



**RADA
EVROPSKÉ UNIE**

**Brusel 29. listopadu 2013 (14.01)
(OR. en)**

17067/13

**JAI 1095
USA 64
DATAPROTECT 190
COTER 154**

PRŮVODNÍ POZNÁMKA

Odesílatel: Jordi AYET PUIGARNAU, ředitel,
za generální tajemnici Evropské komise
Datum přijetí: 28. listopadu 2013
Příjemce: Uwe CORSEPIUS, generální tajemník Rady Evropské unie
Č. dok. Komise: COM(2013) 846 final
Předmět: Sdělení Komise Evropskému parlamentu a Radě
Obnovení důvěry v toky údajů mezi EU a USA

Delegace naleznou v příloze dokument Komise COM(2013) 846 final.

Příloha: COM(2013) 846 final



V Bruselu dne 27.11.2013
COM(2013) 846 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

Obnovení důvěry v toky údajů mezi Eu a USA

1. ÚVOD: MĚNÍCÍ SE PROSTŘEDÍ V OBLASTI ZPRACOVÁNÍ ÚDAJŮ MEZI EU A USA

Evropská unie a Spojené státy jsou strategičtí partneři a toto partnerství je kriticky důležité pro posazování našich sdílených hodnot, bezpečnosti a společné vedoucí úlohy v celosvětových záležitostech.

Důvěra v tomto partnerství však byla narušena a je třeba ji obnovit. EU, její členské státy a občané Evropy vyjadřují hluboké znepokojení nad odhalením rozsáhlých programů Spojených států na shromažďování zpravodajských informací, zejména pokud jde o ochranu osobních údajů¹. Masové sledování soukromé komunikace, ať už občanů, podniků nebo politických představitelů, je nepřijatelné.

Předávání osobních údajů je důležitým a nezbytným prvkem transatlantických vztahů. Tvoří nedílnou součást transatlantických obchodních výměn, mimo jiné pro potřeby nových rostoucích digitálních odvětví, jakými jsou sociální média nebo cloud computing, v jejichž rámci putuje z EU do USA velké množství údajů. Představují také kriticky důležitou součást spolupráce mezi EU a USA v oblasti prosazování práva a spolupráce mezi členskými státy a USA v oblasti vnitrostátní bezpečnosti. USA a EU zavedly řadu dohod a režimů, aby usnadnily toky údajů a současně zajistily vysokou úroveň ochrany údajů v souladu s požadavky práva EU.

Obchodními výměnami se zabývá rozhodnutí 2000/520/ES² (dále jen „rozhodnutí o bezpečném přístavu“). Toto rozhodnutí poskytuje právní základ pro předávání osobních údajů z EU společností usazeným v USA, které přijímají zásady bezpečného přístavu.

Výměna osobních údajů mezi EU a USA pro účely prosazování práva včetně prevence terorismu a jiných forem závažné trestné činnosti a boje proti nim se řídí řadou dohod na úrovni EU. Jde o Dohodu o vzájemné právní pomoci³, Dohodu o využívání a předávání jmenné evidence cestujících (PNR)⁴, Dohodu o zpracovávání a předávání údajů o finančních transakcích pro účely Programu sledování financování terorismu (TFTP)⁵ a Dohodu mezi Europolem a USA. Tyto dohody reagují na vážné bezpečnostní výzvy a odpovídají společným bezpečnostním zájmům EU a USA při současném zachování vysoké úrovně ochrany osobních údajů. EU a USA navíc v současné době jednájí o rámcové dohodě o ochraně údajů v oblasti policejní a soudní spolupráce („zastřešující dohoda“)⁶. Cílem je zajistit vysokou úroveň ochrany předávaných údajů o občanech, a tím dále posílit spolupráci mezi EU a USA při boji proti trestné činnosti a terorismu na základě sdílených hodnot a dohodnutých ochranných opatření.

¹ Pro účely tohoto sdělení zahrnují zmínky o občanech EU také subjekty údajů mimo EU spadající do oblasti působnosti právních předpisů Evropské unie o ochraně osobních údajů.

² 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, 25.8.2000, s. 7.

³ Rozhodnutí Rady 2009/820/SZBP ze dne 23. října 2009 o uzavření Dohody o vydávání mezi Evropskou unií a Spojenými státy americkými a Dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými jménem Evropské unie, Úř. věst. L 291, 7.11.2009, s. 40.

⁴ Rozhodnutí Rady 2012/472/EU ze dne 26. dubna 2012 o uzavření Dohody mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států, Úř. věst. L 215, 11.8.2012, s. 4.

⁵ Rozhodnutí Rady ze dne 13. července 2010 o uzavření Dohody mezi Evropskou unií a Spojenými státy americkými o zpracovávání a předávání údajů o finančních transakcích z Evropské unie do Spojených států pro účely Programu sledování financování terorismu, Úř. věst. L 195, 27.7.2010, s. 3.

⁶ Rada přijala rozhodnutí, kterým pověřuje Komisi jednáním o této dohodě, dne 3. prosince 2010. Viz IP/10/1661 ze dne 3. prosince 2010.

Tyto nástroje se používají v prostředí, v němž toky osobních údajů nabývají stále více na důležitosti.

Rozvoj digitální ekonomiky vede na jedné straně k exponenciálnímu růstu činností zpracování údajů z hlediska kvantity, kvality, rozmanitosti i povahy. Vzrostla míra využívání služeb elektronických komunikací občany v běžném životě. Osobní údaje se staly velmi cenným statkem: odhadovaná hodnota osobních údajů občanů EU v roce 2011 činila 315 miliard EUR a má potenciál zvýšit se do roku 2020 na roční hodnotu téměř 1 bilionu EUR⁷. Trh pro analýzu velkých souborů údajů roste celosvětově o 40 % ročně⁸. Obdobně technický rozvoj, například v souvislosti s cloud computingem, dal nový obsah pojmu mezinárodního předávání údajů, neboť přeshraniční toky údajů se stávají každodenní realitou.⁹

Rozmach využívání služeb elektronických komunikací a zpracování údajů, včetně cloud computingu, rovněž výrazně zvýšil rozsah a význam předávání údajů přes Atlantik. Faktory jako ústřední postavení amerických společností v digitální ekonomice¹⁰, transatlantické směřování velké části elektronických komunikací a objem toků elektronických údajů mezi EU a USA získaly ještě více na významu.

Na druhé straně, moderní metody zpracování osobních údajů vyvolávají nové a důležité otázky. To se týká jak nových prostředků pro zpracování spotřebitelských údajů ve velkém pro obchodní účely soukromými firmami, tak zvýšené schopnosti zpravodajských služeb sledovat ve velkém komunikační údaje.

Rozsáhlé programy Spojených států pro shromažďování zpravodajských informací jako například PRISM se dotýkají základních práv Evropanů, konkrétně jejich práva na soukromí a ochranu osobních údajů. Tyto programy také ukazují spojitost mezi vládním sledováním a zpracováním údajů soukromými společnostmi, zejména americkými internetovými firmami. V důsledku toho mohou mít tyto programy hospodářský dopad. Jestliže budou mít občané obavy z rozsáhlého zpracovávání svých osobních údajů soukromými společnostmi nebo ze sledování svých údajů při používání internetových služeb zpravodajskými službami, může to ovlivnit jejich důvěru v digitální ekonomiku, což může mít negativní důsledky pro růst.

Tento vývoj staví toky údajů mezi EU a USA před nové výzvy. Toto sdělení se těmito výzvami zabývá. Hledá cestu kupředu na základě zjištění obsažených ve zprávě spolupředsedů EU *ad hoc* pracovní skupiny EU-USA a ve sdělení o bezpečném přístavu.

Snaží se nastítnit účinnou cestu ke znovuoobnovení důvěry a posílení spolupráce mezi EU a USA v těchto oblastech a k posílení transatlantických vztahů v širším kontextu.

Toto sdělení vychází z předpokladu, že normy na ochranu osobních údajů musí být pojednány ve svém správném kontextu, aniž by měly dopad na další rozměry vztahů mezi EU a USA, včetně probíhajícího jednání o transatlantickém obchodním a investičním partnerství. Z tohoto důvodu se normy na ochranu údajů nebudou projednávat v rámci transatlantického obchodního a investičního partnerství, jež bude pravidla pro ochranu údajů plně respektovat.

⁷ Viz Boston Consulting Group, „The Value of our Digital Identity“ (Hodnota naší digitální identity), listopad 2012.

⁸ Viz McKinsey, „Big data: The next frontier for innovation, competition, and productivity“ (Velké údaje: další krok pro inovace, hospodářskou soutěž a produktivitu), 2011.

⁹ Sdělení o Uvolnění potenciálu cloud computingu v Evropě, COM(2012) 529 final.

¹⁰ Například počet jedinečných návštěvníků stránek Microsoft Hotmail, Google Gmail a Yahoo! Mail z evropských zemí činil v červnu 2012 dohromady více než 227 milionů, což zastihuje počet návštěvníků všech ostatních poskytovatelů. Počet jedinečných evropských uživatelů, kteří se přihlašují na Facebook a mobilní Facebook, činil v březnu 2012 dohromady 196,5 milionu, což dělá z Facebooku největší sociální síť v Evropě. Google je největší internetový vyhledávač s celosvětovým podílem 90,2 % uživatelů internetu. Americkou mobilní službu zpráv What's App využívalo v červnu 2013 v Německu 91 % uživatelů iPhone.

Je důležité poznamenat, že zatímco EU může přijímat opatření v oblastech své působnosti, zejména za účelem ochrany uplatňování práva EU¹¹, vnitrostátní bezpečnost zůstává výlučnou odpovědností každého členského státu¹².

2. DOPAD NA NÁSTROJE PRO PŘEDÁVÁNÍ ÚDAJŮ

Zaprvé, pokud jde o údaje předávané pro obchodní účely, jako důležitý nástroj pro předávání údajů mezi EU a USA se osvědčil „bezpečný přístav“. Jeho obchodní význam vzrůstá úměrně tomu, jak toky osobních údajů získávají větší důležitost v transatlantických obchodních vztazích. Za posledních 13 let se systém bezpečného přístavu rozšířil na více než 3 000 společností, z nichž více než polovina se do tohoto systému přihlásila v posledních pěti letech. Rostou však obavy ohledně úrovně ochrany osobních údajů občanů EU předaných v rámci systému bezpečného přístavu do USA. Vzhledem k dobrovolné a deklaratorní povaze tohoto systému se pozornost stále více zaostřuje na jeho transparentnost a prosazování. Většina amerických společností sice jeho zásady uplatňuje, avšak některé společnosti s vlastním osvědčením tak nečiní. Toto nedodržování zásad bezpečného přístavu některými společnostmi s vlastním osvědčením poskytuje těmto společnostem konkurenční výhodu oproti evropským společnostem aktivním na stejných trzích.

Navíc podle zásad bezpečného přístavu jsou sice povolena omezení pravidel pro ochranu údajů, je-li to nezbytné z důvodů vnitrostátní bezpečnosti¹³, vzniká však otázka, zdali rozsáhlé shromažďování a zpracovávání osobních údajů v rámci programů Spojených států pro sledování je nezbytné a přiměřené pro naplnění zájmů vnitrostátní bezpečnosti. Ze zjištění *ad hoc* pracovní skupiny EU-USA je také jasné, že občané EU nemají v rámci těchto programů stejná práva a procesní ochranu jako Američané.

Dosah těchto programů sledování spolu s nerovným zacházením ve vztahu k občanům EU vyvolává pochybnosti ohledně úrovně ochrany, kterou systém bezpečného přístavu poskytuje. Orgány Spojených států mohou mít přístup k osobním údajům občanů EU zaslaným do USA podle zásad bezpečného přístavu a dále je zpracovávat způsobem, který je neslučitelný s důvody, pro které byly tyto údaje v EU původně shromážděny, a s účelem, pro který byly do USA předány. Většina amerických internetových společností, kterých se zřejmě tyto programy přímo týkají, vlastní osvědčení systému bezpečného přístavu.

Zadruhé, pokud jde o výměny údajů pro účely prosazování práva, stávající dohody (PNR, TFTP) se osvědčily jako velmi cenné nástroje pro řešení společných bezpečnostních hrozeb spojených se závažnou nadnárodní trestnou činností a terorismem a přitom zavedly ochranné prvky zajišťující vysokou úroveň ochrany údajů¹⁴. Tyto ochranné prvky se vztahují na všechny občany EU a dohody stanoví mechanismy pro přezkum jejich provádění a řešení souvisejících obav. Dohoda TFTP zavádí také systém dohledu, při němž nezávislí pracovníci dohledu z EU kontrolují, jak údaje, na které se dohoda vztahuje, prohledává americká strana.

¹¹ Viz rozsudek Soudního dvora Evropské unie ve věci C-300/11, ZZ v. Secretary of State for the Home Department.

¹² Čl. 4 odst. 2 SEU.

¹³ Viz např. rozhodnutí o bezpečném přístavu, Příloha I.

¹⁴ Viz Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (společná zpráva Komise a ministerstva financí Spojených států o hodnotě údajů TFTP poskytnutých podle čl. 6 odst. 6 Dohody mezi Evropskou unií a Spojenými státy americkými o zpracovávání a předávání údajů o finančních transakcích z Evropské unie do Spojených států pro účely Programu sledování financování terorismu).

Na základě obav, které se v EU objevily ohledně programů Spojených států pro sledování, využívá Evropská komise těchto mechanismů, aby kontrolovala, jak jsou tyto dohody uplatňovány. V případě dohody PNR byl proveden společný přezkum za účasti odborníků na ochranu údajů z EU a USA, kteří zkoumali, jak je dohoda prováděna¹⁵. Tento přezkum nepřinesl žádný náznak, že by programy Spojených států pro sledování zahrnovaly údaje o cestujících, na které se vztahuje dohoda PNR, nebo že by na ně měly dopad. Pokud jde o dohodu TFTP, Komise zahájila formální konzultace poté, co se objevila tvrzení, že zpravodajské služby Spojených států v rozporu s dohodou přímo přistupují k osobním údajům v EU. Tyto konzultace neodhalily žádné prvky, které by prokazovaly porušení dohody TFTP, a vedly Spojené státy k tomu, aby poskytly písemné ujištění, že nedochází k žádnému přímému shromažďování údajů, které by bylo v rozporu s ustanoveními dohody.

Rozsáhlé shromažďování a zpracovávání osobních údajů v programech Spojených států pro sledování však vyžaduje, aby velmi pečlivé monitorování provádění dohod PNR a TFTP pokračovalo i v budoucnu. EU a USA se proto dohodly na uspořádání příštího společného přezkumu dohody TFTP, který se bude konat na jaře roku 2014. Při tomto a dalších společných přezkumech bude zajištěna větší transparentnost ohledně toho, jak systém dohledu funguje a jak chrání údaje občanů EU. Zároveň budou podniknuty kroky, které zajistí, aby systém dohledu nadále pečlivě sledoval, jak se zpracovávají údaje předané v rámci dohody do USA, a zvláště se zaměřil na to, jak jsou tyto údaje sdíleny mezi orgány Spojených států.

Zatřetí, nárůst objemu zpracovávaných osobních údajů podtrhuje význam použitelných právních a správních ochranných opatření. Jedním z cílů *ad hoc* pracovní skupiny EU-USA bylo stanovit, která ochranná opatření se mají uplatnit, aby byl minimalizován dopad zpracovávání na základní práva občanů EU. Ochranná opatření jsou potřebná také pro ochranu firem. Některé právní předpisy Spojených států, jako například Patriot Act, umožňují orgánům Spojených států od společností přímo požadovat přístup k údajům uloženým v EU. Od evropských společností a amerických společností přítomných v EU tedy může být požadováno, aby v rozporu s právními předpisy EU a členských států předávaly údaje do Spojených států, a jsou tudíž vystaveny požadavkům kolizních právních povinností. Právní nejistota vyplývající z takových přímých požadavků může brzdit rozvoj nových digitálních služeb, jako je cloud computing, které mohou poskytovat efektivní a levnější řešení pro fyzické osoby i podniky.

3. ZAJIŠTĚNÍ ÚČINNÉ OCHRANY ÚDAJŮ

Předávání osobních údajů mezi EU a USA tvoří podstatnou složku transatlantických obchodních vztahů. Sdílení informací je rovněž podstatnou složkou bezpečnostní spolupráce mezi EU a USA, která je kriticky důležitá pro společný cíl předcházení závažné trestné činnosti a terorismu a boje proti nim. Nedávná odhalení programů Spojených států pro shromažďování zpravodajských informací však měla negativní dopad na důvěru, na níž je tato spolupráce založena. Zejména ovlivnila důvěru ve způsob zpracování osobních údajů. V zájmu digitální ekonomiky, bezpečnosti EU i USA a širších transatlantických vztahů by proto s cílem obnovit důvěru v předávání údajů měly být podniknuty dále popsané kroky.

¹⁵ Viz zprávu Komise „Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security“ (Společný přezkum provádění Dohody mezi Evropskou unií a Spojenými státy americkými o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států).

3.1. Reforma ochrany údajů v EU

Reforma ochrany údajů navržená Komisí v lednu 2012¹⁶ představuje důležitou reakci, pokud jde o ochranu osobních údajů. Zvláště důležitých je pět prvků navrhovaného balíčku pro ochranu údajů.

Zaprvé, pokud jde o územní působnost, navrhovaný právní předpis ujasňuje, že společnosti, které nejsou usazené v Unii, budou muset uplatňovat právní předpisy EU o ochraně údajů, budou-li nabízet zboží a služby evropským spotřebitelům nebo sledovat jejich chování. Jinými slovy, základní právo na ochranu údajů bude respektováno bez ohledu na zeměpisné umístění společnosti nebo jejího zařízení na zpracování údajů¹⁷.

Zadruhé, u mezinárodního předávání stanoví navrhované nařízení podmínky, za nichž mohou být údaje předávány mimo EU. Předávání bude povoleno pouze tehdy, když budou tyto podmínky, které chrání práva fyzických osob na vysokou úroveň ochrany, splněny¹⁸.

Zatřetí, co se týče prosazování, navrhovaná pravidla stanoví přiměřené a odstrašující sankce (až do výše 2 % celosvětového ročního obrátu společnosti), aby tak bylo zajištěno, že společnosti budou právní předpisy EU dodržovat¹⁹. Existence věrohodných sankcí zvýší pobídku společností dodržovat právní předpisy EU.

Začtvrté, navrhované nařízení obsahuje jasná pravidla týkající se povinností a závazků zpracovatelů údajů, jako jsou poskytovatelé cloudových řešení, včetně povinností a závazků týkajících se bezpečnosti²⁰. Jak ukázala odhalení programů Spojených států pro shromažďování zpravodajských informací, jde o kritický prvek, protože tyto programy se dotýkají údajů uložených v cloudu. Společnosti poskytující úložné prostory v cloudu, které budou požádány o poskytnutí osobních údajů cizím orgánům, se také nebudou moci vyhnout odpovědnosti odkazem na své postavení zpracovatelů údajů, a nikoliv jejich kontrolorů.

Zapáté, tento balíček povede k zavedení komplexních pravidel pro ochranu osobních údajů zpracovávaných v oblasti prosazování práva.

Očekává se, že balíček bude schválen včas v průběhu roku 2014²¹.

¹⁶ COM(2012) 10 final: Návrh směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů, Brusel, 25.1.2012, a COM(2012) 11 final: Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů).

¹⁷ Komise bere na vědomí, že Evropský parlament potvrdil a posílil tuto důležitou zásadu zakotvenou v článku 3 navrhovaného nařízení dne 21. října 2013 ve svém hlasování o zprávách o reformě ochrany údajů, které předložili poslanci Evropského parlamentu Jan-Philipp Albrecht a Dimitrios Droutsas ve Výboru pro občanské svobody, spravedlnost a vnitřní věci (LIBE).

¹⁸ Komise bere na vědomí, že výbor Evropského parlamentu LIBE ve svém hlasování dne 21. října 2013 navrhl zařadit do budoucího nařízení ustanovení, které by žádosti cizích orgánů o přístup k osobním údajům shromážděným v EU, pokud by taková žádost byla podána mimo rámec smlouvy o vzájemné právní pomoci nebo jiné mezinárodní dohody, podmínilo tím, že musejí nejprve získat povolení od vnitrostátního orgánu pro ochranu údajů.

¹⁹ Komise bere na vědomí, že výbor LIBE ve svém hlasování dne 21. října 2013 navrhl posílit návrh Komise ustanovením, že pokuty mohou dosáhnout až 5 % celosvětového ročního obrátu společnosti.

²⁰ Komise bere na vědomí, že výbor LIBE ve svém hlasování dne 21. října 2013 schválil posílení povinností a závazků zpracovatelů údajů, zejména s ohledem na článek 26 navrhovaného nařízení.

²¹ Závěry Evropské rady z října 2013 uvádějí: „Je důležité podporovat důvěru občanů a podniků v digitální ekonomiku. Včasné přijetí silného rámce EU pro obecnou ochranu údajů a směrnice o kybernetické bezpečnosti má pro dokončení jednotného digitálního trhu do roku 2015 zásadní význam.“

3.2. Učinit bezpečný přístav bezpečnějším

Systém bezpečného přístavu je důležitou složkou obchodních vztahů mezi EU a USA, kterou využívají společnosti na obou stranách Atlantiku.

Zpráva Komise o fungování bezpečného přístavu nalezla v tomto systému řadu slabých míst. V důsledku nedostatečné transparentnosti a nedostatečného prosazování někteří členové systému s vlastním osvědčením jeho zásady v praxi nedodržují. To má negativní dopad na základní práva občanů EU. Rovněž se tak evropské společnosti dostávají do nevýhody oproti konkurenčním americkým společnostem, které se systému účastní, ale v praxi jeho zásady neuplatňují. Tato slabina má vliv také na většinu amerických společností, které systém řádně uplatňují. Bezpečný přístav také funguje jako cesta pro předávání osobních údajů občanů EU z EU do USA společnostmi, které jsou povinny vydávat údaje zpravodajským službám Spojených států podle programů Spojených států pro shromažďování zpravodajských informací. Nebudou-li tyto nedostatky napraveny, vzniká tak podnikům z EU konkurenční nevýhoda a dochází k negativnímu dopadu na základní právo občanů EU na ochranu údajů.

Evropské orgány pro ochranu údajů ve své reakci na nedávná odhalení programů sledování zdůraznily nedostatky systému bezpečného přístavu. Článek 3 rozhodnutí o bezpečném přístavu zmocňuje tyto orgány za určitých okolností zastavit toky údajů ke společnostem s osvědčením.²² Němečtí komisaři pro ochranu údajů se rozhodli nevydávat nová povolení pro předávání údajů do zemí mimo EU (například pro účely využívání některých cloudových služeb). Budou rovněž zkoumat, zdali by mělo být zastaveno předávání údajů prováděné v rámci bezpečného přístavu.²³ Riziko spočívá v tom, že taková opatření přijatá na vnitrostátní úrovni by vytvořila rozdíly v oblastech působnosti, a bezpečný přístav by tudíž přestal být základním mechanismem pro předávání osobních údajů mezi EU a USA.

Komise má podle směrnice 95/46/ES pravomoc pozastavit nebo zrušit rozhodnutí o bezpečném přístavu, jestliže tento systém již neposkytuje odpovídající úroveň ochrany. Dále článek 3 rozhodnutí o bezpečném přístavu stanoví, že Komise může rozhodnutí zrušit, pozastavit nebo může omezit jeho působnost, a podle článku 4 je může kdykoli upravit s ohledem na zkušenosti s jeho uplatňováním.

V tomto kontextu lze zvažovat několik variant politiky, a sice:

- zachovat *status quo*,
- posílit systém bezpečného přístavu a důkladně přezkoumat jeho fungování,
- pozastavit nebo zrušit rozhodnutí o bezpečném přístavu.

Vzhledem k nalezeným slabinám nelze ve stávajícím provádění systému bezpečného přístavu pokračovat. Jeho zrušení by však mělo negativní dopad na zájmy členských společností v EU a v USA. Komise je toho názoru, že bezpečný přístav by měl být posílen.

Zlepšení by se měla týkat strukturálních nedostatků souvisejících s transparentností a prosazováním, věcných zásad bezpečného přístavu i výjimky z důvodů národní bezpečnosti. Konkrétněji, aby systém bezpečného přístavu fungoval zamýšleným způsobem, musí být sledování a dohled orgánů Spojených států nad dodržováním zásad bezpečného přístavu společnostmi s osvědčením účinnější a systematictější. U společností s osvědčením se musí

²² Konkrétně podle článku 3 rozhodnutí o bezpečném přístavu může k takovému zastavení dojít v případech, kdy je velmi pravděpodobné, že zásady jsou porušovány; pokud se lze důvodně domnívat, že příslušný výkonný orgán včas nepřijal nebo nepřijme přiměřená opatření nezbytná pro vyřešení sporné věci; pokud by pokračování v předávání údajů vyvolalo bezprostřední riziko vzniku vážné újmy subjektům údajů a pokud příslušné orgány členského státu za daných okolností přiměřeně usilují o informování organizace a poskytly jí možnost zaujmout stanovisko.

²³ Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, tisková zpráva ze dne 24. července 2013.

zlepšit transparentnost politik ochrany soukromí. Občanům EU musí být také zaručena existence a cenová dostupnost mechanismů pro řešení sporů.

Komise bude naléhavě jednat s orgány Spojených států, aby s nimi diskutovala o zjištěných nedostatcích. Nápravná opatření by měla být popsána do léta 2014 a uplatněna co nejdříve. Na jejich základě provede Komise úplnou inventuru fungování bezpečného přístavu. Tento širší postup přezkumu by měl zahrnovat otevřenou konzultaci a debatu v Evropském parlamentu a v Radě i diskuse s orgány Spojených států.

Je rovněž důležité, aby výjimka z důvodů vnitrostátní bezpečnosti stanovená v rozhodnutí o bezpečném přístavu byla využívána pouze v rozsahu, který je naprosto nezbytný a přiměřený.

3.3. Posílení ochranných opatření na ochranu údajů při spolupráci v oblasti prosazování práva

EU a USA v současné době jednají o „zastřešující“ dohodě o ochraně údajů pro předávání a zpracovávání osobních informací v kontextu policejní a justiční spolupráce v trestních věcech. Uzavření takové dohody, která by stanovila vysokou úroveň ochrany osobních údajů, by představovalo významný příspěvek k posílení transatlantické důvěry. Pokrok v oblasti práv občanů EU na ochranu údajů by pomohl posílit transatlantickou spolupráci, jejímž cílem je prevence trestné činnosti a terorismu a boj proti nim.

Podle rozhodnutí, jímž byla Komise pověřena vyjednat tuto zastřešující dohodu, by mělo být cílem jednání zajistit vysokou úroveň ochrany v souladu s právními předpisy EU o ochraně údajů. To by se mělo odrazit v dohodnutých pravidlech a ochranných opatřeních týkajících se mimo jiné omezení účelu, podmínek a doby uchovávání údajů. V kontextu vyjednávání by Komise rovněž měla získat závazky týkající se vymahatelných práv včetně soudních opravných prostředků pro občany EU, kteří nemají bydliště v USA²⁴. Těsná spolupráce EU a USA při řešení společných výzev v oblasti bezpečnosti by měla být souběžně doprovázena úsilím zajistit, aby se občané na obou stranách Atlantiku těšili stejným právům při zpracovávání stejných údajů pro stejné účely. Je rovněž důležité, aby výjimky z důvodů potřeb národní bezpečnosti byly úzce definovány. V této věci by měla být dohodnuta ochranná opatření a omezení.

Tato jednání poskytují příležitost vyjasnit, že k osobním údajům, které drží soukromé společnosti a které jsou umístěny v EU, nebudou mít přímý přístup orgány prosazování práva Spojených států ani jim nebudou předávány jinak než prostřednictvím formálních cest spolupráce, jako jsou například dohody o vzájemné právní pomoci nebo odvětvové dohody mezi EU a USA, jimiž se takové předávání povoluje. Jiný způsob přístupu by měl být vyloučen, ledaže k němu dojde v jasně definovaných, výjimečných a soudně přezkoumatelných situacích. Spojené státy by měly v tomto smyslu učinit závazky²⁵.

²⁴ Viz příslušnou pasáž ve společné tiskové zprávě vydané po jednání ministrů spravedlnosti a vnitřních věcí EU-USA konaném dne 18. listopadu 2013 ve Washingtonu: „Jsme proto odhodláni s naléhavostí rychle postupovat v jednáních o zastřešující dohodě o rozumné a komplexní ochraně údajů v oblasti prosazování práva. Tato dohoda bude sloužit jako základ umožňující předávání údajů v kontextu policejní a justiční spolupráce v trestních věcech tím, že zajistí vysokou úroveň ochrany osobních údajů pro občany USA a EU. Jsme odhodláni pracovat na vyřešení zbývajících otevřených otázek vznesených oběma stranami, včetně soudních opravných prostředků (což je zásadní záležitost pro EU). Naším cílem je dokončit jednání o této dohodě do léta 2014.“

²⁵ Viz příslušnou pasáž ve společné tiskové zprávě vydané po jednání ministrů spravedlnosti a vnitřních věcí EU-USA dne konaném 18. listopadu 2013 ve Washingtonu: „Rovněž zdůrazňujeme hodnotu dohody mezi EU a USA o vzájemné právní pomoci. Znovu připomínáme svůj závazek zajistit, aby byla široce a účinně využívána pro účely dokazování v trestním řízení. Diskutovalo se také o tom, že je nutné ujasnit, že k osobním údajům drženým soukromými subjekty na území druhé strany nebudou mít orgány prosazování práva přístup mimo právně schválené cesty. Dále souhlasíme s přezkoumáním fungování dohody o vzájemné právní pomoci, jak je v dohodě zamýšleno, a se vzájemnými konzultacemi kdykoli budou zapotřebí.“

„Zastřešující“ dohoda sjednaná podle těchto zásad by měla poskytnout obecný rámec pro zajištění vysoké úrovně ochrany osobních údajů při jejich předávání do USA pro účely prevence trestné činnosti a terorismu nebo boje proti nim. Odvětvové dohody by měly tam, kde je to nutné s ohledem na povahu dotčeného předání údajů, stanovit další pravidla a ochranná opatření, například následovat příklad dohod PNR a TFTP mezi EU a USA, které stanoví přísné podmínky pro předávání údajů a ochranná opatření pro občany EU.

3.4. Jak jsou evropské obavy řešeny v rámci probíhajících reforem v USA

Prezident Spojených států Obama oznámil, že probíhá přezkum činnosti vnitrostátních bezpečnostních orgánů Spojených států, včetně použitelného právního rámce. Tento probíhající proces poskytuje dobrou příležitost, jak reagovat na obavy EU vyplývající z nedávných odhalení programů Spojených států pro shromažďování zpravodajských informací. Nejdůležitějšími změnami by bylo rozšíření ochranných opatření platných pro občany USA a pro osoby, které mají v USA bydliště, na občany EU, kteří v USA bydliště nemají, větší transparentnost zpravodajských činností a další posílení dohledu. Takové změny by obnovily důvěru ve výměny údajů mezi EU a USA a podpořily využívání internetových služeb Evropany.

Pokud jde o rozšíření ochranných opatření platných pro občany USA a pro osoby, které mají v USA bydliště, na občany EU, měly by být přezkoumány právní normy týkající se programů Spojených států pro sledování, které zacházejí odlišně s občany USA a s občany EU, a to také z hlediska nutnosti a přiměřenosti, a zároveň by mělo být zohledněno těsné transatlantické partnerství v oblasti bezpečnosti, které je založeno na společných hodnotách, právech a svobodách. To by snížilo rozsah toho, jak jsou Evropané dotčeni programy Spojených států pro shromažďování zpravodajských informací.

Je zapotřebí větší transparentnost právního rámce programů Spojených států pro shromažďování zpravodajských informací i jeho výkladu soudy Spojených států, a to i pokud jde o kvantitativní rozměr programů Spojených států pro shromažďování zpravodajských informací. Prospěch z takových změn by měli i občané EU.

Dohled nad programy Spojených států pro shromažďování zpravodajských informací by se zlepšil posílením úlohy soudu Foreign Intelligence Surveillance Court a zavedením opravných prostředků pro fyzické osoby. Tyto mechanismy by mohly snížit míru zpracovávání osobních údajů Evropanů, které nejsou důležité pro účely vnitrostátní bezpečnosti.

3.5. Mezinárodní podpora norem pro ochranu soukromí

Otázky, jež moderní metody ochrany údajů vzbuzují, se neomezují na předávání údajů mezi EU a USA. Vysoká úroveň ochrany osobních údajů by měla být zajištěna každé fyzické osobě. Pravidla EU pro shromažďování, zpracovávání a předávání údajů by měla být prosazována mezinárodně.

Nedávno byla navržena řada iniciativ na podporu ochrany soukromí, zejména na internetu²⁶. EU by měla zajistit, aby takové iniciativy, pokud budou prováděny, plně zohledňovaly zásady ochrany základních práv, svobody projevu, osobních údajů a soukromí, jak jsou stanoveny v právu EU a ve strategii EU pro kybernetickou bezpečnost, a neohrožovaly svobodu, otevřenost a bezpečnost kybernetického prostoru. To zahrnuje demokratický a efektivní model správy, na níž se podílí více zúčastněných stran.

Probíhající reformy právních předpisů o ochraně údajů na obou stranách Atlantiku také dávají EU a USA jedinečnou příležitost prosadit tyto normy mezinárodně. Velkým přínosem pro

²⁶ V tomto ohledu viz návrh rezoluce navržené Valnému shromáždění OSN Německem a Brazílií, která vyzývá k ochraně soukromí online i offline.

výměny údajů přes Atlantik a dál by bylo posílení domácího právního rámce Spojených států, včetně části týkající se zákona o právech spotřebitelů na soukromí („Consumer Privacy Bill of Rights“), jež prezident Obama ohlásil v únoru 2012 jako součást komplexního plánu na zlepšení ochrany soukromí spotřebitelů. Existence sady silných a vymahatelných pravidel pro ochranu údajů zakotvených v EU i v USA by představovala dobrý základ pro přeshraniční toky údajů.

Pokud jde o mezinárodní podporu norem na ochranu soukromí, mělo by být podporováno také přistoupení k úmluvě Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat („Úmluva č. 108“), která je otevřena i státům, jež nejsou členy Rady Evropy²⁷. Ochranná opatření a záruky dohodnuté na mezinárodních fórech by měly přinést vysokou úroveň ochrany, která je slučitelná s požadavky práva EU.

4. ZÁVĚRY A DOPORUČENÍ

Otázky popsané v tomto sdělení vyžadují, aby byly podniknuty kroky jak na straně USA, tak na straně EU a jejích členských států.

Obavy týkající se transatlantických výměn údajů EU a členským státům především připomínají, aby v reformě ochrany údajů postupovaly rychle a ambiciózně. Ukazují, že silný legislativní rámec s jasnými pravidly, která jsou vymahatelná i v situacích, kdy se údaje předávají do zahraničí, je více než kdy dříve nutností. Orgány EU by proto měly pokračovat v práci směřující k přijetí reformy EU v oblasti ochrany údajů do jara 2014, aby tak byla zajištěna účinná a komplexní ochrana osobních údajů.

Vzhledem k významu transatlantických toků údajů je důležité, aby nástroje, na nichž jsou tyto výměny založeny, odpovídajícím způsobem reagovaly na výzvy a příležitosti digitální éry a nového technického vývoje, jako je cloud computing. Stávající a budoucí režimy a dohody by měly zajistit, že i na druhé straně Atlantiku bude nadále zaručena vysoká úroveň ochrany.

Robustní systém bezpečného přístavu je v zájmu občanů a společností z EU i USA. V krátké době by měl být posílen lepším sledováním a prováděním, a na tomto základě pak širším přezkoumáním jeho fungování. Aby bylo zajištěno, že původní cíle rozhodnutí o bezpečném přístavu – tedy kontinuita ochrany údajů, právní jistota a volný pohyb údajů mezi EU a USA – jsou nadále naplňovány, jsou nutná zlepšení.

Tato zlepšení by se měla zaměřit na potřebu, aby orgány Spojených států lépe dohlížely na dodržování zásad bezpečného přístavu společnostmi s vlastním osvědčením a sledovaly je.

Je rovněž důležité, aby výjimka z důvodů vnitrostátní bezpečnosti stanovená v rozhodnutí o bezpečném přístavu byla využívána pouze v rozsahu, který je naprosto nezbytný a přiměřený.

V oblasti prosazování práva by současná jednání o „zastřešující dohodě“ měla vést k vysoké úrovni ochrany občanů na obou stranách Atlantiku. Taková dohoda by posílila důvěru Evropanů ve výměny údajů mezi EU a USA a poskytla základ pro další rozvoj bezpečnostní spolupráce a partnerství mezi EU a USA. V kontextu těchto jednání by měly být získány závazky o tom, že Evropanům, kteří nemají bydliště v USA, budou k dispozici procesní ochranná opatření včetně soudních opravných prostředků.

Od vlády Spojených států by měly být žádány závazky, že k osobním údajům, které drží soukromé subjekty v EU, nebudou mít orgány prosazování práva Spojených států přímý přístup jinak, než prostřednictvím formálních cest spolupráce, jako jsou například dohody o vzájemné právní pomoci nebo odvětvové dohody mezi EU a USA, např. PNR a TFTP, jimiž se takové předávání povoluje za přísných podmínek a pouze v jasně definovaných, výjimečných a soudně přezkoumatelných situacích.

²⁷ Spojené státy jsou již stranou jiné úmluvy Rady Evropy: Úmluvy z roku 2001 o kyberkriminalitě (též nazývané „Budapešťská úmluva“).

Spojené státy by rovněž měly rozšířit ochranná opatření, která jsou k dispozici občanům USA a osobám, které mají bydliště v USA, na občany EU, kteří v USA bydliště nemají, zajistit nezbytnost a přiměřenost programů, větší transparentnost a dohled v rámci právních předpisů použitelných na orgány vnitrostátní bezpečnosti Spojených států.

Oblasti vyjmenované v tomto sdělení budou vyžadovat konstruktivní přístup na obou stranách Atlantiku. EU a USA jako strategičtí partneři jsou společně schopni překonat současné napětí v transatlantických vztazích a obnovit důvěru v oblasti toků údajů mezi EU a USA. Společně učiněné politické a právní závazky k další spolupráci v těchto oblastech povedou k celkovému posílení transatlantických vztahů.