona o generálních inspektorech; § 103H(c) zákona o národní bezpečnosti; § 17(b) zákona o CIA.

⁽⁴⁾ Viz § 4(a), 6(a)(2) zákona o generálních inspektorech; § 103H(c), (g)(2)(A) zákona o národní bezpečnosti; § 17(a), (c) zákona o CIA.

⁽⁵⁾ § 3(d), 6(a)(7), 6(f) zákona o CIA; § 103H(d), (i), (j), (m) zákona o národní bezpečnosti; § 17(e)(7), (f) zákona o CIA.

⁽⁶⁾ § 6(a)(1), (3), (4), (5), (6) zákona o CIA; § 103H(g)(2) zákona o národní bezpečnosti; § 17(e)(1), (2), (4), (5) zákona o CIA.

⁽⁷⁾ Viz např. § 8(b), 8E(a) zákona o generálních inspektorech; § 103H(f) zákona o národní bezpečnosti; § 17(b) zákona o CIA.

⁽⁸⁾ § 4(a)(5) zákona o generálních inspektorech; § 103H(a)(b)(3), (4) zákona o národní bezpečnosti; § 17(a)(2), (4) zákona o CIA.

⁽⁹⁾ § 2(3), 4(a), 5 zákona o generálních inspektorech; § 103H(k) zákona o národní bezpečnosti; § 17(d) zákona o CIA. Generální inspektor ministerstva spravedlnosti poskytuje své zveřejněné zprávy na internetu na adrese <http://oig.justice.gov/reports/all.htm>. Obdobně generální inspektor zpravodajské komunity zveřejňuje své pololetní zprávy na adrese <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

provedení do těchto i jiných zpráv poskytovaných Kongresu a v některých případech veřejnosti ⁽¹⁾. Mimo tuto strukturu dvojího předkládání zpráv jsou generální inspektori také povinni doprovázet vládní oznamovatele do příslušných výborů Kongresu pro dohled, aby je uvedení oznamovatelé mohli informovat o údajných podvodech, plýtvání nebo zneužívání v rámci vládních programů a činností. Totožnost těch, kdo vystoupí, je chráněna před sdělením moci výkonné, což oznamovatele chrání před potenciálními zakázanými personálními opatřeními nebo před opatřeními v rámci bezpečnostních prověrek přijatými v odvětví za podání hlášení generálnímu inspektorovi ⁽²⁾. Jelikož oznamovatelé jsou často zdrojem vyšetřování generálních inspektorů, možnost oznámit své obavy Kongresu bez ovlivňování moci výkonnou zvyšuje účelnost dohledu generálních inspektorů. Díky této nezávislosti mohou generální inspektori objektivně a čestně podporovat hospodárnost, efektivnost a odpovědnost ve vládních agenturách.

A konečně, Kongres ustavil Radu generálních inspektorů pro integritu a efektivnost. Tato rada mj. vypracovává normy pro audit, vyšetřování a přezkumy generálních inspektorů, podporuje výcvik a má pravomoc přezkoumávat obvinění generálních inspektorů ze zneužití pravomoci veřejného činitele, čímž nad generálními inspektory, kteří jsou pověřeni sledovat všechny ostatní, kriticky bdí. ⁽³⁾

Doufám, že Vám tyto informace budou nápomocny.

S pozdravem
Robert S. Litt
Generální rada

⁽¹⁾ § 2(3), 4(a), 5 zákona o generálních inspektorech; § 103H(k) zákona o národní bezpečnosti; § 17(d) zákona o CIA. Generální inspektor ministerstva spravedlnosti poskytuje své zveřejněné zprávy na internetu na adrese <http://oig.justice.gov/reports/all.htm>. Obdobně generální inspektor zpravodajské komunity zveřejňuje své pololetní zprávy na adrese <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

⁽²⁾ § 7 zákona o generálních inspektorech; § 103H(g)(3) zákona o národní bezpečnosti; § 17(e)(3) zákona o CIA.

⁽³⁾ § 11 zákona o generálních inspektorech.

PŘÍLOHA VII

Dopis zástupce náměstka ministryně spravedlnosti a rady pro mezinárodní záležitosti Bruce Swartze, Ministerstvo spravedlnosti Spojených států amerických

19. února 2016

Justin S. Antonipillai
Rada
Ministerstvo obchodu Spojených států amerických
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Zástupce náměstka ministryně
Odbor pro mezinárodní obchod
1401 Constitution Ave., NW
Washington, DC 20230

Vážený pane Antonipillai, vážený pane Deane,

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⁽¹⁾. Tyto zákonné postupy nerozlišují státní příslušnost subjektu údajů, jehož informace mají být získány od společností ve Spojených státech, včetně společností, které se budou autocertifikovat prostřednictvím rámce štítu EU-USA na ochranu soukromí. Dále společnosti, které ve Spojených státech obdrží soudní příkaz, jej mohou napadnout u soudu, jak je uvedeno níže⁽²⁾.

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 neexistuje 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). 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) (cit. *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). 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.

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

⁽¹⁾ 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, viz 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, a pro elektronický dohled, příkazy k prohlídce, obchodní záznamy a další shromažďování komunikací podle zákona FISA, viz 50 U.S.C. § 1801 a násl..

⁽²⁾ V tomto dopise se hovoří o pravomocích federálních donucovacích a regulačních orgánů; porušení státních zákonů jsou vyšetřována a souzena na úrovni jednotlivých států USA. 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 ochraně podle ústavy 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.

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. *See* 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 občansko-právním 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 látek a ve vyšetřováních generálního inspektora týkajících se vládních agentur. Usiluje-li vláda o uplatnění správního předvolání u soudu, adresát správního předvolání, stejně jako adresát předvolání velkou porotou, může 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 signalování, 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 ochraně údajů v elektronických komunikacích (*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 telefonních společností poskytujících internetové služby a jiných třetích stran poskytujících služby podle hlavy II zákona o ochraně údajů v elektronických komunikacích, 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 fakturačních informací 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 donucovací orgány obvykle získají od soudce příkaz na základě důvodného podezření, že dotčený účet obsahuje důkaz trestného činu. Zákon o uchovávaných komunikacích také upravuje občanskoprávní odpovědnost a trestní sankce.

Soudní nařízení 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. §§ 2510-2522. Tuto pravomoc mohou vykonávat pouze v souladu se soudním nařízením,

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 – 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 jiné nařízení k předložení informací. Viz čtvrtý dodatek Ústavy Spojených států amerických (jak je podrobněji uvedeno výše) a Fed. R. Crim. P. 41. Subjekt příkazu k prohlídce může usilovat o prohlášení příkazu za neplatný z důvodu přílišné šíře, kverulantství nebo jinak nepatřičného způsobu jeho získání a dotčené strany s oprávněným nárokem mohou usilovat o to, aby byly za neplatné prohlášeny jakékoli důkazy získané při nezákonné prohlídce. Viz věc *Mapp v. Ohio*, 367 U.S. 643 (1961).

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 FBI (září 2008) dostupné na adrese <http://www.justice.gov/archive/opa/docs/guidelines.pdf> stanovují 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 „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 AG FBI Guidelines, s. 5. Federální úřad pro vyšetřování tyto pokyny provedl prostřednictvím operační příručky FBI pro vnitrostátní vyšetřování, která je dostupná na adrese [https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20\(DIOG\)](https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG)) a která je komplexní příručkou, jež zahrnuje podrobná omezení týkající se 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 **United States Attorneys' Manual** (USAM), která je také dostupná na adrese <http://www.justice.gov/usam/united-states-attorneys-manual>.

Občanské a regulační orgány (veřejný zájem):

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 omezený 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. Viz 31 U.S.C. § 5318, 31 C.F.R. Part X. Další podniky se mohou opírat o zákon o spravedlivém informování o úvěrové spolehlivosti (*Fair Credit Reporting Act*), viz 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. *Right to Financial Privacy Act*, 12 U.S.C. §§ 3401–3422. 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 předpisů. Tyto činnosti také musí být v souladu s příslušnými postupy, včetně pokynů ministra spravedlnosti, které upravují federální činnosti prosazování práva. Výše popsaný 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.

S pozdravem

Bruce C. Swartz

zástupce náměstka ministryně spravedlnosti a rada
pro zahraniční záležitosti
