

II

(Nelegislatívne akty)

ROZHODNUTIA

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2016/1250

z 12. júla 2016

**podľa smernice Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej
štítom na ochranu osobných údajov medzi EÚ a USA**

[oznámené pod číslom C(2016) 4176]

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na smernicu Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov ⁽¹⁾, a najmä na jej článok 25 ods. 6,po porade s európskym dozorným úradníkom pre ochranu údajov ⁽²⁾,

1. ÚVOD

- (1) V smernici 95/46/ES sú stanovené pravidlá pre prenosy osobných údajov z členských štátov do tretích krajín do tej miery, v akej tieto prenosy patria do jej rozsahu pôsobnosti.
- (2) Článok 1 smernice 95/46/ES a odôvodnenia 2 a 10 jej preambuly majú za cieľ zabezpečiť nielen účinnú a úplnú ochranu základných práv a slobôd fyzických osôb, najmä základného práva na rešpektovanie súkromného života s ohľadom na spracovanie osobných údajov, ale aj vysokú úroveň ochrany týchto základných práv a slobôd ⁽³⁾.
- (3) Význam základného práva na rešpektovanie súkromného života zaručeného článkom 7 a základného práva na ochranu osobných údajov zaručeného článkom 8 Charty základných práv Európskej únie sa zdôrazňuje aj v judikatúre Súdneho dvora ⁽⁴⁾.
- (4) Podľa článku 25 ods. 1 smernice 95/46/ES sú členské štáty povinné zabezpečiť, aby sa prenos osobných údajov do tretej krajiny mohol uskutočniť len vtedy, ak príslušná tretia krajina zaistí primeranú úroveň ochrany a ak sú pred prenosom údajov dodržané právne predpisy členských štátov, ktorými sa vykonávajú iné ustanovenia uvedenej smernice. Komisia môže konštatovať, že tretia krajina zabezpečuje túto primeranú úroveň ochrany z dôvodu svojho vnútroštátneho práva alebo medzinárodných záväzkov, ktoré prijala v záujme ochrany práv fyzických osôb. V takom prípade a bez toho, aby tým bolo dotknuté dodržiavanie vnútroštátnych ustanovení prijatých podľa iných ustanovení tejto smernice, sa osobné údaje môžu preniesť z členských štátov bez toho, aby boli potrebné dodatočné záruky.

⁽¹⁾ Ú. v. ES L 281, 23.11.1995, s. 31.

⁽²⁾ Pozri stanovisko 4/2016 k návrhu rozhodnutia o primeranosti štítu na ochranu osobných údajov medzi EÚ a USA, uverejnené 30. mája 2016.

⁽³⁾ Vec C-362/14, Maximillian Schrems/Data Protection Commissioner (ďalej len vec „Schrems“), EU:C:2015:650, bod 39.

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

- (5) Podľa článku 25 ods. 2 smernice 95/46/ES by sa úroveň ochrany údajov, ktorú poskytuje tretia krajina, mala hodnotiť s ohľadom na všetky okolnosti týkajúce sa operácie prenosu údajov alebo súboru operácií prenosu údajov vrátane všeobecných a odvetvových právnych noriem platných v danej tretej krajine.
- (6) V rozhodnutí Komisie 2000/520/ES ⁽⁵⁾ sa na účely článku 25 ods. 2 smernice 95/46/ES „zásady bezpečného prístavu“ uplatňované v súlade s usmerneniami, ktoré boli poskytnuté prostredníctvom tzv. „často kladených otázok“ vydaných Ministerstvom obchodu USA, považovali za zabezpečujúce primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám so sídlom v USA.
- (7) Komisia vo svojich oznámeniach COM(2013) 846 final ⁽⁶⁾ a COM(2013) 847 final z 27. novembra 2013 ⁽⁷⁾ usúdila, že je nutné preskúmať samotný základ systému bezpečného prístavu a posilniť ho s ohľadom na viacero faktorov vrátane exponenciálneho nárastu tokov údajov a ich rozhodujúceho významu pre transatlantické hospodárstvo, rýchleho rastu počtu spoločností z USA, ktoré dodržiavajú systém bezpečného prístavu, a nových informácií o rozsahu a zameraní niektorých spravodajských programov USA, ktoré vyvolávajú otázky v súvislosti s úrovňou ochrany, ktorú dokázu USA zaručiť. Komisia okrem toho v systéme bezpečného prístavu identifikovala niekoľko nedostatkov.
- (8) Na základe dôkazov zhromaždených Komisiou vrátane informácií vyplývajúcich z práce kontaktnej skupiny EÚ – USA v oblasti ochrany súkromia ⁽⁸⁾ a informácií o spravodajských programoch USA zhromaždených v rámci ad hoc pracovnej skupiny EÚ – USA ⁽⁹⁾ Komisia sformulovala 13 odporúčaní na preskúmanie systému bezpečného prístavu. Tieto odporúčania boli zamerané na posilnenie základných zásad ochrany súkromia, zvýšenie transparentnosti podmienok ochrany súkromia spoločností v USA, ktoré osvedčili svoje dodržiavanie zásad, lepší dohľad nad dodržiavaním týchto zásad, jeho monitorovanie a presadzovanie zo strany orgánov USA, dostupnosť cenovo dostupných mechanizmov riešenia sporov a potrebu zabezpečiť, aby bolo používanie výnimky týkajúcej sa národnej bezpečnosti stanovenej v rozhodnutí 2000/520/ES obmedzené na nevyhnutne potrebnú a primeranú mieru.
- (9) Súdny dvor Európskej únie vo svojom rozsudku zo 6. októbra 2015 vo veci C-362/14, Maximillian Schrems/Data Protection Commissioner ⁽¹⁰⁾ vyhlásil rozhodnutie 2000/520/ES za neplatné. Súd bez posúdenia obsahu zásad bezpečného prístavu konštatoval, že Komisia v tomto rozhodnutí neuviedla, že USA naozaj „zaistujú“ primeranú úroveň ochrany z dôvodu svojho vnútroštátneho práva alebo medzinárodných dohôd, ktoré podpísali ⁽¹¹⁾.
- (10) V tejto súvislosti Súdny dvor vysvetlil, že hoci pojem „adekvátna úroveň ochrany“ v článku 25 ods. 6 smernice 95/46/ES neznamena úroveň ochrany rovnocennú úrovni ochrany zaručenej právnym poriadkom EÚ, musí sa chápať v tom zmysle, že vyžaduje, aby táto tretia krajina zabezpečila úroveň ochrany základných práv a slobôd, ktorá je „v podstate rovnocenná“ úrovni ochrany zaručenej v rámci Únie na základe smernice 95/46/ES vykladanej v duchu Charty základných práv. Aj keď prostriedky, ktoré v tomto ohľade využíva táto tretia krajina, môžu byť rozdielne od tých, ktoré sa využívajú v rámci Únie, tieto prostriedky musia byť v praxi efektívne ⁽¹²⁾.
- (11) Súdny dvor kritizoval neexistenciu dostatočných zistení v rozhodnutí 2000/520/ES, čo sa týka existencie pravidiel štátnej povahy v USA, ktorých cieľom by bolo obmedzenie prípadných zásahov do základných práv osôb, ktorých údaje sa prenášajú z Únie do USA, teda zásahov, ktoré by subjekty verejnej moci tejto krajiny boli oprávnené uskutočniť v rámci sledovania legitímnych cieľov, akým je napríklad národná bezpečnosť, ako aj existencie účinnej právnej ochrany pred zásahmi tohto druhu ⁽¹³⁾.

⁽⁵⁾ Rozhodnutie Komisie 2000/520/ES z 26. júla 2000 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej zásadami „bezpečného prístavu“ a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA (Ú. v. ES L 215, 28.8.2000, s. 7).

⁽⁶⁾ Oznámenie Komisie Európskemu parlamentu a Rade Obnovenie dôvery v toky údajov medzi EÚ a USA, COM(2013) 846 final z 27. novembra 2013.

⁽⁷⁾ Oznámenie Komisie Európskemu parlamentu a Rade o fungovaní systému bezpečného prístavu z pohľadu občanov EÚ a spoločností usadených v EÚ, COM(2013) 847 final z 27. novembra 2013.

⁽⁸⁾ Pozri napr. Rada Európskej únie, záverečná správa kontaktnej skupiny EÚ – USA na vysokej úrovni o výmene informácií a ochrane súkromia a osobných údajov, poznámka 9831/08, 28. mája 2008, dostupná na internetovej adrese: <http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf>.

⁽⁹⁾ Správa o zisteniach európskych spolupredsedom ad hoc pracovnej skupiny EÚ – USA pre ochranu údajov, 27. novembra 2013, dostupná na internetovej adrese: <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>.

⁽¹⁰⁾ Pozri poznámku pod čiarou č. 3.

⁽¹¹⁾ Vec Schrems, bod 97.

⁽¹²⁾ Vec Schrems, body 73 – 74.

⁽¹³⁾ Vec Schrems, body 88 – 89.

- (12) V roku 2014 Komisia začala rokovať s orgánmi USA s cieľom prediskutovať posilnenie systému bezpečného prístavu v súlade s 13 odporúčaniami uvedenými v oznámení COM(2013) 847 final. Po rozsudku Súdneho dvora Európskej únie vo veci Schrems sa tieto rozhovory ešte zintenzívnili s cieľom dospieť k možnému novému rozhodnutiu o primeranosti, ktoré by spĺňalo požiadavky článku 25 smernice 95/46/ES podľa výkladu Súdneho dvora. Výsledkom týchto diskusií sú dokumenty, ktoré sú pripojené k tomuto rozhodnutiu a budú uverejnené aj vo Federálnom registri USA. Zásady ochrany súkromia (príloha II) spolu s oficiálnymi vyhláseniami a záväzkami rôznych orgánov USA, ktoré sa nachádzajú v dokumentoch v prílohách I, III až VII, tvoria „štít na ochranu osobných údajov medzi EÚ a USA“.
- (13) Komisia dôkladne analyzovala zákony a prax v USA vrátane týchto oficiálnych vyhlásení a záväzkov. Na základe zistení uvedených v odôvodneniach 136 – 140 Komisia dospela k záveru, že USA zaisťujú primeranú úroveň ochrany osobných údajov prenášaných v rámci štítu na ochranu osobných údajov medzi EÚ a USA z Únie organizáciám v USA, ktoré osvedčili svoje dodržiavanie zásad štítu.

2. „ŠTÍT NA OCHRANU OSOBNÝCH ÚDAJOV MEDZI EÚ a USA“

- (14) Štít na ochranu osobných údajov medzi EÚ a USA je založený na systéme osvedčení samotnými spoločnosťami, v rámci ktorého sa organizácie v USA zaviazujú dodržiavať súbor zásad ochrany súkromia – rámcových zásad štítu na ochranu osobných údajov medzi EÚ a USA vrátane doplnkových zásad (ďalej spoločne: „zásady“) – vydaných Ministerstvom obchodu USA, ktoré sú uvedené v prílohe II k tomuto rozhodnutiu. Vzťahuje sa na prevádzkovateľov aj spracovateľov (zástupcov), pričom osobitosť spočíva v tom, že spracovatelia sa musia zmluvne zaviazovať, že budú konať len na pokyny prevádzkovateľa z EÚ a pomáhať mu pri odpovedaní fyzickým osobám, ktoré si uplatnia svoje práva v zmysle zásad ⁽¹⁴⁾.
- (15) Bez toho, aby bolo dotknuté dodržiavanie vnútroštátnych ustanovení prijatých podľa smernice 95/46/ES, má toto rozhodnutie za následok, že sa povoľujú prenosy od prevádzkovateľa alebo spracovateľa v Únii organizáciám v USA, ktoré ministerstvu obchodu osvedčili svoje dodržiavanie zásad a zaviazali sa k ich dodržiavaniu. Zásady sa vzťahujú výlučne na spracovanie osobných údajov zo strany organizácie v USA, pokiaľ spracovanie zo strany takýchto organizácií nepatrí do rozsahu pôsobnosti právnych predpisov Únie ⁽¹⁵⁾. Štít na ochranu osobných údajov nemá vplyv na uplatňovanie právnych predpisov Únie, ktorými sa upravuje spracovanie osobných údajov v členských štátoch ⁽¹⁶⁾.

⁽¹⁴⁾ Pozri odd. III ods. 10 písm. a) prílohy II. V súlade s vymedzením v odd. I.8.c. stanoví prevádzkovateľ z EÚ účel a prostriedky spracovania osobných údajov. V zmluve so zástupcom sa navyše musí objasniť, či sa povoľujú ďalšie prenosy [pozri odd. III ods. 10 písm. a) bod ii.2)].

⁽¹⁵⁾ Platí to aj v prípade, ak sa to týka údajov o ľudských zdrojoch prenášaných z Únie v súvislosti s pracovnoprávnym vzťahom. Hoci v zásadách sa zdôrazňuje „prvotná zodpovednosť“ zamestnávateľa z EÚ [pozri odd. III ods. 9 písm. d) bod i) prílohy II], zároveň sa v nich vysvetľuje, že na jeho konanie sa budú vzťahovať pravidlá platné v Únii a/alebo príslušnom členskom štáte, a nie zásady. Pozri odd. III ods. 9 písm. a) bod i), písm. b) bod ii, písm. c) bod i), písm. d) bod i) prílohy II.

⁽¹⁶⁾ Vzťahuje sa to aj na spracovanie, ktoré sa uskutočňuje zariadením nachádzajúcim sa v Únii, ktoré však používa organizácia so sídlom mimo Únie (pozri článok 4 ods. 1 písm. c) smernice 95/46/ES). Všeobecné nariadenie o ochrane údajov sa bude od 25. mája 2018 vzťahovať na spracovanie osobných údajov i) v kontexte činností prevádzkarne prevádzkovateľa alebo spracovateľa v Únii (aj keď sa spracovanie uskutočňuje v USA); alebo ii) dotknutých osôb, ktoré sú v Únii, zo strany prevádzkovateľa alebo spracovateľa, ktorý nemá sídlo v Únii, ak sa činnosti spracovania týkajú a) ponuky tovarov alebo služieb takýmto dotknutým osobám v Únii bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba; alebo b) monitorovania ich konania, pokiaľ k ich konaniu dochádza v Únii. Pozri článok 3 ods. 1 a 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracovávaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

- (16) Ochrana, ktorá sa osobným údajom poskytuje v rámci štítu na ochranu osobných údajov, sa vzťahuje na každú dotknutú osobu z EÚ ⁽¹⁷⁾, ktorej osobné údaje boli prenesené z Únie organizáciám v USA, ktoré ministerstvu obchodu osvedčili svoje dodržiavanie zásad.
- (17) Zásady sa uplatňujú ihneď po osvedčení. Jedna výnimka sa týka zásady zodpovednosti za ďalší prenos v prípade, že organizácia, ktorá osvedčuje svoje dodržiavanie zásad štítu na ochranu osobných údajov, už má predchádzajúce obchodné vzťahy s tretími stranami. Vzhľadom na skutočnosť, že zosúladienie týchto obchodných vzťahov s pravidlami platnými v zmysle zásady zodpovednosti za ďalší prenos môže trvať istý čas, organizácia bude povinná to urobiť čo najskôr a v každom prípade najneskôr deväť mesiacov po poskytnutí osvedčenia (za predpokladu, že k tomu dôjde v prvých dvoch mesiacoch po dni, keď štít na ochranu osobných údajov nadobudne platnosť). Organizácia musí počas tohto prechodného obdobia uplatňovať zásadu oznámenia a možnosti voľby (teda umožniť dotknutej osobe z EÚ vyjadriť nesúhlas) a, ak sa osobné údaje prenášajú tretej strane konajúcej ako zástupca, musí zaistiť, aby zástupca zabezpečil aspoň rovnakú úroveň ochrany, aká sa požaduje v zásadách ⁽¹⁸⁾. Týmto prechodným obdobím sa zabezpečuje odôvodnená a primeraná rovnováha medzi dodržiavaním základného práva na ochranu osobných údajov a oprávnenými potrebami podnikov získať dostatočný čas na prispôbenie sa novému rámcu, pričom to závisí aj od ich obchodných vzťahov s tretími stranami.
- (18) Tento systém bude spravovať a monitorovať ministerstvo obchodu na základe svojich záväzkov stanovených vo vyhláseniach ministra obchodu USA (príloha I k tomuto rozhodnutiu). Pokiaľ ide o presadzovanie zásad, Federálna obchodná komisia (Federal Trade Commission – FTC) a ministerstvo dopravy vydali vyhlásenia, ktoré sú uvedené v prílohe IV a prílohe V k tomuto rozhodnutiu.

2.1. Zásady ochrany súkromia

- (19) V rámci osvedčenia na základe štítu na ochranu osobných údajov medzi EÚ a USA sa organizácie musia zaviazat k dodržiavaniu zásad ⁽¹⁹⁾.
- (20) Podľa zásady oznámenia sú organizácie povinné poskytnúť dotknutým osobám informácie o niekoľkých kľúčových prvkoch týkajúcich sa spracovania ich osobných údajov (napr. o druhu zhromaždených údajov, účele spracovania, práve na prístup a voľbu, podmienkach ďalších prenosov a zodpovednosti). Uplatňujú sa aj ďalšie záruky, najmä požiadavka, aby organizácie zverejňovali svoje podmienky ochrany súkromia (ktoré odzrkadľujú zásady) a aby uvádzali odkazy na webové sídlo ministerstva obchodu (s ďalšími podrobnosťami o osvedčovaní, právach dotknutých osôb a dostupných opravných mechanizmoch), zoznam organizácií zapojených do štítu na ochranu osobných údajov (uvedený v odôvodnení 30) a webové sídlo príslušného poskytovateľa alternatívneho riešenia sporov.
- (21) Podľa zásady integrity údajov a obmedzenia účelu musia byť osobné údaje obmedzené na to, čo je relevantné na účely spracovania, spoľahlivé na svoje určené použitie, presné, úplné a aktuálne. Organizácia nesmie spracúvať osobné údaje spôsobom, ktorý je nezlučiteľný s účelom, na ktorý boli pôvodne zhromaždené alebo ktorý bol následne schválený dotknutou osobou. Organizácie musia zaistiť, aby boli osobné údaje spoľahlivé na svoje plánované použitie, presné, úplné a aktuálne.

⁽¹⁷⁾ Toto rozhodnutie má význam pre EHP. V Dohode o Európskom hospodárskom priestore (Dohoda o EHP) sa stanovuje rozšírenie vnútorného trhu Európskej únie na tri štáty EHP – Island, Lichtenštajnsko a Nórsko. Na právne predpisy Únie v oblasti ochrany osobných údajov vrátane smernice 95/46/ES sa vzťahuje Dohoda o EHP a tieto predpisy boli začlenené do prílohy XI k tejto dohode. O začleníení tohto rozhodnutia do Dohody o EHP musí rozhodnúť Spoločný výbor EHP. Keď sa bude toto rozhodnutie vzťahovať na Island, Lichtenštajnsko a Nórsko, do štítu na ochranu osobných údajov medzi EÚ a USA budú patriť aj tieto tri krajiny a odkazy v balíku dokumentov týkajúcom sa štítu na ochranu osobných údajov na EÚ a jej členské štáty sa budú chápať tak, že zahŕňajú aj Island, Lichtenštajnsko a Nórsko.

⁽¹⁸⁾ Pozri odd. III ods. 6 písm. e) prílohy II.

⁽¹⁹⁾ Na údaje v oblasti ľudských zdrojov zhromaždené v súvislosti s pracovným pomerom sa vzťahujú osobitné pravidlá, ktoré poskytujú dodatočné záruky a sú stanovené v doplnkovej zásade „Údaje v oblasti ľudských zdrojov“ v rámci zásad ochrany súkromia (pozri odd. III ods. 9 prílohy II). Zamestnávateľia by napríklad mali vyhovieť zamestnancom uprednostňujúcim ochranu svojho súkromia obmedzením prístupu k ich osobným údajom, anonymizovaním určitých údajov alebo pridelením kódov alebo pseudonymov. A čo je najdôležitejšie, organizácie sú povinné spolupracovať a dodržiavať rady orgánov EÚ na ochranu údajov, pokiaľ ide o tieto údaje.

- (22) Ak je nový (zmenený) účel značne odlišný, ale naďalej zlučiteľný s pôvodným účelom, *zásadou možnosti voľby* sa dotknutým osobám poskytuje právo na vznesenie námietky (vyjadrenie nesúhlasu). *Zásada možnosti voľby* nenahrádza výslovný zákaz nezlučiteľného spracovania ⁽²⁰⁾. Osobitné pravidlá, ktorými sa vo všeobecnosti umožňuje „kedykoľvek“ vyjadriť nesúhlas s použitím osobných údajov, sa vzťahujú na priamy marketing ⁽²¹⁾. V prípade citlivých údajov musia organizácie obvykle získať potvrdzujúci výslovný súhlas dotknutej osoby (vyjadrenie súhlasu).
- (23) V rámci *zásady integrity údajov a obmedzenia účelu* možno osobné informácie uchovávať vo forme, ktorou sa fyzická osoba identifikuje alebo ktorá ju robí identifikovateľnou (a teda vo forme osobných údajov), len pokiaľ to slúži na účel (účely), na ktorý(-é) boli pôvodne zhromaždené alebo ktorý bol následne odsúhlasený. Táto povinnosť nebráni organizáciám zapojeným do štítu na ochranu osobných údajov v tom, aby pokračovali v spracovávaní osobných informácií dlhší čas, ale len počas obdobia a v rozsahu, v akom takéto spracovanie odôvodnene slúži na jeden z týchto osobitných účelov: archivácia, žurnalistika, literatúra a umenie, vedecký a historický výskum a štatistická analýza. Dlhšie uchovávanie osobných údajov na jeden z týchto účelov bude podliehať zárukám stanoveným v zásadách.
- (24) Podľa *zásady bezpečnosti* organizácie, ktoré vytvárajú, uchovávajú, využívajú alebo rozširujú osobné údaje, musia prijať „primerané a vhodné“ bezpečnostné opatrenia s ohľadom na riziká spojené so spracovaním údajov a ich povahou. V prípade spracovania údajov subdodávateľom musia organizácie uzavrieť so subdodávateľom zmluvu, ktorou sa zaručí rovnaká úroveň ochrany, akú poskytujú zásady, a musia prijať opatrenia na zabezpečenie jej riadneho vykonávania.
- (25) Podľa *zásady prístupu* ⁽²²⁾ majú dotknuté osoby právo bez nutnosti odôvodnenia a len za nie príliš vysoký poplatok získať od organizácie potvrdenie o tom, či táto organizácia spracúva osobné údaje, ktoré sa ich týkajú, a získať od nej tieto údaje v primeranom čase. Toto právo možno obmedziť len vo výnimočných prípadoch; akékoľvek odopretie alebo obmedzenie práva na prístup musí byť nevyhnutné a riadne odôvodnené, pričom organizácia nesie bremeno preukazovania, že tieto požiadavky sú splnené. Dotknuté osoby musia mať možnosť opraviť, zmeniť alebo vymazať osobné informácie, ak sú nepresné alebo boli spracované v rozpore so zásadami. V oblastiach, v ktorých sa spoločnosti s najväčšou pravdepodobnosťou uchýľujú k automatizovanému spracovaniu osobných údajov v záujme prijatia rozhodnutí, ktoré sa dotýkajú danej fyzickej osoby (napríklad poskytovanie úverov, ponuky hypoték, zamestnanie), sa v právnych predpisoch USA poskytujú osobitné ochranné prvky pred nepriaznivými rozhodnutiami ⁽²³⁾. V týchto zákonoch sa obvykle stanovuje, že fyzické osoby majú právo byť informované o osobitných dôvodoch, na základe ktorých sa rozhodnutie (napríklad zamietnutie úveru) prijalo, právo namietať proti neúplným alebo nepresným informáciám (ako aj proti opieraniu sa o nezákonné faktory) a právo dožadovať sa nápravy. Tieto pravidlá ponúkajú ochranu v pravdepodobne dosť obmedzenom počte prípadov, v ktorých by automatizované rozhodnutia prijala samotná organizácia zapojená do štítu na ochranu osobných údajov ⁽²⁴⁾. Vzhľadom na rastúce používanie automatizovaného spracovania (vrátane profilovania) ako základu pre prijímanie rozhodnutí, ktoré majú v modernom digitálnom hospodárstve vplyv na fyzické osoby, však ide o oblasť, ktorú treba dôkladne monitorovať. S cieľom uľahčiť toto monitorovanie sa s orgánmi USA dohodlo, že súčasťou prvého každoročného preskúmania a v prípade potreby aj následných preskúmaní bude dialóg o automatizovanom rozhodovaní vrátane komunikácie o podobných a rozdielnych prvkoch v prístupe EÚ a USA v tomto ohľade.

⁽²⁰⁾ Týka sa to všetkých prenosov údajov v rámci štítu na ochranu osobných údajov vrátane prípadov, keď sa prenosy týkajú údajov zhromaždených prostredníctvom pracovnoprávného vzťahu. Hoci organizácia z USA, ktorá osvedčila svoje dodržiavanie zásad, môže v zásade používať údaje o ľudských zdrojoch na iné účely, ktoré nesúvisia s pracovnoprávnym pomerom (napríklad určité marketingové oznámenia), musí dodržiavať zákaz nezlučiteľného spracovania a okrem toho to môže robiť len v súlade so *zásadou oznámenia* a *zásadou možnosti voľby*. Zákazom toho, aby organizácie v USA prijali akékoľvek represívne opatrenie voči zamestnancovi za vykonanie takejto voľby vrátane akéhokoľvek obmedzenia pracovných príležitostí, sa zaisťuje, že napriek vzťahu podriadenosti a súvisiacej závislosti sa na zamestnanca nebude vyvíjať tlak, a tak bude môcť vykonať skutočnú slobodnú voľbu.

⁽²¹⁾ Pozri odd. III ods. 12 prílohy II.

⁽²²⁾ Pozri aj doplnkovú zásadu „Prístup“ (odd. III ods. 8 prílohy II).

⁽²³⁾ Pozri napríklad zákon o rovnakých úverových príležitostiach (Equal Credit Opportunity Act – ECOA, 15 U.S.C. 1691 a nasl.), zákon o náležitom podávaní informácií o úverovej schopnosti (Fair Credit Reporting Act – FCRA, 15 USC § 1681 a nasl.), alebo zákon o spravodlivom bývaní (Fair Housing Act – FHA, 42 U.S.C. 3601 a nasl.).

⁽²⁴⁾ V súvislosti s prenosom osobných údajov, ktoré boli zhromaždené v EÚ, bude mať zmluvný vzťah s danou fyzickou osobou (zákazníkom) vo väčšine prípadov prevádzkovateľ v EÚ, ktorý musí dodržiavať pravidlá EÚ v oblasti ochrany osobných údajov – a teda každé rozhodnutie na základe automatizovaného spracovania obvykle prijme tento prevádzkovateľ v EÚ. Ide okrem iného o scenáre, pri ktorých spracovanie vykonáva organizácia zapojená do štítu na ochranu osobných údajov, ktorá koná ako zástupca v mene prevádzkovateľa v EÚ.

- (26) Podľa *zásady nápravy, presadzovania a zodpovednosti* ⁽²⁵⁾ musia zúčastnené organizácie vytvoriť spoľahlivé mechanizmy na zabezpečenie dodržiavania ostatných zásad a mechanizmy nápravy pre dotknuté osoby z EÚ, ktorých osobné údaje boli spracované nevyhovujúcim spôsobom, a to vrátane účinných opravných prostriedkov. Keď sa organizácia dobrovoľne rozhodne predložiť osvedčenie ⁽²⁶⁾ v rámci štítu na ochranu osobných údajov medzi EÚ a USA, je povinná zásady skutočne dodržiavať. Ak chce byť táto organizácia naďalej súčasťou štítu na ochranu osobných údajov, aby mohla získavať osobné údaje z Únie, musí každoročne opätovne osvedčovať svoju účasť v tomto rámci. Organizácie musia zároveň prijať opatrenia na overenie ⁽²⁷⁾, či sú ich zverejnené podmienky ochrany súkromia v súlade so zásadami a či sa skutočne dodržiavajú. Môžu to vykonať buď prostredníctvom systému posúdenia samotnou organizáciou, ktorý musí zahŕňať interné postupy na zabezpečenie odbornej prípravy zamestnancov zameranej na uplatňovanie podmienok ochrany súkromia organizácie a pravidelného preskúmania ich dodržiavania objektívnym spôsobom, alebo prostredníctvom externých posúdení dodržiavania, ktorých metódy môžu zahŕňať audit alebo náhodné kontroly. Organizácia musí navyše zaviesť účinný nápravný mechanizmus na riešenie sťažností (v tejto súvislosti pozri aj odôvodnenie 43) a musí podliehať vyšetrovacím právomociam a právomociam presadzovania práva FTC, ministerstva dopravy alebo iného oprávneného zákonom zriadeného orgánu USA v oblasti vyšetrovania a presadzovania, čím sa účinne zaistí dodržiavanie zásad.
- (27) Osobitné pravidlá sa vzťahujú na tzv. „ďalšie prenosy“, t. j. prenosy osobných údajov z organizácie prevádzkovateľovi alebo spracovateľovi, ktorý je treťou stranou, bez ohľadu na to, či sa tento prevádzkovateľ alebo spracovateľ nachádza v USA alebo v tretej krajine mimo USA (a Únie). Účelom týchto pravidiel je zaistiť, aby ochrana, ktorá je zaručená pre osobné údaje dotknutých osôb z EÚ, nebola narušená a nebolo ju možné obísť prostredníctvom ďalšieho prenosu tretím stranám. Je to osobitné dôležité v komplexnejších spracovateľských reťazcoch, ktoré sú typické pre dnešné digitálne hospodárstvo.
- (28) V zmysle *zásady zodpovednosti za ďalší prenos* ⁽²⁸⁾ môže každý ďalší prenos prebiehať iba i) na obmedzené a konkrétne účely; ii) na základe zmluvy (alebo porovnateľnej dohody v rámci skupiny podnikov ⁽²⁹⁾) a iii) iba v prípade, že táto zmluva poskytuje rovnakú úroveň ochrany, ako je ochrana zaručená zásadami, čo zahŕňa požiadavku, že uplatnenie zásad sa môže obmedzovať iba v rozsahu potrebnom na splnenie účelov týkajúcich sa národnej bezpečnosti, presadzovania práva a ostatných verejných záujmov ⁽³⁰⁾. Malo by sa to chápať v spojení so *zásadou oznámenia* a v prípade ďalšieho prenosu prevádzkovateľovi, ktorý je treťou stranou ⁽³¹⁾, so *zásadou možnosti voľby*, podľa ktorých musia byť dotknuté osoby informované (okrem iného) o type/totožnosti každého príjemcu, ktorý je treťou stranou, účele ďalšieho prenosu, ako aj o ponúkanej možnosti voľby a môžu namietať (vyjadriť nesúhlas) alebo, v prípade citlivých údajov, musia poskytnúť „potvrdzujúci výslovný súhlas“ (vyjadrenie súhlasu) s ďalšími prenosmi. Vzhľadom na *zásadu integrity údajov a obmedzenia účelu* sa povinnosťou poskytnúť rovnakú úroveň ochrany, aká sa zaručuje zásadami, stanovuje, že tretia strana môže spracovávať len osobné informácie, ktoré jej boli postúpené na účely, ktoré sú zlučiteľné s účelmi, na ktoré boli pôvodne zhromaždené, alebo na ktoré dala fyzická osoba následne súhlas.
- (29) Povinnosť poskytnúť rovnakú úroveň ochrany, aká sa vyžaduje v zásadách, sa vzťahuje na všetky tretie strany zapojené do spracovania takto prenášaných údajov bez ohľadu na to, kde sa nachádzajú (v USA alebo inej tretej krajine), ako aj v prípade, keď samotný pôvodný príjemca, ktorý je treťou stranou, vykoná prenos týchto údajov inému príjemcovi – tretej strane, napríklad na účely spracovania subdodávateľom. Vo všetkých prípadoch sa musí v zmluve s príjemcom, ktorý je treťou stranou, stanoviť, že tento príjemca upovedomí organizáciu zapojenú do štítu na ochranu osobných údajov v prípade, že rozhodne, že túto povinnosť už nemôže splňať. Spracovanie

⁽²⁵⁾ Pozri aj doplnkovú zásadu „Riešenie sporov a presadzovanie“ (odd. III ods. 11 prílohy II).

⁽²⁶⁾ Pozri aj doplnkovú zásadu „Osvedčenie vydávané samotnou organizáciou“ (odd. III ods. 6 prílohy II).

⁽²⁷⁾ Pozri aj doplnkovú zásadu „Overovanie“ (odd. III ods. 7 prílohy II).

⁽²⁸⁾ Pozri aj doplnkovú zásadu „Povinné uzavretie zmlúv pre ďalšie prenosy“ (odd. III ods. 10 prílohy II).

⁽²⁹⁾ Pozri doplnkovú zásadu „Povinné uzavretie zmlúv pre ďalšie prenosy“ [odd. III ods. 10 písm. b) prílohy II]. Hoci sa touto zásadou umožňujú prenosy, ktoré sa zakladajú aj na nezmluvných nástrojoch (napr. programy v rámci skupiny týkajúce sa dodržiavania predpisov a kontroly), z textu jasne vyplýva, že týmito nástrojmi sa musí vždy „zaistiť nepretržitosť ochrany osobných informácií v zmysle zásad“. Okrem toho vzhľadom na skutočnosť, že organizácia v USA, ktorá osvedčila svoje dodržiavanie zásad, zostáva zodpovednou za dodržiavanie zásad, bude mať silný motív použiť nástroje, ktoré sú v praxi skutočne účinné.

⁽³⁰⁾ Pozri odd. I ods. 5 prílohy II.

⁽³¹⁾ Fyzické osoby nebudú mať právo vyjadriť nesúhlas v prípadoch, v ktorých sa osobné údaje prenášajú tretej strane, ktorá koná ako zástupca vykonávajúci úlohy v mene organizácie v USA na základe jej pokynov. To si však vyžaduje zmluvu so zástupcom a organizácia v USA bude niesť zodpovednosť za zaručenie ochrany stanovenej v zásadách tým, že uplatní svoje právomoci vydať pokyny.

treťou stranou sa pri takomto rozhodnutí ukončí, prípadne je potrebné prijať iné odôvodnené a primerané kroky s cieľom napraviť túto situáciu ⁽³²⁾. Ak vzniknú problémy s dodržaním tejto zásady v (subdodávateľskom) spracovateľskom reťazci, organizácia zapojená do štítu na ochranu osobných údajov pôsobiaca ako prevádzkovateľ osobných údajov bude musieť preukázať, že nie je zodpovedná za udalosť, ktorá viedla k vzniku škody, inak bude niesť zodpovednosť, ako je uvedené v *zásade nápravy, presadzovania a zodpovednosti*. V prípade ďalšieho prenosu zástupcovi, ktorý je treťou stranou, sa uplatňujú ďalšie ochranné opatrenia ⁽³³⁾.

2.2. Transparentnosť a správa štítu na ochranu osobných údajov medzi EÚ a USA a dohľad nad ním

- (30) Štítom na ochranu osobných údajov medzi EÚ a USA sa zabezpečujú mechanizmy dohľadu a presadzovania s cieľom zaistiť, aby spoločnosti z USA, ktoré osvedčili dodržiavanie zásad, zásady dodržiavali a aby sa riešilo každé nedodržanie zásad, a overiť, či sa tak robí. Tieto mechanizmy sú vymedzené v zásadách (príloha II) a v záväzkoch, ktoré prijalo ministerstvo obchodu (príloha I), FTC (príloha IV) a ministerstvo dopravy (príloha V).
- (31) V záujme riadneho uplatňovania štítu na ochranu osobných údajov medzi EÚ a USA musia zainteresované strany, napríklad dotknuté osoby, vývozcovia údajov a vnútroštátne orgány pre ochranu osobných údajov, byť schopné určiť tie organizácie, ktoré dodržiavajú zásady. S týmto cieľom ministerstvo obchodu vzalo na seba povinnosť viesť a sprístupňovať verejnosti zoznam organizácií, ktoré osvedčili svoje dodržiavanie zásad a ktoré patria do jurisdikcie prinajmenšom jedného z orgánov presadzovania práva uvedených v prílohách I a II k tomuto rozhodnutiu (ďalej len „zoznam organizácií zapojených do štítu na ochranu osobných údajov“) ⁽³⁴⁾. Ministerstvo obchodu bude tento zoznam aktualizovať na základe predložených informácií o každoročnom opätovnom osvedčení organizácie a vždy, keď organizácia opustí štít na ochranu osobných údajov medzi EÚ a USA alebo z neho bude vyradená. Takisto bude viesť a sprístupňovať verejnosti oficiálne záznamy o organizáciách, ktoré boli vyradené zo zoznamu, pričom v každom prípade uvedie dôvod vyradenia. A napokon poskytne hypertextový odkaz na zoznam prípadov FTC súvisiacich s presadzovaním štítu na ochranu osobných údajov, ktorý sa nachádza na webovom sídle FTC.
- (32) Zoznam organizácií zapojených do štítu na ochranu osobných údajov a opätovné osvedčenia zverejní ministerstvo obchodu na vyhradenom webovom sídle. Organizácie, ktoré osvedčili svoje dodržiavanie zásad, musia zase ministerstvu poskytnúť webovú adresu do zoznamu organizácií zapojených do štítu na ochranu osobných údajov. Navyše, ak sú podmienky ochrany súkromia organizácie dostupné on-line, musia obsahovať hypertextový odkaz na webové sídlo štítu na ochranu osobných údajov, ako aj hypertextový odkaz na webové sídlo alebo formulár na podanie sťažnosti v rámci nezávislého mechanizmu nápravy, ktorý je k dispozícii na vyšetrovanie nevyriešených sťažností. Ministerstvo obchodu bude v súvislosti s osvedčením a opätovným osvedčením organizácie v tomto rámci systematicky overovať súlad jej podmienok ochrany súkromia so zásadami.
- (33) Organizácie, ktoré trvalo nedodržiavajú zásady, budú vyradené zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov a budú musieť vrátiť alebo vymazať osobné údaje, ktoré získali v rámci štítu na ochranu osobných údajov medzi EÚ a USA. V ostatných prípadoch vyradenia, napríklad v prípade dobrovoľného stiahnutia z účasti alebo nepredloženia opakovaného osvedčenia, si organizácia môže ponechať tieto údaje, ak každoročne ministerstvu obchodu potvrdí svoje odhodlanie pokračovať v dodržiavaní zásad alebo poskytne primeranú ochranu osobných údajov inými povolenými prostriedkami (napr. prostredníctvom zmluvy, ktorá plne odzrkadľuje požiadavky príslušných štandardných zmluvných doložiek schválených Komisiou). V takom prípade musí organizácia určiť kontaktné miesto v rámci organizácie pre všetky otázky súvisiace so štítom na ochranu osobných údajov.
- (34) Ministerstvo obchodu bude monitorovať organizácie, ktoré už nie sú členmi štítu na ochranu osobných údajov medzi EÚ a USA buď preto, lebo ho dobrovoľne opustili, alebo preto, lebo platnosť ich osvedčenia uplynula, s cieľom overiť, či vrátia, vymažú alebo si ponechajú ⁽³⁵⁾ osobné údaje zhromaždené v minulosti na základe tohto

⁽³²⁾ Situácia sa líši v závislosti od toho, či je tretia strana prevádzkovateľom alebo spracovateľom (zástupcom). Pri prvom scenári sa v zmluve s treťou stranou musí stanoviť, že tretia strana ukončí spracovanie alebo prijme iné odôvodnené a primerané kroky s cieľom napraviť situáciu. Pri druhom scenári je prijatie týchto opatrení na organizácii zapojenej do štítu na ochranu osobných údajov – ako tej, ktorá má kontrolu nad spracovaním a podľa pokynov ktorej zástupca koná.

⁽³³⁾ Organizácia v USA musí v takom prípade takisto prijať odôvodnené a primerané kroky i) s cieľom zaistiť, aby zástupca účinne spracoval osobné údaje prenášané spôsobom, ktorý je v súlade s povinnosťami organizácie v zmysle zásad a ii) s cieľom zastaviť a napraviť nepovolené spracovanie na základe oznámenia.

⁽³⁴⁾ Informácie o správe zoznamu organizácií zapojených do štítu na ochranu osobných údajov možno nájsť v prílohe I a prílohe II (odd. I ods. 3, odd. I ods. 4, odd. III ods. 6 písm. d) a odd. III ods. 11 písm. g).

⁽³⁵⁾ Pozri napr. odd. I ods. 3, odd. III ods. 6 písm. f) a odd. III ods. 11 písm. g) bod i) prílohy II.

rámca. Ak si tieto údaje nechajú, organizácie majú povinnosť naďalej na ne uplatňovať zásady. V prípadoch, keď ministerstvo obchodu vyradí organizácie z rámca v dôsledku pretrvávajúceho nedodržovania zásad, zabezpečí, aby tieto organizácie vrátili alebo vymazali osobné údaje, ktoré získali na základe tohto rámca.

- (35) Ak organizácia z akéhokoľvek dôvodu opustí štít na ochranu osobných údajov medzi EÚ a USA, musí odstrániť všetky verejné vyhlásenia naznačujúce, že sa aj naďalej zúčastňuje na tomto štíte alebo že má nárok využívať jeho výhody, najmä všetky odkazy na tento štít vo svojich zverejnených podmienkach ochrany súkromia. Ministerstvo obchodu bude aktívne vyhľadávať a riešiť nepravdivé tvrdenia o účasti v rámci, a to vrátane tvrdení jeho bývalých členov ⁽³⁶⁾. Akékoľvek nepravdivé vyhlásenie pre verejnosť v súvislosti s dodržiavaním zásad organizáciou vo forme zavádzajúcich vyhlásení alebo praktík je postihnutelné zo strany FTC, ministerstva dopravy alebo iných príslušných orgánov presadzovania práva USA; nepravdivé vyhlásenia pre ministerstvo obchodu sú postihnutelné podľa zákona o nepravdivých vyhláseniach (18 U.S.C. § 1001) ⁽³⁷⁾.
- (36) Ministerstvo obchodu bude *ex officio* monitorovať všetky nepravdivé tvrdenia o účasti v štíte na ochranu osobných údajov alebo prípady neoprávneného používania certifikačnej značky štítu, pričom orgány pre ochranu osobných údajov môžu navrhnúť preskúmanie organizácií na vyhradenom kontaktnom mieste na ministerstve. Keď organizácia opustí štít na ochranu osobných údajov medzi EÚ a USA, opätovne nepredloží osvedčenie alebo je vyradená zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov, ministerstvo obchodu bude priebežne overovať, či zo svojich zverejnených podmienok ochrany súkromia odstránila všetky odkazy na štít na ochranu osobných údajov, ktoré by naznačovali jej pokračujúcu účasť, a, ak bude naďalej zverejňovať nepravdivé vyhlásenia, postúpi prípad FTC, ministerstvu dopravy alebo inému príslušnému orgánu, ktorý môže začať konanie. Jeho úlohou bude aj posilať dotazníky organizáciám, platnosť osvedčenia ktorých uplynula alebo ktoré dobrovoľne opustili štít na ochranu osobných údajov medzi EÚ a USA, aby overilo, či organizácia vráti alebo vymaže osobné údaje alebo či bude naďalej uplatňovať zásady ochrany súkromia na tieto osobné údaje, ktoré získala počas účasti na štíte, a, ak si organizácia osobné údaje nechá, overí, kto v rámci organizácie bude naďalej slúžiť ako kontaktné miesto pre otázky súvisiace so štítom na ochranu osobných údajov.
- (37) Ministerstvo obchodu bude priebežne vykonávať *ex officio* preskúmanie dodržiavania zásad ⁽³⁸⁾ organizáciami, ktoré osvedčili svoje dodržiavanie zásad, okrem iného aj prostredníctvom zasielania podrobných dotazníkov. Bude takisto systematicky vykonávať preskúmania, a to vždy, keď dostane konkrétnu (opodstatnenú) sťažnosť, keď organizácia neposkytne uspokojivé odpovede na jeho otázky, alebo keď sa vyskytnú vierohodné dôkazy naznačujúce, že organizácia možno nedodríava zásady. Ministerstvo obchodu bude v prípade potreby viesť konzultácie týkajúce sa týchto preskúmaní dodržiavania zásad aj s orgánmi pre ochranu osobných údajov.

2.3. Mechanizmy nápravy, vybavovanie sťažností a presadzovania

- (38) V rámci štítu na ochranu osobných údajov medzi EÚ a USA sa od organizácií prostredníctvom *zásady nápravy, presadzovania a zodpovednosti* požaduje, aby fyzickým osobám, ktorých sa nedodržanie zásad dotýka, poskytli možnosť nápravy, a teda možnosť pre dotknuté osoby z EÚ podať sťažnosti v súvislosti s nedodržaním zásad zo strany spoločností v USA, ktoré osvedčili svoje dodržiavanie zásad, a dosiahnuť vybavenie týchto sťažností, v prípade potreby aj na základe rozhodnutia poskytujúceho účinný opravný prostriedok.
- (39) Organizácie musia ako súčasť osvedčenia samotnou organizáciou splniť požiadavky zásady nápravy, presadzovania a zodpovednosti poskytnutím účinných a ľahko dostupných nezávislých mechanizmov nápravy, na základe ktorých možno sťažnosti a spory každej fyzickej osoby vyšetriť a bezodkladne vyriešiť bez toho, aby danej osobe vznikli akékoľvek náklady.
- (40) Organizácie si môžu vybrať nezávislé mechanizmy nápravy buď v Únii, alebo v USA. To zahŕňa možnosť dobrovoľne sa zaviazat k spolupráci s orgánmi pre ochranu osobných údajov v EÚ. Takáto možnosť však

⁽³⁶⁾ Pozri odd. „Vyhľadávanie nepravdivých tvrdení o zapojení do štítu a ich riešenie“ prílohy I.

⁽³⁷⁾ Pozri odd. III ods. 6 písm. h) a odd. III ods. 11 písm. f) prílohy II.

⁽³⁸⁾ Pozri prílohu I.

neexistuje v prípadoch, že organizácie spracovávajú údaje o ľudských zdrojoch, keďže spolupráca s orgánmi pre ochranu osobných údajov je potom povinná. K iným alternatívam patrí nezávislé alternatívne riešenie sporov alebo *programy ochrany súkromia* vytvorené súkromným sektorom, v prípade ktorých sú zásady o ochrane údajov začlenené do ich pravidiel. Programy ochrany súkromia musia zahŕňať účinné mechanizmy presadzovania v súlade s požiadavkami zásady nápravy, presadzovania a zodpovednosti. Organizácie majú povinnosť napraviť všetky problémy súvisiace s nedodržiavaním zásad. Takisto musia uviesť, že podliehajú vyšetrovacím právomociam a právomociam presadzovania práva FTC, ministerstva dopravy alebo iného oprávneného zákonom zriadeného orgánu USA.

- (41) Štítom na ochranu osobných údajov sa preto dotknutým osobám poskytuje niekoľko možností na presadzovania ich práv, podávanie sťažností týkajúcich sa nedodržania zásad zo strany organizácií v USA, ktoré osvedčili svoje dodržiavanie zásad, a vyriešenie ich sťažností, v prípade potreby aj na základe rozhodnutia poskytujúceho účinný opravný prostriedok. Fyzické osoby môžu sťažnosť predložiť priamo organizácii, nezávislému orgánu pre riešenie sporov určenému organizáciou, vnútroštátnym orgánom pre ochranu osobných údajov alebo FTC.
- (42) V prípadoch, keď sa ich sťažnosti nevybavia na základe žiadneho z týchto mechanizmov nápravy alebo presadzovania práva, majú fyzické osoby takisto právo využiť záväzné rozhodcovské konanie v rámci výboru pre štít na ochranu osobných údajov (príloha 1 prílohy II k tomuto rozhodnutiu). Okrem rozhodcovského výboru, v prípade ktorého sa požaduje, aby sa pred jeho využitím už vyčerpali určité opravné prostriedky, môžu fyzické osoby využiť ktorýkoľvek nápravný mechanizmus alebo všetky nápravné mechanizmy podľa vlastného výberu a nie sú povinné prednostne si zvoliť jeden mechanizmus ani dodržať osobitné poradie. Existuje však určité logické poradie, ktoré sa odporúča dodržať, ako sa uvádza ďalej.
- (43) Po prvé dotknuté osoby z EÚ môžu riešiť prípady nedodržiavania zásad prostredníctvom priamych kontaktov so *spoločnosťami v USA, ktoré osvedčili svoje dodržiavanie zásad*. V záujme uľahčenia riešenia musí organizácia zaviesť účinný nápravný mechanizmus na riešenie týchto sťažností. Podmienky ochrany súkromia organizácie musia preto obsahovať jasnú informáciu o kontaktnom mieste vnútri alebo mimo organizácie, ktoré sa bude zaoberať sťažnosťami (vrátane prípadnej prevádzkarne v Únii, ktorá môže odpovedať na otázky alebo sťažnosti), a o nezávislých mechanizmoch vybavovania sťažností.
- (44) Po prijatí sťažnosti fyzickej osoby, priamo od fyzickej osoby alebo prostredníctvom ministerstva obchodu na základe postúpenia orgánom pre ochranu osobných údajov, musí organizácia poskytnúť dotknutej osobe z EÚ odpoveď v lehote 45 dní. Táto odpoveď musí obsahovať posúdenie opodstatnenosti sťažnosti a informácie o tom, ako organizácia napraviť daný problém. Organizácie takisto musia rýchlo odpovedať na otázky a iné žiadosti o informácie od ministerstva obchodu alebo orgánu pre ochranu osobných údajov ⁽³⁹⁾ (ak sa organizácia zaviazala spolupracovať s orgánmi pre ochranu osobných údajov), ktoré sa týkajú ich dodržiavania zásad. Organizácie si musia viesť záznamy o uplatňovaní svojich podmienok ochrany súkromia a musia ich na požiadanie sprístupniť v súvislosti s vyšetrovaním alebo sťažnosťou týkajúcou sa nedodržiavania zásad nezávislému mechanizmu nápravy alebo FTC (alebo inému orgánu USA s právomocou vyšetrovať nekalé a klamlivé praktiky).
- (45) Po druhé fyzické osoby môžu tiež predložiť sťažnosť priamo *nezávislému orgánu pre riešenie sporov* (v USA alebo v Únii) určenému organizáciou, ktorý bude vyšetrovať a riešiť ich sťažnosti (pokiaľ nie sú zjavne neopodstatnené alebo nezmyselné) a bezplatne poskytovať fyzickým osobám vhodné nápravné opatrenia. Sankcie a opravné prostriedky uložené takýmto orgánom musia byť dostatočne prísne, aby sa zabezpečilo, že organizácie budú dodržiavať zásady, a mali by poskytovať spôsob, akým organizácia odstráni alebo napraviť účinky nedodržania zásad, a v závislosti od okolností aj možnosť ukončenia ďalšieho spracovania príslušných osobných údajov a/alebo ich vymazania, ako aj povinnosť zverejniť zistenia o nedodržaní zásad. Nezávislé orgány pre riešenie sporov určené organizáciou budú povinné uvádzať na svojom verejnom webovom sídle relevantné informácie o štíte na ochranu osobných údajov medzi EÚ a USA a o službách, ktoré na jeho základe poskytujú. Každý rok musia zverejniť výročnú správu so súhrnnými štatistickými údajmi o týchto službách ⁽⁴⁰⁾.

⁽³⁹⁾ Ide o spracujúci orgán určený výborom orgánov pre ochranu osobných údajov, ktorý je stanovený v doplnkovej zásade „Úloha orgánov pre ochranu osobných údajov“ (odd. III ods. 5 prílohy II).

⁽⁴⁰⁾ Výročná správa musí obsahovať: 1. celkový počet sťažností súvisiacich so štítom na ochranu osobných údajov prijatých počas sledovaného roka; 2. druhy prijatých sťažností; 3. kvalitatívne parametre riešenia sporov, napríklad čas potrebný na spracovanie sťažností a 4. výsledky prijatých sťažností, najmä počet a druh uložených opravných prostriedkov alebo sankcií.

- (46) Ministerstvo obchodu v rámci svojich postupov preskúmania dodržiavania zásad overí, či sa spoločnosti v USA, ktoré osvedčili svoje dodržiavanie zásad, skutočne zaregistrovali v nezávislých nápravných mechanizmoch, o ktorých to tvrdia. Organizácie aj zodpovedné nezávislé mechanizmy nápravy sú povinné rýchlo reagovať na otázky a žiadosti ministerstva obchodu o informácie týkajúce sa štítu na ochranu osobných údajov.
- (47) Ak organizácia nesplní rozhodnutie orgánu pre riešenie sporov alebo samoregulačného orgánu, tento orgán musí túto skutočnosť oznámiť ministerstvu obchodu a FTC (alebo inému orgánu USA s právomocou vyšetrovať nekalé alebo klamlivé praktiky), prípadne príslušnému súdu⁽⁴¹⁾. Ak organizácia odmietne vyhovieť konečnému rozhodnutiu akéhokoľvek samoregulačného orgánu, ktorý sa zaoberá ochranou súkromia, nezávislého orgánu pre riešenie sporov alebo štátneho orgánu, alebo ak tento orgán rozhodne, že organizácia často nedodržiava zásady, bude sa to považovať za pretrvávajúce nedodržiavanie zásad, pričom výsledkom bude, že ministerstvo obchodu po tom, ako organizácii, ktorá nedodržiava zásady, najprv 30 dní vopred poskytne oznámenie a príležitosť na odpoveď, vyškrtne túto organizáciu zo zoznamu⁽⁴²⁾. Ak organizácia po jej odstránení zo zoznamu naďalej tvrdí, že má osvedčenie na základe štítu na ochranu osobných údajov, ministerstvo túto záležitosť postúpi FTC alebo inému orgánu presadzovania práva⁽⁴³⁾.
- (48) Po tretie môžu fyzické osoby svoje sťažnosti podať aj vnútroštátnemu orgánu pre ochranu osobných údajov. Organizácie majú povinnosť spolupracovať pri vyšetrovaní a riešení sťažnosti zo strany orgánu pre ochranu osobných údajov, buď ak sa týka spracovávaní údajov o ľudských zdrojoch zhromaždených v rámci pracovno-právneho vzťahu, alebo ak sa príslušné organizácie dobrovoľne podrobili dohľadu orgánov pre ochranu osobných údajov. Organizácie predovšetkým musia odpovedať na otázky, dodržiavať odporúčania orgánu pre ochranu osobných údajov, a to aj v súvislosti s opravnými alebo kompenzačnými opatreniami, a predložiť orgánu pre ochranu osobných údajov písomné potvrdenie, že takéto opatrenia boli prijaté.
- (49) Orgány pre ochranu osobných údajov budú poskytovať odporúčania prostredníctvom neformálneho výboru orgánov pre ochranu osobných údajov ustanoveného na úrovni Únie⁽⁴⁴⁾, ktorý bude pomáhať zabezpečovať harmonizovaný a jednotný prístup ku konkrétnej sťažnosti. Odporúčania sa poskytnú po tom, ako obe strany sporu dostanú primeranú možnosť vyjadriť sa a poskytnúť akékoľvek dôkazy podľa svojho želania. Výbor poskytne odporúčanie tak rýchlo, ako to umožní požiadavka na náležitý proces, a spravidla do 60 dní od prijatia sťažnosti. Ak určitá organizácia do 25 dní odo dňa vydania rád nekoná v súlade s nimi a neposkytne žiadne uspokojujúce vysvetlenie omeškania, výbor oznámi svoj zámer buď predložiť záležitosť FTC (alebo inému orgánu presadzovania práva USA), alebo dospieť k záveru, že záväzok spolupracovať bol závažným spôsobom porušený. V prvom prípade to môže viesť k začatiu konania podľa oddielu 5 zákona o FTC (alebo podľa podobného zákona). V druhom prípade výbor informuje ministerstvo obchodu, ktoré posúdi odmietnutie organizácie dodržať odporúčanie výboru orgánov pre ochranu osobných údajov ako pretrvávajúce nedodržiavanie zásad, čo bude mať za následok vyradenie organizácie zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov.
- (50) Ak orgán pre ochranu osobných údajov, ktorému bola sťažnosť predložená, prijal nedostatočné alebo neprijal žiadne opatrenia na riešenie sťažnosti, má každý sťažovateľ možnosť napadnúť toto konanie (nekonanie) na vnútroštátnych súdoch príslušného členského štátu.
- (51) Fyzické osoby môžu predložiť sťažnosti orgánu pre ochranu osobných údajov dokonca aj v prípade, keď výbor orgánov pre ochranu osobných údajov nebol určený ako orgán pre riešenie sporov danej organizácie. Orgán pre ochranu osobných údajov môže v týchto prípadoch postúpiť takéto sťažnosti buď ministerstvu obchodu, alebo FTC. V záujme uľahčenia a posilnenia spolupráce v otázkach týkajúcich sa sťažností fyzických osôb a nedodržiavania zásad zo strany organizácií zapojených do štítu na ochranu osobných údajov vytvorí ministerstvo obchodu vyhradené kontaktné miesto, ktoré bude plniť úlohu sprostredkovateľa a pomáhať s otázkami orgánov pre ochranu osobných údajov týkajúcimi sa dodržiavania zásad organizáciou⁽⁴⁵⁾. FTC sa takisto zaviazala, že zriadi vyhradené kontaktné miesto⁽⁴⁶⁾ a že poskytne orgánom pre ochranu osobných údajov pomoc pri vyšetrovaní podľa zákona USA o bezpečnom internete⁽⁴⁷⁾.

⁽⁴¹⁾ Pozri odd. III ods. 11 písm. e) prílohy II.

⁽⁴²⁾ Pozri odd. III ods. 11 písm. g) prílohy II, najmä body ii) a iii).

⁽⁴³⁾ Pozri odd. „Vyhľadávanie nepravdivých tvrdení o zapojení do štítu a ich riešenie“ prílohy I.

⁽⁴⁴⁾ Orgány pre ochranu osobných údajov by mali na základe svojej kompetencie v oblasti organizovania svojej práce a vzájomnej spolupráce stanoviť rokovací poriadok neformálneho výboru orgánov pre ochranu osobných údajov.

⁽⁴⁵⁾ Pozri oddiel „Zintenzívniť spoluprácu s orgánmi pre ochranu osobných údajov“ a „Uľahčovať riešenie sťažností týkajúcich sa nedodržiavania zásad“ prílohy I a odd. III ods. 7 písm. e) prílohy II.

⁽⁴⁶⁾ Pozri prílohu IV, s. 6.

⁽⁴⁷⁾ Tamže.

- (52) Po štvrté, *ministerstvo obchodu* sa navyše zaviazalo prijímať a skúmať sťažnosti týkajúce sa nedodržiavania zásad organizáciou a vyvinúť maximálne úsilie o ich vybavenie. Na tieto účely ministerstvo obchodu stanovilo pre orgány pre ochranu osobných údajov osobitné postupy na postupovanie sťažností vyhradenému kontaktnému miestu, ich sledovanie a následnú komunikáciu so spoločnosťami s cieľom uľahčiť ich vybavovanie. V záujme urýchlenia spracovania sťažností fyzických osôb bude kontaktné miesto v otázkach dodržiavania zásad spolupracovať priamo s príslušným orgánom pre ochranu osobných údajov, a predovšetkým mu poskytne aktuálne informácie o stave sťažnosti v lehote najviac 90 dní od jej postúpenia. To umožní dotknutým osobám podávať sťažnosti týkajúce sa nedodržiavania zásad zo strany spoločností v USA, ktoré osvedčili svoje dodržiavanie zásad, priamo svojim vnútroštátnym orgánom pre ochranu osobných údajov, ktoré ich postúpia ministerstvu obchodu ako orgánu, ktorý má v USA na starosti správu štítu na ochranu osobných údajov medzi EÚ a USA. Ministerstvo obchodu sa zároveň zaviazalo predložiť v rámci každoročného preskúmania fungovania štítu na ochranu osobných údajov medzi EÚ a USA správu, ktorá v súhrnnej forme analyzuje sťažnosti prijaté za daný rok ⁽⁴⁸⁾.
- (53) Ak ministerstvo obchodu na základe svojich overení *ex officio*, na základe sťažností alebo akýchkoľvek iných informácií dospeje k záveru, že organizácia trvale nedodržiava zásady ochrany súkromia, vyradí takú organizáciu zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov. Odmietnutie vyhovieť konečnému rozhodnutiu akéhokoľvek samoregulačného orgánu, ktorý sa zaoberá ochranou súkromia, nezávislého orgánu na riešenie sporov alebo štátneho orgánu vrátane orgánu pre ochranu osobných údajov sa bude považovať za trvalé nedodržiavanie zásad.
- (54) Po piate organizácia zapojená do štítu na ochranu osobných údajov musí podliehať vyšetrovacím právomociam a právomociam presadzovania práva orgánov USA, predovšetkým *Federálnej obchodnej komisie (FTC)* ⁽⁴⁹⁾, ktoré účinne zaisťujú dodržiavanie zásad. FTC sa bude pri stanovovaní, či bol porušený oddiel 5 zákona o FTC, prioritne zaoberať prípadmi nedodržania zásad ochrany súkromia postúpenými nezávislými orgánmi pre riešenie sporov alebo samoregulačnými orgánmi, ministerstvom obchodu a orgánmi pre ochranu osobných údajov (ktoré konajú z vlastného podnetu alebo na základe sťažností) ⁽⁵⁰⁾. FTC sa zaviazala vytvoriť štandardizovaný proces postupovania, určiť kontaktné miesto v rámci svojej štruktúry na prijímanie prípadov postúpených orgánmi pre ochranu osobných údajov a vymieňať si informácie o postúpených prípadoch. Okrem toho bude prijímať sťažnosti priamo od fyzických osôb a vykonávať vyšetrovania týkajúce sa štítu na ochranu osobných údajov z vlastného podnetu, najmä ako súčasť rozsiahlejších vyšetrovaní otázok ochrany súkromia.
- (55) FTC môže presadzovať dodržiavanie zásad prostredníctvom správnych opatrení („consent orders“) a bude systematicky monitorovať dodržiavanie týchto opatrení. Ak ich organizácia nespĺní, FTC môže postúpiť prípad príslušnému súdu, ktorý môže uložiť občianskoprávne tresty a iné opravné prostriedky vrátane náhrady prípadnej ujmy spôsobenej protiprávnym konaním. Prípadne môže FTC priamo požiadať o predbežné opatrenie, súdny príkaz ukládajúci povinnosť zdržať sa určitého konania, alebo iné opravné prostriedky federálny súd. Každý „consent order“ vydaný organizácii zapojenej do štítu na ochranu osobných údajov bude obsahovať ustanovenia o predkladaní správ touto organizáciou ⁽⁵¹⁾ a organizácie budú povinné zverejniť všetky príslušné oddiely týkajúce sa štítu nachádzajúce sa vo všetkých správach o dodržiavaní zásad alebo o posúdení predložených FTC. A napokon, FTC bude viesť on-line zoznam spoločností, na ktoré sa vzťahujú správne opatrenia FTC alebo súdne príkazy v prípadoch súvisiacich so štítom na ochranu osobných údajov.
- (56) Po šieste, v prípade, že sa sťažnosť fyzickej osoby z EÚ uspokojivo nevyriešila žiadnymi inými dostupnými nápravnými mechanizmami, môže sa dovolávať záväzného rozhodcovského konania „výboru pre štít na ochranu osobných údajov“ ako nápravného mechanizmu „poslednej inštancie“. Organizácie musia fyzické osoby informovať o možnosti za istých podmienok využiť záväzné rozhodcovské konanie a sú povinné odpovedať po tom, ako osoba využila túto možnosť dorúčením oznámenia dotknutej organizácii ⁽⁵²⁾.

⁽⁴⁸⁾ Pozri oddiel „Uľahčovať riešenie sťažností týkajúcich sa nedodržiavania zásad“ prílohy I.

⁽⁴⁹⁾ Organizácia zapojená do štítu na ochranu osobných údajov musí verejne vyhlásiť svoj záväzok, že bude dodržiavať zásady, zverejňovať svoje podmienky ochrany súkromia v súlade s týmito zásadami a že ich bude v plnej miere uplatňovať. Nedodržanie tejto požiadavky je právne postihnutelné podľa oddielu 5 zákona o FTC, ktorým sa zakazujú nekalé alebo klamlivé praktiky v rámci obchodu alebo tie, ktoré majú naň vplyv.

⁽⁵⁰⁾ Na základe informácií od FTC nemá FTC právomoc vykonávať inšpekcie na mieste v oblasti ochrany súkromia. Má však právomoc vyžadovať od organizácií, aby vypracovali dokumenty a poskytli svedecké výpovede (pozri oddiel 20 zákona o FTC) a v prípade nesplnenia týchto požiadaviek môže v záujme ich presadenia využiť súdny systém.

⁽⁵¹⁾ Správnymi opatreniami FTC alebo súdnymi príkazmi sa môže od spoločností vyžadovať, aby zaviedli programy ochrany súkromia a pravidelne predkladali FTC správy alebo posúdenia nezávislých tretích strán týkajúce sa plnenia týchto programov.

⁽⁵²⁾ Pozri odd. III ods. 1 bod xi) a odd. III ods. 7 písm. c) prílohy II.

- (57) Tento rozhodcovský výbor sa vytvorí zo skupiny najmenej 20 rozhodcov určených ministerstvom obchodu a Komisiou na základe ich nezávislosti, poctivosti, ako aj skúseností s právnymi predpismi USA a Únie v oblasti ochrany osobných údajov. V každom jednotlivom spore strany vyberú z tejto skupiny výbor zložený z jedného alebo troch ⁽⁵³⁾ rozhodcov. Konanie sa bude riadiť štandardnými pravidlami rozhodcovského konania, na ktorých sa dohodnú ministerstvo obchodu a Komisia. Týmto pravidlami sa doplní už uzatvorený rámec, ktorý obsahuje niekoľko prvkov, ktorými sa posilňuje prístupnosť tohto mechanizmu pre dotknuté osoby z EÚ: i) pri príprave sťažnosti výboru môže dotknutej osobe pomôcť príslušný vnútroštátny orgán pre ochranu osobných údajov; ii) keďže rozhodcovské konanie sa bude konať v USA, dotknuté osoby z EÚ sa môžu rozhodnúť zúčastniť sa prostredníctvom videokonferencie alebo telefonической konferencie, a to bez toho, aby im tým vznikli nejaké náklady; iii) keďže jazykom, ktorý sa bude používať v rozhodcovskom konaní, bude spravidla angličtina, tlmočenie a preklad v rámci rozhodcovského konania sa dotknutej osobe poskytnú štandardne ⁽⁵⁴⁾ na základe odôvodnenej žiadosti a bezplatne; iv) a napokon, hoci každý účastník si náklady na právneho zástupcu hradí sám, ak je zastúpený pred výborom právnym zástupcom, ministerstvo obchodu zriadi fond s ročnými príspevkami od organizácií zapojených do štítu na ochranu osobných údajov, z ktorého sa budú hradí oprávnené trovy rozhodcovského konania až do maximálnej sumy, ktorú stanovujú orgány USA po konzultácii s Komisiou.
- (58) Výbor pre štít na ochranu osobných údajov bude mať právomoc uložiť „nepenažnú spravodlivú náhradu pre konkrétnu osobu“ ⁽⁵⁵⁾ potrebnú na nápravu nedodržania zásad. Hoci výbor pri rozhodovaní zohľadní aj iné opravné prostriedky už zhromaždené prostredníctvom iných mechanizmov v rámci štítu na ochranu osobných údajov, fyzické osoby môžu vždy využiť rozhodcovské konanie, ak sa domnievajú, že tieto iné opravné prostriedky sú nedostatočné. To umožní dotknutým osobám z EÚ využiť rozhodcovské konanie vo všetkých prípadoch, keď sa v dôsledku konania alebo nekonania príslušných orgánov USA (napríklad FTC) uspokojivo nevyriešia ich sťažnosti. Rozhodcovského konania sa nemožno dovolávať, ak má orgán pre ochranu osobných údajov podľa právnych predpisov právomoc riešiť danú sťažnosť týkajúcu sa spoločnosti v USA, ktorá osvedčila svoje dodržiavanie zásad, najmä v tých prípadoch, kde je organizácia buď povinná spolupracovať a dodržiavať rady orgánov pre ochranu osobných údajov, pokiaľ ide o spracovanie údajov o ľudských zdrojoch v súvislosti s pracovným pomerom, alebo sa k tomu dobrovoľne zaviazala. Fyzické osoby môžu vymáhať rozhodcovské rozhodnutia na súdoch USA podľa federálneho zákona o rozhodcovskom konaní, čím sa zabezpečuje právny prostriedok nápravy v prípade, že spoločnosť rozhodcovské rozhodnutie nevykoná.
- (59) Po siedme ak organizácia neplní svoj záväzok dodržiavať zásady a zverejnené podmienky ochrany súkromia, môžu byť k dispozícii ďalšie prostriedky súdnej nápravy podľa práva jednotlivých štátov USA, ktoré ustanovuje právne prostriedky nápravy podľa práva občianskoprávných deliktov a v prípadoch podvodného nepravdivého vyhlásenia, nekalých a klamlivých činov alebo postupov alebo porušenia zmluvy.
- (60) Okrem toho, ak orgán pre ochranu osobných údajov po prijatí sťažnosti dotknutej osoby z EÚ usúdi, že pri prenose osobných údajov tejto osoby organizácii v USA bolo porušené právo EÚ v oblasti ochrany osobných údajov, vrátane prípadu, keď vývozca údajov z EÚ má dôvod domnievať sa, že organizácia nedodržiava zásady, môže uplatniť svoje právomoci aj voči vývozci údajov a podľa potreby pozastaviť prenos údajov.
- (61) Vzhľadom na informácie v tomto oddiele sa Komisia domnieva, že zásady vydané Ministerstvom obchodu USA ako také zabezpečujú úroveň ochrany osobných údajov, ktorá je v podstate rovnocenná ochrane zaručenej hlavnými základnými zásadami stanovenými v smernici 95/46/ES.
- (62) Účinné uplatňovanie zásad je navyše zaručené povinnosťami týkajúcimi sa transparentnosti a tým, že štít na ochranu osobných údajov spravuje a jeho dodržiavanie kontroluje ministerstvo obchodu.
- (63) Komisia sa navyše domnieva, že mechanizmy dohľadu, nápravy a presadzovania, ktoré poskytuje štít na ochranu osobných údajov, ako celok umožňujú v praxi odhaľovať a trestať porušenia zásad organizáciami zapojenými do štítu na ochranu osobných údajov a poskytujú právne prostriedky nápravy, prostredníctvom ktorých môže dotknutá osoba získať prístup k osobným údajom, ktoré sa jej týkajú, a domôcť sa opravy alebo vymazania týchto údajov.

⁽⁵³⁾ Na počte rozhodcov vo výbore sa musia dohodnúť účastníci.

⁽⁵⁴⁾ Výbor však môže konštatovať, že za okolností konkrétného rozhodcovského konania by úhrada viedla k neopodstatneným alebo neprimeraným nákladom.

⁽⁵⁵⁾ Fyzické osoby si nesmú v rozhodcovskom konaní nárokovat náhradu škody, využitie rozhodcovského konania však neznamená stratu možnosti nárokovat si náhradu škody na bežných súdoch v USA.

3. PRÍSTUP K OSOBNÝM ÚDAJOM PRENÁŠANÝM V RÁMCI ŠTÍTU NA OCHRANU OSOBNÝCH ÚDAJOV MEDZI EÚ A USA ORGÁNMI VEREJNEJ MOCI USA A ICH POUŽÍVANIE

- (64) Ako vyplýva z odd. I ods. 5 prílohy II, dodržiavanie zásad ochrany súkromia je obmedzené na rozsah potrebný na splnenie požiadaviek národnej bezpečnosti, verejného záujmu alebo presadzovania práva.
- (65) Komisia posúdila obmedzenia a záruky, ktoré sú k dispozícii v rámci práva USA v súvislosti s prístupom k osobným údajom prenášaným v rámci štítu na ochranu osobných údajov medzi EÚ a USA orgánmi verejnej moci USA na účely národnej bezpečnosti, presadzovania práva a iné účely verejného záujmu a s ich používaním. Vláda USA navyše prostredníctvom svojho Úradu riaditeľa národnej spravodajskej služby (Office of the Director of National Intelligence – ODNI) ⁽⁵⁶⁾ poskytla Komisii podrobné vyhlásenia a záväzky, ktoré sú uvedené v prílohe VI k tomuto rozhodnutiu. Listom podpísaným ministrom zahraničných vecí a priloženým ako príloha III k tomuto rozhodnutiu sa vláda USA takisto zaviazala vytvoriť nový mechanizmus dohľadu nad zásahmi na účely národnej bezpečnosti, a to funkciu ombudsmana pre štít na ochranu osobných údajov, ktorý je nezávislý od spravodajských služieb (Intelligence Community). A napokon, vo vyhlásení Ministerstva spravodlivosti USA uvedeného v prílohe VII k tomuto rozhodnutiu sa opisujú obmedzenia a záruky vzťahujúce sa na prístup k údajom a ich používanie orgánmi verejnej moci na účely presadzovania práva a iné účely verejného záujmu. V záujme zvýšenia transparentnosti a ako výraz právnej povahy týchto záväzkov sa všetky uvedené dokumenty priložené k tomuto rozhodnutiu uverejnia vo Federálnom registri USA.
- (66) Zistenia Komisie týkajúce sa obmedzení prístupu k osobným údajom prenášaným z Európskej únie do USA orgánmi verejnej moci USA a ich používania a existencie účinnej právnej ochrany sú podrobnejšie opísané ďalej.

3.1. Prístup a použitie zo strany orgánov verejnej moci USA na účely národnej bezpečnosti

- (67) Z analýzy Komisie vyplýva, že právne predpisy USA obsahujú niekoľko obmedzení prístupu k osobným údajom prenášaným v rámci štítu na ochranu osobných údajov medzi EÚ a USA na účely národnej bezpečnosti a ich používania, ako aj mechanizmy dohľadu a nápravné mechanizmy, ktoré poskytujú dostatočné záruky, že tieto údaje budú účinne chránené proti nezákonným zásahom a riziku zneužitia ⁽⁵⁷⁾. Od roku 2013, keď Komisia vydala svoje dve oznámenia (pozri odôvodnenie 7), bol tento právny rámec podstatne posilnený, ako je opísané ďalej.

3.1.1. Obmedzenia

- (68) Podľa ústavy USA patrí zabezpečenie národnej bezpečnosti do právomoci prezidenta ako vrchného veliteľa, najvyššieho predstaviteľa výkonnej moci, a, pokiaľ ide o zahraničné spravodajstvo, ako osoby, ktorá vykonáva zahraničnú politiku USA ⁽⁵⁸⁾. Hoci Kongres má právomoc ukladať obmedzenia a robí to v rôznych ohľadoch, prezident môže v rámci týchto hraníc usmerňovať činnosť spravodajských služieb USA, a to najmä prostredníctvom vykonávacích nariadení alebo prezidentských smerníc. To, samozrejme, platí aj v tých oblastiach, kde neexistujú žiadne usmernenia Kongresu. V súčasnosti sú dva ústredné právne nástroje v tomto ohľade vykonávacie nariadenie č. 12333 ⁽⁵⁹⁾ a prezidentská politická smernica 28.

⁽⁵⁶⁾ Riaditeľ národnej spravodajskej služby (Director of National Intelligence – DNI) je vedúcim orgánom spravodajských služieb a pôsobí ako hlavný poradca prezidenta a Rady pre národnú bezpečnosť. Pozri zákon o reforme spravodajskej služby a predchádzaní terorizmu z roku 2004, vyd. L. 108 – 458 zo 17. decembra 2004. Úrad ODNI okrem iného stanovuje požiadavky na zadávanie úloh, zber, analýzu, tvorbu a šírenie národných spravodajských informácií spravodajskými službami a tieto procesy riadi a usmerňuje, a to vrátane vypracúvania usmernení o tom, ako sa získava prístup k informáciám alebo spravodajským údajom a ako sa používajú a vymieňajú. Pozri oddiel 1 ods. 3 písm. a) a b) vykonávacieho nariadenia č. 12333.

⁽⁵⁷⁾ Pozri vec Schrems, bod 91.

⁽⁵⁸⁾ Ústava USA, článok II. Pozri aj úvod prezidentskej politickej smernice 28.

⁽⁵⁹⁾ Vykonávacie nariadenie č. 12333: Spravodajská činnosť USA, Federálny register zv. 40, č. 235 (8. decembra 1981). Vo verejne prístupnom rozsahu vykonávacieho nariadenia sa vymedzujú ciele, pokyny, povinnosti a úlohy v spravodajstve USA (vrátane úloh jednotlivých zložiek spravodajských služieb) a stanovujú sa v ňom všeobecné parametre vykonávania spravodajskej činnosti (najmä potreba stanoviť osobitné procesné pravidlá). Podľa odd. 3.2 vykonávacieho nariadenia č. 12333 prezident za podpory Rady pre národnú bezpečnosť a riaditeľa pre národné spravodajstvo (Director of National Intelligence – DNI) vydáva také vhodné smernice, postupy a usmernenia, ktoré sú potrebné na vykonanie nariadenia.

- (69) V prezidentskej politickej smernici 28 vydanéj 17. januára 2014 sa ukladá niekoľko obmedzení operácií „signálového spravodajstva“⁽⁶⁰⁾. Táto prezidentská smernica je právne záväzná pre spravodajské orgány USA⁽⁶¹⁾ a zostane účinná aj po zmene vlády v USA⁽⁶²⁾. Prezidentská politická smernica 28 má osobitný význam pre osoby, ktoré nie sú občanmi ani rezidentmi USA, vrátane dotknutých osôb z EÚ. Okrem iného sa v nej stanovuje, že:
- a) získavanie signálového spravodajstva musí byť založené na zákone alebo prezidentskom povolení a musí sa vykonávať v súlade s ústavou USA (najmä so štvrtým dodatkom) a právom USA;
 - b) so všetkými osobami sa musí zaobchádzať s dôstojnosťou a rešpektom bez ohľadu na ich štátnu príslušnosť alebo bydlisko;
 - c) všetky osoby majú pri narábaní s ich osobnými informáciami oprávnené záujmy týkajúce sa ochrany súkromia;
 - d) pri plánovaní činností USA v oblasti signálového spravodajstva sa musí brať ohľad na súkromie a občianske slobody;
 - e) činnosti USA v oblasti signálového spravodajstva musia preto zahŕňať primerané záruky v súvislosti s osobnými informáciami všetkých fyzických osôb bez ohľadu na ich štátnu príslušnosť alebo bydlisko.
- (70) V prezidentskej politickej smernici 28 sa stanovuje, že signálové spravodajstvo možno získavať výlučne vtedy, keď existuje účel súvisiaci so zahraničným spravodajstvom alebo kontrašpionážou týkajúci sa podpory národných a rezortných misií, a nie na žiadne iné účely (napr. na získanie konkurenčnej výhody pre spoločnosti z USA). V tejto súvislosti ODNI vysvetľuje, že zložky spravodajských služieb „by mali vyžadovať, aby všade tam, kde je to možné, bol zber zameraný na konkrétne ciele alebo témy zahraničného spravodajstva pomocou diskriminantov (napr. konkrétne komunikačné prostriedky, výberové pojmy a identifikátory)“.⁽⁶³⁾ Vyhláseniami sa navyše poskytuje uistenie, že rozhodnutia o získavaní spravodajstva nie sú ponechané na uváženie jednotlivých spravodajských dôstojníkov, ale sú predmetom podmienok a postupov, ktoré jednotlivé zložky (agentúry) spravodajských služieb USA musia zaviesť s cieľom vykonať prezidentskú politickú smernicu 28⁽⁶⁴⁾. Preto hľadanie a stanovenie vhodných selektorov prebieha v celkovom „rámci priorit národného spravodajstva“ (National Intelligence Priorities Framework – NIPF), ktorý zabezpečuje, že priority spravodajstva stanovujú vysokopostavení politici a že sa pravidelne prehodnocujú, aby vždy reagovali na aktuálne národné bezpečnostné hrozby a zohľadňovali možné riziká vrátane rizík pre súkromie⁽⁶⁵⁾. Na základe toho pracovníci agentúry skúmajú a identifikujú konkrétne výberové pojmy, pomocou ktorých by sa malo získavať zahraničné spravodajstvo zamerané na priority⁽⁶⁶⁾. Výberové pojmy, alebo „selektory“, sa musia pravidelne prehodnocovať s cieľom stanoviť, či naďalej poskytujú cenné spravodajské informácie v súlade s prioritami⁽⁶⁷⁾.
-
- ⁽⁶⁰⁾ Podľa vykonávacieho nariadenia č. 12333 je riaditeľ Národnej bezpečnostnej agentúry (National Security Agency – NSA) funkčným riaditeľom pre signálové spravodajstvo a spravuje jednotnú organizáciu pre činnosti signálového spravodajstva.
- ⁽⁶¹⁾ Vymedzenie pojmu „spravodajské služby“ je uvedené v odd. 3 ods. 5 písm. h) vykonávacieho nariadenia č. 12333 a poznámke pod čiarou č. 1 prezidentskej politickej smernice 28.
- ⁽⁶²⁾ Pozri oznámenie Úradu právneho poradcu ministerstva spravodlivosti prezidentovi Clintonovi, 29. januára 2000. Podľa tohto právneho názoru majú prezidentské smernice „rovnaký hmotný právny účinok ako vykonávacie nariadenie“.
- ⁽⁶³⁾ Vyhlásenia ODNI (príloha VI), s. 3.
- ⁽⁶⁴⁾ Pozri odd. 4 písm. b) a c) prezidentskej politickej smernice 28. Podľa verejných informácií sa pri preskúmaní v roku 2015 potvrdilo šesť existujúcich účelov. Pozri ODNI, Signals Intelligence Reform (Reforma signálového spravodajstva), výročná správa z roku 2016.
- ⁽⁶⁵⁾ Vyhlásenia ODNI (príloha VI), s. 6 (s odkazom na smernicu o spravodajských službách 204). Pozri aj odd. 3 prezidentskej politickej smernice 28.
- ⁽⁶⁶⁾ Vyhlásenia ODNI (príloha VI), s. 6. Pozri napríklad Úrad NSA pre ochranu občianskych slobôd a súkromia (NSA Civil Liberties and Privacy Office – NSA CLPO), Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 (Ochrana občianskych slobôd a súkromia pre ciele činnosti SIGINT podľa vykonávacieho nariadenia č. 12333), 7. októbra 2014. Pozri aj správu o stave ODNI z roku 2014. V prípade žiadostí o prístup podľa odd. 702 zákona FISA sa otázky riadia postupmi minimalizácie schválenými súdom pre sledovanie v rámci zahraničného spravodajstva (Foreign Intelligence Surveillance Court – FISC). Pozri NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 (Vykonávanie oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva zo strany NSA), 16.4.2014.
- ⁽⁶⁷⁾ Pozri Signals Intelligence Reform (Reforma signálového spravodajstva), výročná správa z roku 2015. Pozri aj vyhlásenia ODNI (príloha VI), s. 6, 8 – 9, 11.

- (71) Okrem toho sa v požiadavkách stanovených v prezidentskej politickej smernici 28 uviedlo, že získavanie spravodajských informácií musí byť vždy ⁽⁶⁸⁾ „v čo najväčšej uskutočniteľnej miere prispôbené“ a že spravodajské služby majú uprednostniť dostupnosť iných informácií a primerané a uskutočniteľné alternatívy ⁽⁶⁹⁾, zohľadniť všeobecné pravidlo uprednostnenia cieľného zberu pred hromadným zberom. Podľa uistenia, ktoré poskytol ODNI sa nimi predovšetkým zaisťuje, že hromadný zber nebude ani „hromadný“ a „nerozlišujúci“ a že výnimky nebudú viesť k tomu, že pravidlo už nebude účinné ⁽⁷⁰⁾.
- (72) Hoci sa v prezidentskej politickej smernici 28 sa vysvetľuje, že zložky spravodajských služieb musia niekedy za určitých okolností získavať hromadné signálové spravodajstvo, napríklad s cieľom identifikovať a posudzovať nové alebo vznikajúce hrozby, nariaďuje týmto zložkám uprednostniť alternatívy, ktoré by umožnili vykonávanie cieľného signálového spravodajstva ⁽⁷¹⁾. Z toho vyplýva, že k hromadnému zberu dôjde len v prípade, ak cieľný zber pomocou diskriminantov – t. j. identifikátorov súvisiacich s osobitným cieľom (napríklad e-mailová adresa alebo telefónne číslo cieľa) – nie je „v dôsledku technických alebo prevádzkových faktorov“ ⁽⁷²⁾ možné. Platí to pre spôsob, akým sa signálové spravodajstvo získava, ako aj pre to, čo sa vlastne získava ⁽⁷²⁾.
- (73) Podľa vyhlásení ODNI aj v prípade, že spravodajské služby nemôžu použiť osobitné identifikátory na cieľný zber, budú sa usilovať o „čo najväčšie“ zúženie zberu. Aby to zaistili, „používajú filtre a iné technické nástroje s cieľom zamerať zber na tie zariadenia, ktoré pravdepodobne obsahujú komunikáciu s hodnotou pre zahraničné spravodajstvo“ (a tak budú reagovať na požiadavky, ktoré vyjadrili politickí činitelia USA podľa procesu opísaného v odôvodnení 70). V dôsledku toho bude hromadný zber zacielený aspoň dvoma spôsobmi: Po prvé vždy bude súvisieť s osobitnými cieľmi v oblasti zahraničného spravodajstva (napríklad získať signálové spravodajstvo o činnostiach teroristickej skupiny pôsobiacej v konkrétnom regióne) a bude zameraný na komunikáciu, ktorá zahŕňa takúto spojitosť. Podľa uistenia zo strany ODNI sa to zohľadňuje v skutočnosti, že „činnosti signálového spravodajstva USA sa dotýkajú len nepatrnej časti komunikácie prechádzajúcej internetom“ ⁽⁷³⁾ Po druhé z vyhlásení ODNI vyplýva, že filtre a iné použité technické nástroje budú určené na „čo najpresnejšie“ zameranie zberu s cieľom zaistiť, aby sa minimalizoval objem „nesúvisiacich informácií“.
- (74) A napokon, aj keď USA usúdia, že je potrebné získavať hromadné informácie prostredníctvom signálového spravodajstva za podmienok stanovených v odôvodneniach 70 – 73, prezidentská politická smernica 28 obmedzuje použitie takých informácií na konkrétny zoznam šiestich účelov v oblasti národnej bezpečnosti s ohľadom na ochranu súkromia a občianskych slobôd všetkých osôb bez ohľadu na ich štátnu príslušnosť alebo bydlisko ⁽⁷⁴⁾. Tieto prípustné účely zahŕňajú opatrenia na odhaľovanie hrozieb vyplývajúcich zo špionáže,

⁽⁶⁸⁾ Pozri vyhlásenia ODNI (príloha VI), s. 3.

⁽⁶⁹⁾ Takisto treba poznamenať, že podľa oddielu 2. ods. 4 vykonávacieho nariadenia č. 12333 zložky spravodajských služieb „použijú najmenej obťažujúce techniky zberu uskutočniteľné v USA“. Pokiaľ ide o obmedzenia týkajúce sa nahradenia hromadného zberu v plnej miere cieľnými zbermi, pozri výsledky posúdenia Národnej výskumnej rady, ktoré nahlásila Agentúra Európskej únie pre základné práva: Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU (Dohľad spravodajských služieb: základné práva, záruky a opravné prostriedky v EÚ) (2015), s. 18.

⁽⁷⁰⁾ Vyhlásenia ODNI (príloha VI), s. 4.

⁽⁷¹⁾ Pozri aj odd. 5 písm. d) prezidentskej politickej smernice 28, v ktorom sa riaditeľovi národnej spravodajskej služby nariaďuje, aby v koordinácii s riaditeľmi príslušných zložiek spravodajských služieb a Úradom pre politiku v oblasti vedy a techniky predkladal prezidentovi „správu o posúdení uskutočniteľnosti vytvorenia softvéru, ktorý by umožnil spravodajským službám ľahšie vykonávať cieľné získavanie informácií namiesto hromadného zberu“. Podľa verejných informácií výsledkom tejto správy bolo, že „neexistuje žiadna softvérová alternatíva, ktorá by zabezpečila úplnú náhradu hromadného zberu pri odhaľovaní niektorých hrozieb pre národnú bezpečnosť“. Pozri Signals Intelligence Reform (Reforma signálového spravodajstva), výročná správa z roku 2015.

⁽⁷²⁾ Pozri poznámku pod čiarou č. 68.

⁽⁷³⁾ Vyhlásenia ODNI (príloha VI). Týmto sa konkrétne rieši obava, ktorú vyjadrili vnútroštátne orgány pre ochranu údajov vo svojom stanovisku k návrhu rozhodnutia o primeranosti. Pozri stanovisko 01/2016 pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 k návrhu rozhodnutia o primeranosti štítu na ochranu osobných údajov medzi EÚ a USA (prijaté 13. apríla 2016), s. 38, bod 47.

⁽⁷⁴⁾ Pozri odd. 2 prezidentskej politickej smernice 28.

terorizmu, zbraní hromadného ničenia, hrozieb pre kybernetickú bezpečnosť, hrozieb pre ozbrojené sily alebo vojenský personál, ako aj nadnárodných hrozieb trestnej činnosti súvisiacich s ostatnými piatimi účelmi a boj proti týmto hrozbám, a budú sa prehodnocovať najmenej raz ročne. Podľa vyhlásení vlády USA posilnili zložky spravodajských služieb svoje analytické postupy a normy týkajúce sa vyhľadávania v nevyhodnotených informáciách získaných prostredníctvom signálového spravodajstva, aby tak dosiahli súlad s týmito požiadavkami; používaním cieľového vyhľadávania „sa zabezpečuje, aby sa analytikom dostali na preskúmanie iba tie položky, ktoré sa považujú za potenciálne hodnotné zo spravodajského hľadiska“ ⁽⁷⁵⁾.

- (75) Tieto obmedzenia sa týkajú predovšetkým osobných údajov prenášaných v rámci štítu na ochranu osobných údajov medzi EÚ a USA, a to najmä v prípade, že by k zhromažďovaniu osobných údajov došlo mimo USA, a to aj v priebehu ich prenosu cez transatlantické káble z Únie do USA. Ako potvrdili orgány USA vo vyhláseniach ODNI, na toto zhromažďovanie sa uplatňujú obmedzenia a záruky uvedené v týchto vyhláseniach – vrátane tých, ktoré sú stanovené v prezidentskej politickej smernici 28 ⁽⁷⁶⁾.
- (76) Hoci tieto zásady nie sú formulované v týchto právnych pojmoch, zachytávajú podstatu zásad nevyhnutnosti a proporcionality. Jednoznačnou prioritou je cieľový zber, zatiaľ čo hromadný zber je obmedzený na (mimoriadne) situácie, keď cieľový zber nie je možný z technických alebo prevádzkových dôvodov. Aj keď hromadnému zberu sa nedá vyhnúť, ďalšie „použitie“ týchto údajov prostredníctvom prístupu je prísne obmedzené na špecifické, legitímne účely národnej bezpečnosti ⁽⁷⁷⁾.
- (77) Tieto požiadavky vydané vo forme smernice prezidenta ako najvyššieho predstaviteľa výkonnej moci sú záväzné pre všetky spravodajské služby a ďalej sa uplatňujú prostredníctvom pravidiel a postupov agentúr, ktorými sa transponujú všeobecné zásady do konkrétnych pokynov na každodenné operácie. Navyše, hoci samotný Kongres nie je viazaný prezidentskou politickou smernicou 28, takisto podnikol kroky na zabezpečenie toho, aby získavanie osobných údajov a prístup k nim boli v USA skôr cieľové ako vykonávané „na všeobecnom základe“.
- (78) Z dostupných informácií vrátane vyhlásení získaných od vlády USA vyplýva, že hneď ako boli údaje prenesené organizáciám nachádzajúcim sa v USA, poskytnú osvedčenie v rámci štítu na ochranu osobných údajov medzi EÚ a USA, spravodajské agentúry USA môžu získavať osobné údaje len vtedy ⁽⁷⁸⁾, keď je ich žiadosť v súlade so zákonom o sledovaní v rámci zahraničného spravodajstva (Foreign Intelligence Surveillance Act – FISA) alebo keď ju podá Federálny úrad pre vyšetrovanie (FBI) na základe takzvaného listu národnej bezpečnosti (National Security Letter – NSL) ⁽⁷⁹⁾. Podľa zákona FISA existuje niekoľko právnych základov, ktoré možno použiť na zber (a následné spracovanie) osobných údajov dotknutých osôb z EÚ prenášaných v rámci štítu na ochranu osobných

⁽⁷⁵⁾ Vyhlásenia ODNI (príloha VI), s. 4. Pozri aj smernicu o spravodajských službách 203.

⁽⁷⁶⁾ Vyhlásenia ODNI (príloha VI), s. 2. Podobne sa uplatňujú aj obmedzenia stanovené vo vykonávacom nariadení č. 12333 (napr. nutnosť, aby sa získavané informácie vzťahovali na spravodajské priority stanovené prezidentom).

⁽⁷⁷⁾ Pozri vec Schrems, bod 93.

⁽⁷⁸⁾ Zber údajov zo strany FBI môže byť navyše založený aj na povoleniach na presadzovanie práva (pozri oddiel 3.2 tohto rozhodnutia).

⁽⁷⁹⁾ Ďalšie vysvetlenia použitia NSL sú uvedené vo vyhláseniach ODNI (príloha VI), s. 13 – 14 s č. 38. Ako sa tam uvádza, FBI môže využiť NSL iba na vyžiadanie neobsahových informácií súvisiacich s povoleným vyšetrovaním týkajúcim sa národnej bezpečnosti, ktorého účelom je ochrana pred medzinárodným terorizmom alebo tajnými spravodajskými činnosťami. Pokiaľ ide o prenosy údajov v rámci štítu na ochranu osobných údajov medzi EÚ a USA, najdôležitejším zákonným povolením je zrejme zákon o ochrane súkromia v rámci elektronickej komunikácie (18 U.S.C. § 2709), v ktorom sa vyžaduje, aby sa v každej žiadosti o informácie o účastníkovi alebo o záznamy z transakcie použil „pojem, ktorý konkrétne označuje osobu, subjekt, telefónne číslo alebo účet“.

údajov medzi EÚ a USA. Okrem oddielu 104 zákona FISA ⁽⁸⁰⁾ týkajúceho sa tradičného individualizovaného elektronického sledovania a oddielu 402 zákona FISA ⁽⁸¹⁾ o inštalácii záznamníkov zdrojov a cieľov elektronickej komunikácie sú dvoma ústrednými nástrojmi oddiel 501 zákona FISA [predtým oddiel 215 vlasteneckého zákona USA (PATRIOT ACT)] a oddiel 702 zákona FISA ⁽⁸²⁾.

- (79) V tomto ohľade sa zákonom USA o slobode (Freedom Act), ktorý bol prijatý 2. júna 2015, zakazuje hromadný zber záznamov na základe oddielu 402 zákona FISA (povolenie pre záznamníky zdrojov a cieľov elektronickej komunikácie) a oddielu 501 zákona FISA (predtým: oddiel 215 vlasteneckého zákona USA) ⁽⁸³⁾, ako aj prostredníctvom využitia NSL, a namiesto toho vyžaduje použitie špecifických „výberových podmienok“ ⁽⁸⁴⁾.
- (80) Hoci zákon FISA obsahuje ďalšie zákonné povolenia na vykonávanie národných spravodajských činností vrátane signálového spravodajstva, z posúdenia Komisie vyplýva, že pokiaľ ide o osobné údaje prenášané v rámci štítu na ochranu osobných údajov medzi EÚ a USA, týmito povoleniami sa rovnako obmedzuje zásah orgánov verejnej moci na cieľný zber a prístup.
- (81) Jednoznačné to je v prípade tradičného individualizovaného elektronického sledovania podľa oddielu 104 zákona FISA ⁽⁸⁵⁾. Pokiaľ ide o oddiel 702 zákona FISA, ktorý poskytuje základ pre dva dôležité spravodajské programy realizované spravodajskými agentúrami USA (PRISM, UPSTREAM), vyhľadávanie sa vykonáva cieľovým spôsobom pomocou individuálnych selektorov, ktoré identifikujú špecifické komunikačné prostriedky, napríklad cieľovú e-mailovú adresu alebo telefónne číslo, ale nie kľúčové slová či dokonca mená cieľových osôb ⁽⁸⁶⁾. Ako

⁽⁸⁰⁾ 50 U.S.C. § 1804. Hoci sa v tomto zákonom povolení vyžaduje „vyhlásenie o skutočnostiach a okolnostiach, ktorými žiadateľ odôvodní svoje presvedčenie, že a) cieľom elektronického sledovania je cudzia mocnosť alebo agent cudzej mocnosti“, títo agenti môžu zahŕňať osoby, ktoré nie sú občanmi ani rezidentmi USA a zapájajú sa do medzinárodného terorizmu alebo medzinárodného šírenia zbraní hromadného ničenia (vrátane prípravných krokov) (50 U.S.C. § 1801 písm. b) bod 1). Odkaz na osobné údaje prenášané v rámci štítu na ochranu osobných údajov medzi EÚ a USA je však stále len teoretický, lebo vyhlásenie o skutočnostiach musí takisto odôvodniť presvedčenie, že „každý priestor alebo miesto, ktorého elektronické sledovanie bolo nariadené, používa alebo práve bude používať cudzia mocnosť alebo agent cudzej mocnosti“. V každom prípade použitie tohto povolenia si vyžaduje podanie žiadosti na súd FISC, ktorý okrem iného posúdi, či je na základe predložených skutočností pravdepodobné, že to tak naozaj je.

⁽⁸¹⁾ 50 U.S.C. § 1842 s § 1841 ods. 2 a odd. 3127 hlavy 18. Povolenie sa netýka obsahu komunikácie, ale skôr sa zameriava na informácie o zákazníkovi alebo účastníkovi využívajúcom určitú službu (ako je meno, adresa, číslo účastníka, dĺžka/druh získanej služby, zdroj/mechanizmus platby). Vyžaduje si podanie návrhu na vydanie príkazu súdu FISC (alebo magistrátneho sudcu USA) a použitie konkrétneho výberového pojmu v zmysle § 1841 ods. 4, teda pojmu, ktorý konkrétne identifikuje osobu, účet atď. a používa sa na čo najväčšie prakticky možné obmedzenie rozsahu vyhľadávaných informácií.

⁽⁸²⁾ Kým odd. 501 zákona FISA (predtým odd. 215 vlasteneckého zákona USA) oprávňuje FBI požiadať o súdny príkaz zameraný na získavanie „hmotných vecí“ (najmä telefonických metaúdajov, ale aj obchodných záznamov) na účely zahraničného spravodajstva, odd. 702 zákona FISA umožňuje zložkám spravodajských služieb USA obchádzať o prístup k informáciám vrátane obsahu internetovej komunikácie pochádzajúcej z USA, ale so zacielením na niektoré osoby, ktoré nie sú občanmi ani rezidentmi USA a nachádzajú sa mimo územia USA.

⁽⁸³⁾ Na základe tohto ustanovenia môže FBI požiadať o „hmotné veci“ (napríklad záznamy, publikácie, dokumenty) na základe preukázania súdu FISC, že existujú opodstatnené dôvody domnievať sa, že tieto veci sú relevantné pre konkrétne vyšetrovanie FBI. FBI musí pri vykonávaní vyhľadávania použiť výberové pojmy schválené súdom FISC, v prípade ktorých existuje „opodstatnené, pomenovateľné podozrenie“, že sú spojené s jednou alebo viacerými cudzími mocnosťami alebo ich agentmi zapojenými do medzinárodného terorizmu alebo činností smerujúcich k jeho príprave. Pozri PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 59; NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation (Správa o transparentnosti: zapracovanie pravidiel týkajúcich sa obchodných záznamov podľa zákona USA o slobode do zákona FISA), 15. januára 2016, s. 4 – 6.

⁽⁸⁴⁾ Vyhlásenia ODNI (príloha VI), s. 13 (č. 38).

⁽⁸⁵⁾ Pozri poznámku pod čiarou č. 81.

⁽⁸⁶⁾ PCLOB, Sec. 702 Report (Správa podľa odd. 702), s. 32 – 33 s ďalšími odkazmi. NSA musí podľa svojho úradu na ochranu súkromia overiť, či existuje spojitost medzi cieľom a selektorom, zdokumentovať zahraničné spravodajské informácie, ktoré chce získať, tieto informácie musia skontrolovať a schváliť dvaja vysokopostavení analytici NSA a celý proces bude sledovať ODNI a ministerstvo spravodlivosti na účely následného preskúmania dodržiavania zásad. Pozri NSA CLPO, NSA's Implementation of Foreign Intelligence surveillance Act Section 702 (Vykonávanie oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva zo strany NSA), 16. apríla 2014.

poznačená Rada pre dohľad nad ochranou súkromia a občianskych slobôd (Privacy and Civil Liberties Oversight Board – PCLOB), sledovanie podľa oddielu 702 sa teda „týka výlučne zacielenia na konkrétne osoby (ktoré nie sú občanmi USA), ktoré boli individualizovane určené“⁽⁸⁷⁾. Vzhľadom na doložku o „ukončení platnosti“ sa oddiel 702 zákona FISA bude musieť preskúmať v roku 2017, keď bude Komisia musieť prehodnotiť záruky, ktoré majú k dispozícii dotknuté osoby z EÚ.

- (82) Vláda USA navyše vo svojich vyhláseniach výslovne uistila Európsku komisiu, že spravodajské služby USA „nevykonávajú nerozlišujúce sledovanie nikoho vrátane bežných európskych občanov“⁽⁸⁸⁾. Pokiaľ ide o osobné údaje zhromaždené v rámci USA, toto vyhlásenie podporujú empirické dôkazy, ktoré preukazujú, že *žiadosti o prístup* prostredníctvom NSL a podľa zákona FISA sa jednotlivci aj spoločne týkajú iba pomerne malého počtu cieľov v porovnaní s celkovým tokom údajov na internete⁽⁸⁹⁾.
- (83) Pokiaľ ide o *prístup k zhromaždeným údajom a zabezpečenie údajov*, v prezidentskej politickej smernici 28 sa vyžaduje, aby bol prístup „obmedzený na oprávnený personál, ktorý musí poznať informácie, aby mohol plniť svoje poslanie“, a že osobné informácie „sa spracúvajú a uchovávajú za podmienok, ktoré poskytujú dostatočnú ochranu a bránia prístupu neoprávnených osôb v súlade s príslušnými zárukami na ochranu citlivých informácií“. Spravodajský personál dostáva primeranú a dostatočnú odbornú prípravu o zásadách uvedených v prezidentskej politickej smernici 28⁽⁹⁰⁾.
- (84) A napokon, pokiaľ ide o *uchovávanie* a ďalšie šírenie osobných údajov dotknutých osôb v EÚ zhromaždených spravodajskými orgánmi USA, v prezidentskej politickej smernici 28 sa uvádza, že so všetkými osobami (vrátane osôb, ktoré nie sú občanmi ani rezidentmi USA) sa musí zaobchádzať s úctou a rešpektom, že všetky osoby majú oprávnené záujmy týkajúce sa ochrany súkromia pri nakladaní s ich osobnými údajmi, a že zložky spravodajských služieb preto musia zaviesť pravidlá, ktoré poskytujú dostatočné záruky v súvislosti s týmito údajmi, ktoré sú „primerane navrhnuté tak, aby sa minimalizovalo ich šírenie a uchovávanie“⁽⁹¹⁾.

⁽⁸⁷⁾ PCLOB, Sec. 702 Report (Správa podľa odd. 702), s. 111. Pozri aj vyhlásenia ODNI (príloha VI), s. 9 [„zber informácií podľa oddielu 702 zákona (FISA) nie je „hromadný a nerozlišujúci“, ale je úzko zameraný na zber zahraničných spravodajských informácií o individuálne určených legitímnych cieľoch“] a s. 13, č. 36 (s odkazom na stanovisko FISC z roku 2014); NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 (Vykonávanie oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva zo strany NSA), 16. apríla 2014. Dokonca aj v prípade programu UPSTREAM môže NSA požiadať len o zachytávanie elektronickej komunikácie smerujúcej k určeným selektorom, od nich a o nich.

⁽⁸⁸⁾ Vyhlásenia ODNI (príloha VI), s. 18. Pozri aj s. 6, podľa ktorej príslušné postupy „preukazujú jasné odhodlanie predchádzať svojvoľnému a nerozlišujúcemu zberu informácií prostredníctvom signálového spravodajstva a dodržiavať – od najvyšších úrovní našej vlády – zásadu primeranosti“.

⁽⁸⁹⁾ Pozri Statistical Transparency Report Regarding Use of National Security Authorities (Štatistická správa na účely zabezpečenia transparentnosti týkajúca sa využívania národných bezpečnostných orgánov), 22. apríla 2015. Pre celkový tok údajov na internete pozri napríklad Agentúra pre základné práva, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (Sledovanie spravodajskými službami: záruky základných práv a opravné prostriedky v EÚ) (2015), s. 15 – 16. Čo sa týka programu UPSTREAM, podľa odtajneného stanoviska súdu FISC z roku 2011 viac než 90 % elektronických komunikácií získaných podľa odd. 702 zákona FISA pochádzalo z programu PRISM a menej než 10 % z programu UPSTREAM. Pozri FISC, Memorandum Opinion (stanovisko), 2011 WL 10945618 (FISA Ct., 3. októbra 2011), č. 21 (dostupné na: <http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>).

⁽⁹⁰⁾ Pozri odd. 4 písm. a) bod ii) prezidentskej politickej smernice 28. Pozri aj ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (Správa o stave týkajúca sa vývoja a vykonávania postupov podľa prezidentskej politickej smernice 28), júl 2014, s. 5, podľa ktorej „by podmienky zložiek spravodajských služieb mali posilniť súčasné analytické postupy a normy, pomocou ktorých sa analytici musia snažiť štruktúrovať otázky alebo iné vyhľadávacie pojmy a techniky tak, aby umožnili identifikáciu spravodajských informácií týkajúcich sa legitímnej spravodajskej úlohy alebo úlohy presadzovania práva; zamerať otázky týkajúce sa osôb na kategórie spravodajských informácií, ktoré zodpovedajú spravodajskej požiadavke alebo požiadavke na presadzovanie práva; a minimalizovať skúmanie osobných informácií, ktoré nie sú podstatné z hľadiska spravodajských požiadaviek alebo požiadaviek na presadzovanie práva“. Pozri napr. CIA, Signals Intelligence Activities (Činnosti signálového spravodajstva), s. 5; FBI, prezidentská politická smernica 28 Pravidlá a postupy, s. 3. Podľa správy o pokroku v reforme signálového spravodajstva z roku 2016 zložky spravodajských služieb (vrátane FBI, CIA a NSA) prijali opatrenia na zvýšenie vnímateľnosti svojich zamestnancov k požiadavkám prezidentskej politickej smernice 28 vytvorením nových alebo úpravou existujúcich politík v oblasti odbornej prípravy.

⁽⁹¹⁾ Podľa vyhlásení ODNI sa tieto obmedzenia uplatňujú bez ohľadu na to, či boli informácie zhromaždené hromadne alebo prostredníctvom cieleného zberu, a bez ohľadu na štátnu príslušnosť danej osoby.

- (85) Vláda USA vysvetlila, že táto požiadavka na primeranosť znamená, že zložky spravodajských služieb nebudú musieť prijať „všetky teoreticky možné opatrenia“, ale budú musieť „vyvažovať svoje úsilie na ochranu oprávnených záujmov v oblasti ochrany súkromia a občianskych slobôd s praktickými potrebami činností signálového spravodajstva“⁽⁹²⁾. V tomto ohľade sa s osobami, ktoré nie sú občanmi ani rezidentmi USA, bude zaobchádzať rovnako ako s občanmi alebo rezidentmi USA na základe postupov schválených generálnym prokurátorom⁽⁹³⁾.
- (86) Podľa týchto pravidiel je uchovávanie vo všeobecnosti obmedzené na maximálne päť rokov, pokiaľ neexistuje konkrétne zákonné určenie alebo výslovné určenie riaditeľom národnej spravodajskej služby po dôkladnom vyhodnotení otázok ochrany súkromia – s prihliadnutím k názorom úradníka pre ochranu občianskych slobôd z ODNI a úradníkov danej agentúry pre ochranu súkromia a občianskych slobôd –, z ktorého vyplýva, že ďalšie uchovávanie je v záujme národnej bezpečnosti⁽⁹⁴⁾. Šírenie je obmedzené na prípady, keď sú informácie dôležité pre základný účel zberu údajov, a teda zodpovedajú schválenej požiadavke zahraničného spravodajstva alebo požiadavke na presadzovanie práva⁽⁹⁵⁾.
- (87) Podľa uistení zo strany vlády USA sa osobné údaje nesmú šíriť len preto, lebo daná osoba nie je občanom USA, a „signálové spravodajstvo o bežnej činnosti zahraničnej osoby by sa nemalo považovať za zahraničné spravodajské informácie, ktorá by sa mohli šíriť alebo trvalo uchovávať iba z tohto dôvodu, pokiaľ inak nereagujú na schválenú požiadavku na zahraničné spravodajstvo“⁽⁹⁶⁾.
- (88) Komisia na základe všetkých uvedených skutočností dospela k záveru, že v USA existujú platné pravidlá, ktorých cieľom je obmedziť akékoľvek zásahy do základných práv osôb, ktorých osobné údaje sa prenášajú v rámci štítu na ochranu osobných údajov medzi EÚ a USA, na účely národnej bezpečnosti na to, čo je nevyhnutne potrebné na dosiahnutie príslušného legitímneho cieľa.
- (89) Ako vyplýva z uvedenej analýzy, v práve USA sa zaisťuje, že opatrenia týkajúce sa sledovania sa použijú len na zhromaždenie zahraničných spravodajských informácií – čo je legitímnym politickým cieľom⁽⁹⁷⁾ – a v čo

⁽⁹²⁾ Pozri vyhlásenia ODNI (príloha VI).

⁽⁹³⁾ Pozri odd. 4 písm. a) bod i) prezidentskej politickej smernice 28 s oddielom 2.3 vykonávacieho nariadenia č. 12333.

⁽⁹⁴⁾ Odd. 4 a) ods. i) prezidentskej politickej smernice 28; vyhlásenia ODNI (príloha VI), s. 7. Napríklad v prípade osobných informácií zhromaždených podľa odd. 702 zákona FISA postupy minimalizácie NSA schválené súdom FISC obsahujú pravidlo, že metaúdaje a nevyhodnotený obsah zhromaždené v programe PRISM sa uchovávajú maximálne päť rokov, zatiaľ čo údaje zhromaždené v programe UPSTREAM sa uchovávajú maximálne dva roky. NSA zabezpečuje súlad s týmito obmedzeniami uchovávania prostredníctvom automatického procesu, ktorým sa zhromaždené údaje na konci príslušného obdobia uchovávania vymažú. Pozri NSA, Sec. 702 FISA Minimization Procedures (Postupy minimalizácie podľa odd. 702 zákona FISA), odd. 7 a odd. 6 písm. a) bod 1; NSA CLPO, NSA's Implementation of Foreign Intelligence surveillance Act Section 702 (Vykonávanie oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva zo strany NSA), 16. apríla 2014. Rovnako aj uchovávanie podľa odd. 501 zákona FISA (predtým odd. 215 vlasteneckého zákona USA) je obmedzené na päť rokov, pokiaľ osobné údaje nie sú súčasťou riadne schváleného šírenia zahraničných spravodajských informácií alebo pokiaľ ministerstvo spravodlivosti písomne neoznámí NSA, že na záznamy sa vzťahuje povinnosť uchovania v prebiehajúcom alebo predpokladanom súdnom spore. Pozri NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation (Správa o transparentnosti: zapracovanie pravidiel týkajúcich sa obchodných záznamov podľa zákona USA o slobode do zákona FISA), 15. januára 2016.

⁽⁹⁵⁾ Konkrétne podľa odd. 501 zákona FISA (predtým odd. 215 vlasteneckého zákona USA) sa šírenie osobných informácií môže uskutočňovať len na účely boja proti terorizmu alebo ako dôkaz trestného činu a podľa odd. 702 zákona FISA iba vtedy, keď existuje legitímny účel zahraničného spravodajstva alebo presadzovania práva. Pozri NSA CLPO, NSA's Implementation of Foreign Intelligence surveillance Act Section 702 (Vykonávanie oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva zo strany NSA), 16. apríla 2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation (Správa o transparentnosti: zapracovanie pravidiel týkajúcich sa obchodných záznamov podľa zákona USA o slobode do zákona FISA), 15. januára 2016. Pozri aj NSA, Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 (Ochrana občianskych slobôd a súkromia pre ciele činnosti SIGINT podľa vykonávacieho nariadenia č. 12333), 7. októbra 2014.

⁽⁹⁶⁾ Vyhlásenia ODNI (príloha VI), s. 7 (s odkazom na smernicu o spravodajských službách 203).

⁽⁹⁷⁾ Súdny dvor vysvetlil, že národná bezpečnosť predstavuje legitímny politický cieľ. Pozri vec *Schrems*, bod 88. Pozri aj vec *Digital Rights Ireland a i.*, body 42 – 44 a 51, v ktorej Súdny dvor skonštatoval, že boj proti závažnej trestnej činnosti, predovšetkým organizovanému zločinu a terorizmu, môže vo veľkej miere závisieť od používania moderných vyšetrovacích techník. Okrem toho na rozdiel od vyšetrovaní trestných činov, ktoré sa bežne týkajú spätého určenia zodpovednosti a viny za minulé konanie, sú spravodajské činnosti často zamerané na predchádzanie hrozbám pre národnú bezpečnosť pred vznikom škody. Takéto vyšetrovania preto môže často pokrývať širší rozsah možných aktérov („cieľov“) a väčšiu zemepisnú oblasť. Pozri Európsky súd pre ľudské práva, *Weber and Saravia/Nemecko*, rozhodnutie z 29. júna 2006, číslo žiadosti 54934/00, body 105 – 118 (o tzv. „strategickom monitorovaní“).

najväčšej možnej miere sa prispôbia. Konkrétne hromadný zber sa povolí len vo výnimočných prípadoch, ak nebude realizovateľný cieľový zber, a budú ho sprevádzať dodatočné záruky týkajúce sa minimalizovania objemu zhromaždených údajov a následného prístupu (ktorý bude musieť byť cieľový a povolí sa len na osobitné účely).

- (90) V posúdení Komisie je táto skutočnosť v súlade s normou stanovenou Súdnym dvorom v rozsudku vo veci Schrems, podľa ktorého sa v právnych predpisoch týkajúcich sa zasahovania do základných práv zaručených článkami 7 a 8 charty musia uložiť „minimálne požiadavky“⁽⁹⁸⁾ a „právna úprava, v ktorej sa vo všeobecnosti oprávňuje na uchovávanie všetkých osobných údajov každej osoby, ktorej osobné údaje boli prenesené z Únie do Spojených štátov, nie je obmedzená na úplne nevyhnutné bez toho, aby sa v nej stanovovalo akékoľvek rozlíšenie, obmedzenie alebo výnimka na základe sledovaného cieľa, a“ „bez toho, aby sa stanovovalo objektívne kritérium umožňujúce obmedziť prístup orgánov verejnej moci k údajom a ich neskoršie použitie na účely, ktoré sú konkrétne, prísne obmedzené a schopné odôvodniť zásah, ktorý spôsobuje tak prístup, ako aj používanie týchto údajov“. ⁽⁹⁹⁾ Neuskutoční sa ani neobmedzený zber a uchovávanie údajov všetkých osôb bez akýchkoľvek obmedzení, ani neobmedzený prístup. Okrem toho sa vo vyhláseniach poskytnutých Komisii vrátane uistenia, že činnosti signálového spravodajstva v USA sa dotýkajú len nepatrnej časti komunikácie prechádzajúcej cez internet, vylučuje existencia prístupu k obsahu elektronickej komunikácie „na všeobecnom základe“⁽¹⁰⁰⁾.

3.1.2. Účinná právna ochrana

- (91) Komisia posúdila mechanizmy dohľadu, ktoré existujú v USA v súvislosti s akýmikoľvek zásahmi zo strany spravodajských orgánov USA do osobných údajov prenášaných do USA, ako aj možnosti individuálnej nápravy, ktoré majú k dispozícii dotknuté osoby z EÚ.

Dohľad

- (92) Spravodajské služby USA podliehajú rôznym mechanizmom preskúmania a dohľadu, ktoré patria do právomoci troch zložiek štátnej moci. Zahŕňajú vnútorné a vonkajšie orgány v rámci výkonnej zložky, niekoľko výborov Kongresu, ako aj súdny dohľad, v tomto prípade konkrétne so zreteľom na činnosti na základe zákona o sledovaní v rámci zahraničného spravodajstva.
- (93) Po prvé spravodajská činnosť orgánov USA je predmetom rozsiahleho dohľadu v rámci výkonnej moci.
- (94) Podľa prezidentskej politickej smernice 28, oddielu 4 písm. a) bodu iv), pravidlá a postupy zložiek spravodajských služieb „zahŕňajú primerané opatrenia na uľahčenie dohľadu nad uplatňovaním záruk na ochranu osobných informácií“; tieto opatrenia by mali zahŕňať pravidelné audity⁽¹⁰¹⁾.

⁽⁹⁸⁾ Vec Schrems, bod 91 s ďalšími odkazmi.

⁽⁹⁹⁾ Vec Schrems, bod 93.

⁽¹⁰⁰⁾ Pozri vec Schrems, bod 94.

⁽¹⁰¹⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (Ochrana osobných údajov všetkých ľudí: správa o stave týkajúca sa vývoja a vykonávania postupov podľa prezidentskej politickej smernice 28), s. 7. Pozri napr. CIA, Signals Intelligence Activities (Činnosti signálového spravodajstva), s. 6 (dodržiavanie predpisov); FBI, Presidential Policy Directive 28 Policies and Procedures (Podmienky a postupy podľa prezidentskej politickej smernice 28), odd. III písm. A) bod 4, písm. B) bod 4; NSA, PPD-28 Section 4 Procedures (Postupy podľa oddielu 4 prezidentskej politickej smernice 28), 12. januára 2015, oddiel 8.1, 8.6 písm. c).

- (95) V tomto ohľade bolo zavedených niekoľko vrstiev dohľadu vrátane úradníkov pre ochranu občianskych slobôd alebo súkromia, generálnych inšpektorov, Úradu ODNI na ochranu občianskych slobôd a súkromia, PCLOB a Výboru prezidenta pre dohľad nad spravodajskou službou. Tieto funkcie dohľadu podporujú vo všetkých agentúrach zamestnanci zaoberajúci sa dodržiavaním predpisov ⁽¹⁰²⁾.
- (96) Ako vysvetlila vláda USA ⁽¹⁰³⁾, *úradníci pre ochranu občianskych slobôd alebo súkromia* s úlohami dohľadu existujú na rôznych ministerstvách so spravodajskými úlohami a v spravodajských agentúrach ⁽¹⁰⁴⁾. Hoci konkrétne právomoci týchto úradníkov sa môžu mierne líšiť v závislosti od povolujuceho zákona, zvyčajne zahŕňajú dohľad nad postupmi s cieľom zabezpečiť, aby príslušné ministerstvo/agentúra primerane zohľadňovali otázky ochrany súkromia a občianskych slobôd a zaviedli vhodné postupy vybavovania sťažností fyzických osôb, ktoré sa domnievajú, že bolo narušené ich súkromie alebo občianske slobody (a v niektorých prípadoch, napríklad v rámci ODNI, môžu mať sami právomoc vyšetrovať sťažnosti ⁽¹⁰⁵⁾). Riaditeľ ministerstva/agentúry musí zasa zabezpečiť, aby úradník dostal všetky informácie a mal prístup ku všetkým materiálom potrebným na vykonávanie svojich funkcií. Úradníci pre ochranu občianskych slobôd alebo súkromia pravidelne podávajú správy Kongresu a PCLOB, ktoré okrem iného zahŕňajú informácie o počte a povahe sťažností prijatých ministerstvom/agentúrou a zhrnutia riešení týchto sťažností, vykonaných preskúmaní a zodpovedaných otázok a vplyvu činností vykonaných úradníkom ⁽¹⁰⁶⁾. Podľa posúdenia vnútroštátnych orgánov pre ochranu osobných údajov možno vnútorný dohľad vykonávaný úradníkmi pre ochranu občianskych slobôd alebo súkromia považovať za „pomerné spravodlivý“, hoci podľa ich názoru nedosahujú požadovanú úroveň nezávislosti ⁽¹⁰⁷⁾.
- (97) Každá zložka spravodajských služieb má navyše svojho vlastného *generálneho inšpektora*, ktorý okrem iného zodpovedá za dohľad nad zahraničnou spravodajskou činnosťou ⁽¹⁰⁸⁾. V rámci ODNI to zahŕňa Úrad generálneho inšpektora s rozsiahlou právomocou nad všetkými spravodajskými službami, ktorý je oprávnený vyšetrovať sťažnosti alebo informácie týkajúce sa obvinení z nezákonného konania alebo zneužitia právomoci v súvislosti s programami a činnosťami ODNI a/alebo spravodajských služieb ⁽¹⁰⁹⁾. Generálny inšpektor je zo zákona nezávislý ⁽¹¹⁰⁾ útvar zodpovedný za vykonávanie auditov a vyšetrovaní v súvislosti s programami a činnosťami vykonávanými príslušnou agentúrou na účely národného spravodajstva vrátane zneužitia alebo porušenia zákona ⁽¹¹¹⁾. Má oprávnenie na prístup ku všetkým záznamom, správam, auditom, preskúmaniam, dokumentom,
-
- ⁽¹⁰²⁾ Napríklad NSA zamestnáva viac než 300 takýchto zamestnancov na Riaditeľstve pre dodržiavanie predpisov. Pozri vyhlásenia ODNI (príloha VI), s. 7.
- ⁽¹⁰³⁾ Pozri Mechanizmus ombudsmana (príloha III), odd. 6 písm. b) body i) až iii).
- ⁽¹⁰⁴⁾ Pozri 42 U.S.C. § 2000ee-1. To zahŕňa napríklad ministerstvo zahraničných vecí, ministerstvo spravodlivosti (vrátane FBI), ministerstvo pre vnútornú bezpečnosť, ministerstvo obrany, NSA, CIA a ODNI.
- ⁽¹⁰⁵⁾ Podľa vlády USA, ak Úrad ODNI na ochranu občianskych slobôd a súkromia dostane sťažnosť, ďalšie spracovanie tejto sťažnosti v rámci spravodajských služieb bude koordinovať aj s ďalšími zložkami spravodajských služieb. Pozri Mechanizmus ombudsmana (príloha III), odd. 6 písm. b) bod ii).
- ⁽¹⁰⁶⁾ Pozri 42 U.S.C. § 2000ee-1. písm. f) body 1, 2.
- ⁽¹⁰⁷⁾ Stanovisko 01/2016 pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 k návrhu rozhodnutia o primeranosti štítu na ochranu osobných údajov medzi EÚ a USA (prijaté 13. apríla 2016), s. 41.
- ⁽¹⁰⁸⁾ Vyhlásenia ODNI (príloha VI), s. 7. Pozri napr. NSA, PPD-28 Section 4 Procedures (Postupy podľa oddielu 4 prezidentskej politickej smernice 28), 12. januára 2015, odd. 8.1; CIA, Signals Intelligence Activities (Činnosti signálového spravodajstva), s. 7 (úlohy).
- ⁽¹⁰⁹⁾ Tohto generálneho inšpektora (ktorého funkcia bola vytvorená v októbri 2010) menuje prezident s potvrdením Senátu a môže ho odvolať iba prezident, nie DNI.
- ⁽¹¹⁰⁾ Generálni inšpektori majú istú pozíciu a môže ich odvolať jedine prezident, ktorý musí Kongresu písomne oznámiť dôvody odvolania. To nutne neznamená, že nepodliehajú vôbec žiadnym pokynom. V niektorých prípadoch môže riaditeľ ministerstva zakázať generálnemu inšpektorovi začať, vykonávať alebo dokončiť audit alebo vyšetrovanie, ak to považuje za nevyhnutné na ochranu dôležitých národných (bezpečnostných) záujmov. Kongres však musí byť informovaný o uplatnení tejto právomoci a na tomto základe môže voči príslušnému riaditeľovi vyvolať zodpovednosť. Pozri napr. zákon o povolení spravodajstva na rozpočtový rok 2010, odd. 405 písm. f) (generálny inšpektor spravodajských služieb). Podľa posúdenia vnútroštátnych orgánov pre ochranu osobných údajov generálni inšpektori „pravdepodobne splnia kritérium organizačnej nezávislosti stanovené Súdnym dvorom Európskej únie a Európskym súdom pre ľudské práva prinajmenšom od momentu, odkedy sa na všetkých začne vzťahovať nový nominálny proces.“ Pozri stanovisko 01/2016 pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 k návrhu rozhodnutia o primeranosti štítu na ochranu osobných údajov medzi EÚ a USA (prijaté 13. apríla 2016), s. 40.
- ⁽¹¹¹⁾ Pozri vyhlásenia ODNI (príloha VI), s. 7. Pozri aj zákon o generálnom inšpektorovi z roku 1978, v znení neskorších predpisov, vyd. L. 113 – 126 zo 7. júla 2014.

publikáciám, odporúčaniam alebo iným relevantným materiálom, v prípade potreby aj prostredníctvom predvolania, a môže prijímať výpovede svedkov ⁽¹¹²⁾. Hoci generálni inšpektori môžu vydávať iba nezáväzné odporúčania na nápravné opatrenia, ich správy vrátane správ o následných opatreniach (alebo ich neexistencii) sa zverejňujú a navyše posielajú Kongresu, ktorý môže na tomto základe vykonávať svoju funkciu dohľadu ⁽¹¹³⁾.

- (98) Okrem toho existuje *Rada pre dohľad nad ochranou súkromia a občianskych slobôd*, čo je nezávislá agentúra ⁽¹¹⁴⁾ v rámci exekutívnej zložky zložená z piatich členov pochádzajúcich z dvoch politických strán ⁽¹¹⁵⁾ vymenovaných prezidentom so súhlasom Senátu na určené šesťročné obdobie, ktorá je poverená úlohami v oblasti politiky boja proti terorizmu a ich vykonávania s ohľadom na ochranu súkromia a občianskych slobôd. Pri skúmaní činnosti spravodajských služieb má prístup k všetkým relevantným záznamom, správam, auditom, preskúmaniam, dokumentom, publikáciám a odporúčaniam agentúr vrátane utajovaných informácií, môže viesť vypočúvania a prijímať výpovede svedkov. Prijíma správy od úradníkov pre ochranu občianskych slobôd a súkromia z viacerých federálnych úradov/agentúr ⁽¹¹⁶⁾, môže pre nich vydávať odporúčania a pravidelne podáva správy výborom Kongresu a prezidentovi ⁽¹¹⁷⁾. PCLOB má v rámci svojho mandátu takisto za úlohu pripravovať správu hodnotiacu vykonávanie prezidentskej politickej smernice 28.
- (99) A napokon, uvedené mechanizmy dohľadu dopĺňa *Výbor pre dohľad nad spravodajskou službou* zriadený v rámci Poradného výboru prezidenta pre spravodajskú službu, ktorý dohliada na dodržiavanie ústavy a všetkých príslušných predpisov spravodajskými orgánmi USA.
- (100) V záujme uľahčenia dohľadu sa zložky spravodajských služieb nabádajú, aby vytvorili informačné systémy, ktoré umožnia monitorovanie, zaznamenávanie a skúmanie otázok alebo iných vyhľadávaní osobných informácií ⁽¹¹⁸⁾. Orgány pre dohľad a dodržiavanie predpisov budú pravidelne kontrolovať postupy zložiek spravodajských služieb v oblasti ochrany osobných informácií obsiahnutých v signálovom spravodajstve a ich súlad s týmito postupmi ⁽¹¹⁹⁾.
- (101) Tieto funkcie dohľadu sú navyše podporované rozsiahlymi požiadavkami na podávanie správ o nedodržiavaní predpisov. Postupy agentúr musia najmä zabezpečiť, aby v prípade, že sa vyskytne významný problém s dodržiavaním predpisov v súvislosti s osobnými informáciami akejkoľvek osoby bez ohľadu na jej štátnu príslušnosť, ktoré boli zhromaždené prostredníctvom signálového spravodajstva, bol tento problém ihneď oznámený riaditeľovi zložky spravodajských služieb, ktorý to následne oznámi riaditeľovi národnej spravodajskej služby, a ten podľa prezidentskej politickej smernice 28 určí, či sú potrebné nejaké nápravné opatrenia ⁽¹²⁰⁾. Podľa vykonávacieho nariadenia č. 12333 sú navyše všetky zložky spravodajských služieb povinné hlásiť Výboru pre dohľad nad spravodajskou službou incidenty týkajúce sa nedodržania predpisov ⁽¹²¹⁾. Tieto mechanizmy

⁽¹¹²⁾ Pozri zákon o generálnom inšpektorovi z roku 1978, § 6.

⁽¹¹³⁾ Pozri vyhlásenia ODNI (príloha VI), s. 7. Pozri aj zákon o generálnom inšpektorovi z roku 1978, §§ 4 ods. 5, 5. Podľa odd. 405 písm. b) body 3, 4 zákona o povolení spravodajstva na rozpočtový rok 2010, vyd. L. 111 – 259 zo 7. októbra 2010 generálny inšpektor spravodajských služieb bude informovať DNI a Kongres o nutnosti nápravných opatrení a o ich vykonávaní.

⁽¹¹⁴⁾ Podľa posúdenia vnútroštátnych orgánov pre ochranu osobných údajov PCLOB v minulosti „preukázal svoje nezávislé právomoci“. Pozri stanovisko 01/2016 pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 k návrhu rozhodnutia o primeranosti štítu na ochranu osobných údajov medzi EÚ a USA (prijaté 13. apríla 2016), s. 42.

⁽¹¹⁵⁾ PCLOB navyše zamestnáva približne 20 stálych zamestnancov. Pozri <https://www.pclob.gov/about-us/staff.html>.

⁽¹¹⁶⁾ Patrí medzi ne prinajmenšom ministerstvo spravodlivosti, ministerstvo obrany, ministerstvo pre vnútornú bezpečnosť, riaditeľ národnej spravodajskej služby a Ústredná spravodajská služba, ako aj každé iné ministerstvo, agentúra alebo prvok exekutívy určený PCLOB ako vhodný na zahrnutie.

⁽¹¹⁷⁾ Pozri 42 U.S.C. § 2000ee. Pozri aj Mechanizmus ombudsmana (príloha III), odd. 6 písm. b) bod iv). PCLOB musí okrem iného nahlásiť, ak výkonná agentúra odmietne dodržať jeho odporúčanie.

⁽¹¹⁸⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (Ochrana osobných údajov všetkých ľudí: správa o stave týkajúca sa vývoja a vykonávania postupov podľa prezidentskej politickej smernice 28), s. 7 – 8.

⁽¹¹⁹⁾ Tamže na s. 8. Pozri aj vyhlásenia ODNI (príloha VI), s. 9.

⁽¹²⁰⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (Ochrana osobných údajov všetkých ľudí: správa o stave týkajúca sa vývoja a vykonávania postupov podľa prezidentskej politickej smernice 28), s. 7. Pozri napr. NSA, PPD-28 Section 4 Procedures (Postupy podľa oddielu 4 prezidentskej politickej smernice 28), 12. januára 2015, odd. 7.3, 8.7 písm. c), d); FBI, Presidential Policy Directive 28 Policies and Procedures (Pravidlá a postupy podľa prezidentskej politickej smernice), odd. III písm. A) bod 4, písm. B) bod 4; CIA, Signals Intelligence Activities (Činnosti signálového spravodajstva), s. 6 (dodržiavanie predpisov) a s. 8 (úlohy).

⁽¹²¹⁾ Pozri vykonávacie nariadenie č. 12333, odd. 1.6 písm. c).

zabezpečujú, aby sa problém riešil na najvyššej úrovni spravodajských služieb. Keď ide o osobu, ktorá nie je občanom USA, riaditeľ národnej spravodajskej služby po konzultácii s ministrom zahraničných vecí a riaditeľom oznamujúceho ministerstva alebo agentúry určí, či sa majú prijať opatrenia na oznámenie veci príslušnej zahraničnej vláde v súlade s ochranou zdrojov a metód a pracovníkov USA ⁽¹²²⁾.

- (102) Po druhé, okrem týchto mechanizmov dohľadu v rámci exekutívy vykonáva úlohy dohľadu nad všetkými zahraničnými spravodajskými činnosťami USA vrátane signálového spravodajstva aj Kongres USA, konkrétne výbory *Snemovne reprezentantov* a *Senátu pre spravodajskú službu a súdnictvo*. Podľa zákona o národnej bezpečnosti „prezident zabezpečí, aby výbory Kongresu pre spravodajskú službu boli v plnej miere a ihneď informované o spravodajských činnostiach USA vrátane všetkých významných očakávaných spravodajských činností, ktoré sa vyžadujú podľa tejto podkapitoly“ ⁽¹²³⁾. Zároveň „prezident zabezpečí, aby sa každá protiprávna spravodajská činnosť, ako aj všetky nápravné opatrenia, ktoré boli prijaté alebo sa plánujú prijať v súvislosti s touto protiprávnou činnosťou, urýchlene oznámili výborom Kongresu pre spravodajskú službu“ ⁽¹²⁴⁾. Členovia týchto výborov majú prístup k utajovaným informáciám, ako aj k spravodajským metódam a programom ⁽¹²⁵⁾.
- (103) V neskorších zákonoch sa rozšírili a spresnili oznamovacie požiadavky, pokiaľ ide o zložky spravodajských služieb, príslušných generálnych inšpektorov i generálneho prokurátora. Napríklad v zákone FISA sa vyžaduje, aby generálny prokurátor „plne informoval“ výbory Snemovne reprezentantov a Senátu pre spravodajskú službu a súdnictvo o činnostiach vlády podľa určitých častí zákona FISA ⁽¹²⁶⁾. Ďalej vyžaduje, aby vláda poskytla výborom Kongresu „kópie všetkých rozhodnutí, nariadení alebo stanovísk Súdu pre sledovanie v rámci zahraničného spravodajstva alebo Revízného súdu pre sledovanie v rámci zahraničného spravodajstva ktoré obsahujú významné vysvetlenia alebo výklady“ ustanovení zákona FISA. Dohľad nad sledovaním podľa oddielu 702 zákona FISA sa konkrétne vykonáva prostredníctvom zákonom požadovaných správ pre výbory pre spravodajskú službu a súdnictvo, ako aj prostredníctvom častých brífingov a vypočutí. Patrí medzi ne polročná správa generálneho prokurátora o uplatňovaní oddielu 702 zákona FISA s podpornými dokumentmi, ktoré zahŕňajú najmä správy ministerstva spravodlivosti a ODNI o dodržiavaní predpisov a opis prípadných incidentov týkajúcich sa nedodržania predpisov ⁽¹²⁷⁾, a samostatné polročné posúdenie generálneho prokurátora a DNI, ktoré dokumentuje dodržiavanie postupov zacielenia a minimalizácie vrátane dodržiavania postupov, ktoré zabezpečujú, aby sa zber údajov vykonával na legitímne účely zahraničného spravodajstva ⁽¹²⁸⁾. Kongres dostáva aj správy od generálnych inšpektorov, ktorí sú oprávnení hodnotiť dodržiavanie postupov zacielenia a minimalizácie a usmernení generálneho prokurátora zo strany agentúr.
- (104) Podľa zákona USA o slobode z roku 2015 musí vláda USA Kongresu (a verejnosti) každý rok sprístupniť informácie okrem iného o počte vyžiadaných a prijatých príkazov a smerníc podľa zákona FISA, ako aj odhady počtu občanov a rezidentov USA a iných osôb, ktoré boli predmetom sledovania ⁽¹²⁹⁾. V zákone sa takisto vyžaduje podávanie ďalších verejných správ o počte vydaných NSL, opäť v súvislosti s občanmi alebo rezidentmi

⁽¹²²⁾ Prezidentská politická smernica 28, odd. 4 písm. a) bod iv).

⁽¹²³⁾ Pozri odd. 501 písm. a) bod 1 (50 U.S.C. § 413 písm. a) bod 1). Toto ustanovenie obsahuje všeobecné požiadavky na dohľad Kongresu v oblasti národnej bezpečnosti.

⁽¹²⁴⁾ Pozri odd. 501 písm. b) [50 U.S.C. § 413 písm. b)].

⁽¹²⁵⁾ Pozri odd. 501 písm. d) [50 U.S.C. § 413 písm. d)].

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

⁽¹²⁷⁾ Pozri 50 U.S.C. § 1881f.

⁽¹²⁸⁾ Pozri 50 U.S.C. § 1881a ods. 1 pododsek 1.

⁽¹²⁹⁾ Pozri zákon USA o slobode z roku 2015, vyd. L. č. 114 – 23, odd. 602 písm. a). Podľa odd. 402 navyše „riaditeľ národnej spravodajskej služby po konzultácii s generálnym prokurátorom vykoná preskúmanie na účely odtajnenia každého rozhodnutia, príkazu alebo stanoviska vydaného Súdom pre sledovanie v rámci zahraničného spravodajstva alebo Revíznym súdom pre sledovanie v rámci zahraničného spravodajstva [ktoré sú vymedzené v oddiele 601 písm. e)], ktoré obsahuje významné vysvetlenie alebo výklad akéhokoľvek právneho ustanovenia vrátane akéhokoľvek nového alebo významného vysvetlenia alebo výkladu pojmu „špecifický výberový pojem“, a v súlade s týmto preskúmaním zverejní v najväčšej uskutočniteľnej miere každé také rozhodnutie, príkaz alebo stanovisko“.

USA aj inými osobami (pričom zároveň umožňuje príjemcom príkazov a certifikácií podľa zákona FISA a žiadostí NSL vydávať za určitých podmienok správy na účely zabezpečenia transparentnosti) ⁽¹³⁰⁾.

- (105) Po tretie, v prípade spravodajských činností orgánov verejnej moci USA na základe zákona FISA je možné nechať preskúmať a v niektorých prípadoch vopred schváliť príslušné opatrenia súdom FISC ⁽¹³¹⁾, čo je nezávislý tribunál ⁽¹³²⁾, ktorého rozhodnutia možno napadnúť na Revíznom súde pre sledovanie v rámci zahraničného spravodajstva (Foreign Intelligence Surveillance Court of Review – FISCR) ⁽¹³³⁾ a ako poslednú možnosť aj na Najvyššom súde USA ⁽¹³⁴⁾. V prípade predchádzajúceho schválenia musia žiadajúce orgány (FBI, NSA, CIA atď.) predložiť návrh žiadosti právnikom z oddelenia pre národnú bezpečnosť ministerstva spravodlivosti, ktorí ho skontrolujú a v prípade potreby si vyžadujú ďalšie informácie ⁽¹³⁵⁾. Po dokončení žiadosti ju musí schváliť generálny prokurátor, zástupca generálneho prokurátora alebo asistent generálneho prokurátora pre národnú bezpečnosť ⁽¹³⁶⁾. Ministerstvo spravodlivosti potom predloží žiadosť súdu FISC, ktorý ju posúdi a predbežne stanoví ďalší postup ⁽¹³⁷⁾. Ak sa uskutoční vypočutie, súd FISC je oprávnený prijímať výpovede svedkov, ktoré môžu zahŕňať stanovisko experta ⁽¹³⁸⁾.

- (106) Súd FISC (a FISCR) je podporovaný stálym výborom piatich osôb, ktoré majú odborné poznatky v otázkach národnej bezpečnosti a občianskych slobôd ⁽¹³⁹⁾. Z tejto skupiny súd vymenuje osobu, ktorá bude slúžiť ako *amicus curiae* a pomáhať pri posudzovaní všetkých žiadostí o príkaz alebo preskúmanie, ktoré podľa názoru súdu predstavujú nový alebo významný výklad zákona, pokiaľ súd nezistí, že také vymenovanie nie je vhodné ⁽¹⁴⁰⁾. Tým sa má najmä zabezpečiť, aby sa v posúdení súdu náležite zohľadnili otázky súkromia. Súd môže tiež vymenovať osobu alebo organizáciu za *amicus curiae* (vrátane poskytovania technických poznatkov) vždy, keď to považuje za vhodné, prípadne môže na základe návrhu povoliť osobe alebo organizácii, aby predložila informácie *amicus curiae* ⁽¹⁴¹⁾.

⁽¹³⁰⁾ Zákon USA o slobode, odd. 602 písm. a), 603 písm. a).

⁽¹³¹⁾ V prípade určitých druhov sledovania môže mať právomoc vypočúvať žiadosti a vydávať príkazy magistrátny sudca USA, ktorého verejne vymenúva predseda Najvyššieho súdu USA.

⁽¹³²⁾ Súd FISC sa skladá z jedenástich sudcov, ktorých vymenúva predseda Najvyššieho súdu USA z radov úradujúcich sudcov obvodných súdov USA, ktorých predtým vymenoval prezident a potvrdil Senát. Sudcovia, ktorí majú doživotné funkčné obdobie, môžu byť odvolaní len z dobrých dôvodov, slúžia súdu FISC na sedemročné funkčné obdobie s nejednotným začiatkom. V zákone FISA sa vyžaduje, aby sa sudcovia vyberali aspoň zo siedmich rôznych súdnych obvodov USA. Pozri odd. 103 zákona FISA [50 U.S.C. 1803 písm. a)]; PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 174 – 187. Sudcom pomáhajú skúsení súdni úradníci, ktorí pracujú ako právnici súdu a pripravujú právne analýzy žiadostí týkajúcich sa zberu údajov. Pozri PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 178; List ctihodného Reggieho B. Waltona, predsedajúceho sudcu Súdu pre sledovanie v rámci zahraničného spravodajstva USA, ctihodnému Patrickovi J. Leahymu, predsedovi Výboru pre súdnictvo Senátu USA (29. júla 2013) (ďalej len „Waltonov list“), s. 2 – 3.

⁽¹³³⁾ FISCR sa skladá z troch sudcov, ktorých vymenúva predseda Najvyššieho súdu USA a ktorí sa vyberajú z radov sudcov obvodných súdov alebo odvolacích súdov USA a slúžia na sedemročné funkčné obdobie s nejednotným začiatkom. Pozri odd. 103 FISA [50 U.S.C. § 1803 písm. b)].

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

⁽¹³⁵⁾ Napríklad ďalšie faktické podrobnosti o celi sledovania, technické informácie o metodike sledovania alebo záruky v súvislosti s tým, ako sa zhromaždené informácie budú používať a šíriť. Pozri PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 177.

⁽¹³⁶⁾ 50 U.S.C. §§ 1804 písm. a), 1801 písm. g).

⁽¹³⁷⁾ Súd FISC môže schváliť žiadosť, požiadať o ďalšie informácie, určiť nutnosť vypočutia alebo naznačiť možné zamietnutie žiadosti. Na základe tohto predbežného stanovenia vláda predloží konečnú žiadosť. Tá môže obsahovať podstatné zmeny oproti pôvodnej žiadosti na základe predbežných pripomienok sudcu. Hoci súd FISC schváli veľké percento konečných žiadostí, značná časť z nich obsahuje podstatné zmeny oproti pôvodnej žiadosti, napr. 24 % žiadostí schválených v období od júla do septembra 2013. Pozri PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 179; Waltonov list, s. 3.

⁽¹³⁸⁾ PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 179, č. 619.

⁽¹³⁹⁾ 50 U.S.C. § 1803 písm. i) bod 1, 3 písm. A). Do tohto nového právneho predpisu sa zapracovali odporúčania PCLOB týkajúce sa vytvorenia skupiny odborníkov na otázky ochrany súkromia a občianskych slobôd, ktorí môžu slúžiť ako *amicus curiae*, aby mal súd k dispozícii právne argumenty na posilnenie ochrany súkromia a občianskych slobôd. Pozri PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 183 – 187.

⁽¹⁴⁰⁾ 50 U.S.C. § 1803 písm. i) bod 2 písm. A). Podľa informácií ODNI k takým vymenovaniam už došlo. Pozri Signals Intelligence Reform (Reforma signálového spravodajstva), správa o pokroku z roku 2016.

⁽¹⁴¹⁾ 50 U.S.C. § 1803 písm. i) bod 2 písm. B).

(107) Pokiaľ ide o dve zákonné povolenia sledovania podľa zákona FISA, ktoré sú z hľadiska prenosu údajov v rámci štítu na ochranu osobných údajov medzi EÚ a USA najdôležitejšie, dohľad súdu FISC je odlišný.

(108) Podľa oddielu 501 zákona FISA ⁽¹⁴²⁾, ktorý umožňuje získavanie „akýchkoľvek hmotných vecí (vrátane kníh, záznamov, publikácií, dokumentov a ďalších položiek)“, musí žiadosť adresovaná súdu FISC obsahovať vyhlásenie o skutočnostiach, ktoré preukazujú, že existujú opodstatnené dôvody domnievať sa, že požadované hmotné veci sú relevantné pre povolené vyšetrovanie (okrem posúdenia hrozieb), ktoré sa vykonáva s cieľom získať zahraničné spravodajské informácie o osobe, ktorá nie je občanom USA, alebo na ochranu pred medzinárodným terorizmom alebo tajnou spravodajskou činnosťou. Žiadosť musí obsahovať aj výpočet postupov minimalizácie prijatých generálnym prokurátorom na účely uchovávania a šírenia zhromaždených spravodajských informácií. ⁽¹⁴³⁾

(109) Naopak, podľa oddielu 702 zákona FISA súd FISC ⁽¹⁴⁴⁾ nepovoľuje jednotlivé opatrenia sledovania; povoľuje skôr programy sledovania (ako PRISM, UPSTREAM) na základe každoročných certifikácií pripravených generálnym prokurátorom a riaditeľom národnej spravodajskej služby. Oddiel 702 zákona FISA umožňuje zacielenie na osoby, o ktorých možno odôvodnene predpokladať, že sa nachádzajú mimo územia USA, s cieľom získať zahraničné spravodajské informácie ⁽¹⁴⁵⁾. NSA vykonáva toto zacielenie v dvoch krokoch: po prvé, analytici NSA identifikujú osoby, ktoré nie sú občanmi ani rezidentmi USA, nachádzajúce sa v zahraničí, ktorých sledovanie bude na základe posúdenia analytikov viesť k zhromaždeniu relevantných zahraničných spravodajských informácií stanovených v certifikácii. Po druhé keď boli tieto individualizované osoby identifikované a ich zacielenie bolo schválené prostredníctvom rozsiahleho mechanizmu preskúmania v rámci NSA ⁽¹⁴⁶⁾, určia sa (t. j. vypracujú a uplatnia) selektory, ktoré identifikujú komunikačné kanály (napríklad e-mailové adresy) používané cieľmi ⁽¹⁴⁷⁾. Ako bolo uvedené, certifikácie, ktoré schvaľuje súd FISC, neobsahujú žiadne informácie o jednotlivých osobách, ktoré majú byť zacielené, ale identifikujú kategórie zahraničných spravodajských informácií ⁽¹⁴⁸⁾. Hoci súd FISC neposudzuje – na základe pravdepodobnej príčiny alebo inej normy –, či boli osoby správne zacielené s cieľom získať zahraničné spravodajské informácie ⁽¹⁴⁹⁾, jeho kontrola sa vzťahuje na podmienku, že „významným účelom získavania údajov je získať zahraničné spravodajské informácie“ ⁽¹⁵⁰⁾. Podľa oddielu 702 zákona FISA smie NSA získavať komunikácie osôb, ktoré nie sú občanmi ani rezidentmi USA, mimo USA iba v prípade, ak sa možno odôvodnene domnievať, že daný komunikačný prostriedok sa používa na komunikáciu zahraničných spravodajských informácií (napr. súvisiacich s medzinárodným terorizmom, šírením jadrových zbraní alebo nepriateľskými kybernetickými činnosťami). Určenia na tento účel podliehajú súdnemu preskúmaniu ⁽¹⁵¹⁾. Certifikácie musia obsahovať aj postupy zacielenia a minimalizácie ⁽¹⁵²⁾. Dodržiavanie

⁽¹⁴²⁾ 50 U.S.C. § 1861

⁽¹⁴³⁾ 50 U.S.C. § 1861 písm. b).

⁽¹⁴⁴⁾ 50 U.S.C. § 1881.

⁽¹⁴⁵⁾ 50 U.S.C. § 1881a písm. a).

⁽¹⁴⁶⁾ PCLOB, Sec. 702 Report (Správa podľa odd. 702), s. 46.

⁽¹⁴⁷⁾ 50 U.S.C. § 1881a písm. h).

⁽¹⁴⁸⁾ 50 U.S.C. § 1881a písm. g). Podľa PCLOB sa tieto kategórie doteraz týkali predovšetkým medzinárodného terorizmu a tém, ako je získavanie zbraní hromadného ničenia. Pozri PCLOB, Sec. 702 Report (Správa podľa odd. 702), s. 25.

⁽¹⁴⁹⁾ PCLOB, Sec. 702 Report (Správa podľa odd. 702), s. 27.

⁽¹⁵⁰⁾ 50 U.S.C. § 1881a.

⁽¹⁵¹⁾ „Liberty and Security in a Changing World“, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (Sloboda a bezpečnosť v meniacom sa svete, správa a odporúčania skupiny prezidenta pre preskúmanie spravodajských a komunikačných technológií), 12. decembra 2013, s. 152.

⁽¹⁵²⁾ 50 U.S.C. § 1881a písm. i).

predpisov overuje generálny prokurátor a riaditeľ národnej spravodajskej služby a agentúry sú povinné oznámiť všetky incidenty týkajúce sa nedodržania predpisov súdu FISC ⁽¹⁵³⁾ (ako aj Kongresu a Výboru prezidenta pre dohľad nad spravodajskou službou), ktorý môže na tomto základe upraviť povolenie ⁽¹⁵⁴⁾.

- (110) V záujme zvýšenia účinnosti dohľadu zo strany súdu FISC navyše administratíva USA súhlasila s vykonaním odporúčania PCLOB poskytnúť súdu FISC dokumentáciu o rozhodnutiach o zacielení podľa oddielu 702 vrátane náhodnej vzorky hárkov s úlohami, aby súd FISC mohol posúdiť, ako sa v praxi uplatňuje požiadavka na účel zahraničného spravodajstva ⁽¹⁵⁵⁾. Administratíva USA zároveň súhlasila s revíziou postupov NSA týkajúcich sa zacielenia a prijala na tieto účely príslušné opatrenia s cieľom lepšie zdokumentovať odôvodnenie rozhodnutí o zacielení založené na účele zahraničného spravodajstva ⁽¹⁵⁶⁾.

Individuálna náprava

- (111) Podľa práva USA majú dotknuté osoby z EÚ, ktoré majú obavy v súvislosti s tým, či ich osobné údaje boli spracované (zhromaždené, sprístupnené atď.) zločkami spravodajských služieb USA, a ak áno, či boli dodržané obmedzenia platné podľa práva USA, k dispozícii niekoľko možností. Týkajú sa v podstate troch oblastí: zásahov podľa zákona FISA, nezákonného zámerného prístupu k osobným údajom úradníkmi vlády; a prístupu k informáciám podľa zákona o slobodnom prístupe k informáciám (Freedom of Information Act – FOIA) ⁽¹⁵⁷⁾.
- (112) Po prvé zákon o sledovaní v rámci zahraničného spravodajstva obsahuje viacero opravných prostriedkov aj pre osoby, ktoré nie sú občanmi ani rezidentmi USA, proti nezákonnému elektronickému sledovaniu ⁽¹⁵⁸⁾. Fyzické osoby majú možnosť podať občianskoprávnu žalobu o peňažné odškodné proti USA, keď boli informácie o nich nezákonne a úmyselne použité alebo zverejnené ⁽¹⁵⁹⁾; žalovať osobne úradníkov vlády USA (za protiprávne konanie „pod zámenkou zákona“) o peňažné odškodné ⁽¹⁶⁰⁾; a napadnúť zákonnosť sledovania (s cieľom utajiť informácie) v prípade, že vláda USA chce použiť alebo zverejniť akékoľvek informácie získané alebo odvodené z elektronického sledovania jednotlivcov v súdnom alebo správnom konaní v USA ⁽¹⁶¹⁾.
- (113) Po druhé, vláda USA informovala Komisiu o niekoľkých ďalších možnostiach, ktoré dotknuté osoby z EÚ môžu využiť v snahe uplatniť opravný prostriedok proti úradníkom vlády za nezákonný prístup vlády k osobným

⁽¹⁵³⁾ Pravidlo 13b) vnútorného poriadku súdu FISC vyžaduje, aby vláda predložila súdu písomné oznámenie ihneď po tom, ako zistí, že nejaké povolenie alebo schválenie vydané súdom bolo vykonané spôsobom, ktorý nie je v súlade s povolením alebo schválením súdu alebo s príslušnými právnymi predpismi. Zároveň vyžaduje, aby vláda písomne oznámila súdu skutočnosť a okolnosti, ktoré sú relevantné pre toto nedodržanie predpisov. Vláda zvyčajne predloží konečné oznámenie podľa pravidla 13a), keď sú známe relevantné skutočnosti a všetky neoprávnené zhromaždené údaje boli zničené. Pozri Waltonov list, s. 10.

⁽¹⁵⁴⁾ 50 U.S.C. § 1881 písm. l). Pozri aj PCLOB, Sec. 702 Report (Správa podľa odd. 702), s. 66 – 76. NSA CLPO, NSA's Implementation of Foreign Intelligence surveillance Act Section 702 (Vykonávanie oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva zo strany NSA), 16. apríla 2014. Zber osobných údajov na spravodajské účely podľa odd. 702 zákona FISA podlieha vnútornému aj vonkajšiemu dohľadu v rámci exekutívy. Vnútorný dohľad okrem iného zahŕňa vnútorné programy na vyhodnocovanie dodržiavania postupov zacielenia a minimalizácie a dohľad nad nimi; hlásenie incidentov týkajúcich sa nedodržania postupov na vnútornej i vonkajšej úrovni ODNI, ministerstvu spravodlivosti, Kongresu a súdu FISC; a každoročné preskúmania posielané rovnakým orgánom. Vonkajší dohľad spočíva najmä v preskúmaní zacielenia a minimalizácie vykonávaných ODNI, ministerstvom spravodlivosti a generálnymi inšpektormi, ktorí následne podávajú správy Kongresu a súdu FISC, a to aj o incidentoch týkajúcich sa nedodržania postupov. Významné incidenty týkajúce sa nedodržania postupov sa musia súdu FISC oznámiť ihneď, ostatné sa oznamujú v štvrtročnej správe. Pozri PCLOB, Sec. 702 Report (Správa podľa odd. 702), s. 66 – 77.

⁽¹⁵⁵⁾ PCLOB, Recommendations Assessment Report (Hodnotiacá správa s odporúčaniami), 29. januára 2015, s. 20.

⁽¹⁵⁶⁾ PCLOB, Recommendations Assessment Report (Hodnotiacá správa s odporúčaniami), 29. januára 2015, s. 16.

⁽¹⁵⁷⁾ V odd. 10 zákona o postupoch pre utajované informácie sa uvádza, že v každom trestnom stíhaní, v ktorom USA musia preukázať, že určitý materiál predstavuje utajované informácie (napr. preto, lebo si vyžaduje ochranu pred neoprávneným zverejnením z dôvodu národnej bezpečnosti), USA oznámia odporcov, ktoré časti materiálu chcú odôvodnene využiť na preukázanie skutočnosti, že informácie relevantné pre konanie podliehajú utajeniu.

⁽¹⁵⁸⁾ Pozri tieto vyhlásenia ODNI (príloha VI), s. 16.

⁽¹⁵⁹⁾ 18 U.S.C. § 2712.

⁽¹⁶⁰⁾ 50 U.S.C. § 1810.

⁽¹⁶¹⁾ 50 U.S.C. § 1806.

údajom alebo za ich používanie, a to aj na údajné účely národnej bezpečnosti (t. j. zákon o počítačových podvodoch a zneužívaní ⁽¹⁶²⁾; zákon o ochrane súkromia v rámci elektronickej komunikácie ⁽¹⁶³⁾; a zákon o práve na ochranu osobných finančných údajov ⁽¹⁶⁴⁾). Všetky tieto žalobné dôvody sa týkajú špecifických údajov, cieľov a/alebo druhov prístupu (napr. vzdialeného prístupu k počítaču cez internet) a sú k dispozícii za určitých podmienok (napr. úmyselné/zámerné konanie, konanie mimo úradnej právomoci, utrpená ujma) ⁽¹⁶⁵⁾. V zákone o správnom konaní (5 U.S.C. § 702) sa ponúka všeobecnejšia možnosť nápravy, podľa ktorej „každá osoba, ktorá utrpí právnu krivdu kvôli konaniu agentúry, alebo ktorú konanie agentúry nepriaznivo postihuje alebo poškodzuje“, má nárok dožadovať sa súdneho preskúmania. To zahŕňa možnosť požiadať súd, aby „činnosť agentúry, zistenia a závery, ktoré sa považujú za [...] svojvoľné, nevypočítateľné alebo za zneužitie právomoci, alebo inak v nesúlade so zákonom, vyhlásil za protiprávne a zrušil ich“ ⁽¹⁶⁶⁾.

- (114) A napokon, vláda USA poukazuje na zákon FOIA ako na prostriedok pre osoby, ktoré nie sú občanmi ani rezidentmi USA, ako požiadať o prístup k existujúcim záznamom federálnej agentúry vrátane prípadov, keď obsahujú osobné údaje fyzickej osoby ⁽¹⁶⁷⁾. Vzhľadom na svoje zameranie zákon FOIA neposkytuje možnosť individuálnej nápravy proti zásahom do osobných údajov ako takým, aj keď by v zásade mohol umožniť fyzickým osobám získať prístup k relevantným informáciám držaným národnými spravodajskými agentúrami. Aj v tomto ohľade sa možnosti zdajú obmedzené, lebo agentúry môžu odmietnuť poskytnúť informácie, na ktoré sa vzťahujú niektoré vymenované výnimky, a to vrátane prístupu k utajovaným informáciám súvisiacim s národnou bezpečnosťou a informáciám týkajúcim sa vyšetrovaní v rámci presadzovania práva ⁽¹⁶⁸⁾. Fyzické osoby však môžu napadnúť uplatnenie týchto výnimiek národnými spravodajskými agentúrami, pričom sa môžu domáhať správneho aj súdneho preskúmania.

- (115) Hoci teda fyzické osoby vrátane dotknutých osôb z EÚ majú niekoľko možností nápravy, keď sa stali predmetom nezákonného (elektronického) sledovania na účely národnej bezpečnosti, je jasné aj to, že tieto možnosti sa nevzťahujú aspoň na niektoré právne základy, ktoré spravodajské orgány USA môžu využiť (napr. vykonávacie nariadenie č. 12333). Navyše aj v tých prípadoch, keď v zásade existujú možnosti súdnej nápravy pre osoby, ktoré nie občanmi ani rezidentmi USA, napríklad v prípade sledovania na základe zákona FISA, sú dostupné dôvody žaloby obmedzené ⁽¹⁶⁹⁾, pretože žaloby podané fyzickými osobami (vrátane občanov a rezidentov USA) budú vyhlásené za nepripustné, ak nedokážu preukázať „aktívnu legitimitáciu“ ⁽¹⁷⁰⁾, čo obmedzuje prístup k všeobecným súdom ⁽¹⁷¹⁾.

- (116) S cieľom poskytnúť ďalšiu možnosť nápravy prístupnú pre všetky dotknuté osoby z EÚ sa vláda USA rozhodla vytvoriť nový mechanizmus ombudsmana, ako je uvedené v liste ministra zahraničných vecí USA Komisii, ktorý sa nachádza v prílohe III k tomuto rozhodnutiu. Tento mechanizmus nadväzuje na určenie vysokého koordinátora (na úrovni tajomníka ministra) na ministerstve zahraničných vecí podľa prezidentskej politickej smernice 28, ktorý je kontaktnou osobou pre zahraničné vlády na vyjadrenie obáv v súvislosti s činnosťou USA v oblasti signálového spravodajstva, ale značne presahuje túto pôvodnú koncepciu.

⁽¹⁶²⁾ 18 U.S.C. § 1030.

⁽¹⁶³⁾ 18 U.S.C. §§ 2701 – 2712.

⁽¹⁶⁴⁾ 12 U.S.C. § 3417.

⁽¹⁶⁵⁾ Vyhlásenia ODNI (príloha VI), s. 17.

⁽¹⁶⁶⁾ 5 U.S.C. § 706 ods. 2 písm. A).

⁽¹⁶⁷⁾ 5 U.S.C. § 552. Podobné zákony existujú aj na úrovni jednotlivých štátov.

⁽¹⁶⁸⁾ Ak to tak je, fyzická osoba zvyčajne dostane iba štandardnú odpoveď, ktorou agentúra odmietne potvrdiť alebo vyvrátiť existenciu akýchkoľvek záznamov. Pozri *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

⁽¹⁶⁹⁾ Pozri vyhlásenia ODNI (príloha VI), s. 16. Podľa poskytnutých vysvetlení sa v dostupných dôvodoch žaloby vyžaduje buď existencia *ujmy* (18 U.S.C. § 2712; 50 U.S.C. § 1810), alebo preukázanie, že *vláda má v úmysle použiť alebo zverejniť informácie* zhromaždené alebo odvodené z elektronického sledovania dotknutej osoby proti tejto osobe v *súdnom alebo správnom konaní* v USA (50 U.S.C. § 1806). Ako však Súdny dvor opakovane zdôraznil, na preukázanie existencie zásahu do základného práva na súkromie nezáleží na tom, či dotknutá osoba utrpela akékoľvek nepriaznivé následky z dôvodu tohto zásahu. Pozri vec *Schrems*, bod 89 s ďalšími odkazmi.

⁽¹⁷⁰⁾ Toto kritérium prípustnosti vychádza z článku III Ústavy USA, podľa ktorého sa súdna moc vzťahuje len na skutočné prípady a spory.

⁽¹⁷¹⁾ Pozri *Clapper/Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). Pokiaľ ide o využívanie NSL, v zákone USA o slobode (odd. 502 písm. f) – 503) sa stanovuje, že požiadavky na nezverejnenie sa musia pravidelne preskúmať a že *prijemcovia* NSL musia byť upozornení na to, že skutočnosti už nepodporujú požiadavku na nezverejnenie [pozri vyhlásenia ODNI (príloha VI), s. 13]. To však nezaručuje, že dotknutá osoba z EÚ bude informovaná, že sa stala predmetom vyšetrovania.

- (117) Podľa záväzkov vlády USA sa v rámci mechanizmu ombudsmana konkrétne zaistí, aby sa riadne vyšetrili a vyriešili sťažnosti fyzických osôb a aby fyzické osoby získali nezávislé potvrdenie, že boli dodržané zákony USA, alebo v prípade porušenia týchto zákonov, že ich porušenie bolo napravené ⁽¹⁷²⁾. Mechanizmus zahŕňa „ombudsmana pre štít na ochranu osobných údajov“, t. j. tajomníka ministra a ďalší personál, ako aj ostatné orgány dohľadu s právomocou dohliadať na jednotlivé zložky spravodajskej služby, na ktorej spoluprácu sa ombudsman pre štít o ochranu osobných údajov bude spoliehať pri vybavovaní sťažností. Konkrétne, ak sa žiadosť fyzickej osoby týka zlučiteľnosti sledovania s právom USA, ombudsman pre štít na ochranu osobných údajov sa bude môcť opierať o nezávislé orgány dohľadu s vyšetrovacími právomocami (napríklad generálni inšpektori alebo PCLOB). Minister v každom prípade zaistí, aby mal ombudsman prostriedky, ktorými sa zabezpečí, že odpoveď na jednotlivé žiadosti sa bude zakladať na všetkých potrebných informáciách.
- (118) V rámci mechanizmu ombudsmana sa touto „zloženou štruktúrou“ zaručuje nezávislý dohľad a individuálna náprava. Spolupracou s ostatnými orgánmi dohľadu sa okrem toho zaistuje prístup k nevyhnutným odborným znalostiam. A napokon, tým, že sa ombudsmanovi pre štít na ochranu osobných údajov ukladá povinnosť potvrdiť dodržanie alebo nápravu nedodržania zásad, sa v mechanizme zohľadňuje záväzok zo strany vlády USA ako celku zaoberať sa sťažnosťou a vyriešiť sťažnosť fyzických osôb z EÚ.
- (119) Po piate, na rozdiel od čisto medzivládneho mechanizmu bude ombudsman pre štít na ochranu osobných údajov prijímať sťažnosti fyzických osôb a odpovedať na ne. Tieto sťažnosti možno adresovať dozorným orgánom v členských štátoch, ktoré sú zodpovedné za dohľad nad národnými bezpečnostnými službami a/alebo spracovaním osobných údajov zo strany orgánov verejnej moci, ktoré ich predložia centralizovanému orgánu EÚ, odkiaľ budú postúpené k ombudsmanovi pre štít na ochranu osobných údajov ⁽¹⁷³⁾. To bude v skutočnosti prínosom pre fyzické osoby z EÚ, ktoré sa budú môcť obrátiť na vnútroštátny orgán „blízko domova“ a vo svojom vlastnom jazyku. Úlohou tohto orgánu bude podporovať fyzické osoby pri podávaní žiadostí ombudsmanovi pre štít na ochranu osobných údajov, ktoré budú obsahovať základné informácie, a teda sa budú môcť považovať za „úplné“. Fyzická osoba nemusí preukázať, že vláda USA skutočne získala prístup k jeho osobným údajom prostredníctvom činnosti signálového spravodajstva.
- (120) Po druhé vláda USA sa zaväzuje, že zaistí, aby sa ombudsman pre štít na ochranu osobných údajov pri vykonávaní svojich funkcií mohol spoliehať na spoluprácu v rámci iných mechanizmov dohľadu a preskúmania dodržiavania predpisov, ktoré existujú v práve USA. Niekedy to bude zahŕňať národné spravodajské orgány, najmä v prípade, ak sa má žiadosť chápať ako žiadosť o prístup k dokumentom v zmysle zákona o slobodnom prístupe k informáciám. V ostatných prípadoch, najmä ak sa žiadosti týkajú zlučiteľnosti sledovania s právom USA, bude táto spolupráca zahŕňať nezávislé orgány dohľadu (napríklad generálnych inšpektorov) so zodpovednosťou a právomocou vykonať dôkladné vyšetrovanie (najmä prostredníctvom prístupu k všetkým relevantným dokumentom a právomoci požadovať informácie a vyhlásenia) a zaoberať sa nedodržaním predpisov ⁽¹⁷⁴⁾. Ombudsman pre štít na ochranu osobných údajov bude takisto môcť postúpiť veci na posúdenie PCLOB ⁽¹⁷⁵⁾. Ak jeden z týchto orgánov dohľadu zistí akékoľvek nedodržanie predpisov, daná zložka spravodajských služieb (napríklad spravodajská agentúra) bude musieť toto nedodržanie pravidiel napraviť, pretože len tak sa umožní ombudsmanovi poskytnúť „kladnú“ odpoveď danej fyzickej osobe (t. j. že došlo k náprave každého nedodržania

⁽¹⁷²⁾ V prípade, že sťažovateľ požaduje prístup k dokumentom, ktoré majú v držbe orgány verejnej moci USA, uplatňujú sa pravidlá a postupy stanovené v zákone o slobodnom prístupe k informáciám. To zahŕňa možnosť dožadovať sa súdnej nápravy (namiesto nezávislého dohľadu) v prípade zamietnutia žiadosti, na základe podmienok stanovených v zákone o slobodnom prístupe k informáciám.

⁽¹⁷³⁾ Podľa odd. 4 písm. f) Mechanizmu ombudsmana (príloha III) bude ombudsman pre štít na ochranu osobných údajov komunikovať priamo s orgánom EÚ pre vybavovanie individuálnych sťažností, ktorý bude zase zodpovedný za komunikáciu s fyzickou osobou, ktorý predkladá žiadosť. Ak je súčasťou „základných procesov“, ktoré môžu poskytnúť požadovanú nápravu (napr. žiadosť o prístup podľa zákona FOIA, pozri odd. 5), priama komunikácia, táto komunikácia bude prebiehať v súlade s uplatniteľnými postupmi.

⁽¹⁷⁴⁾ Pozri Mechanizmus ombudsmana (príloha III), odd. 2 písm. a). Pozri aj odôvodnenia 0 – 0.

⁽¹⁷⁵⁾ Pozri Mechanizmus ombudsmana (príloha III), odd. 2 písm. c). Podľa vysvetlení poskytnutých vládou USA komisia PCLOB bude priebežne skúmať podmienky a postupy orgánov USA zodpovedných za boj proti terorizmu, ako aj ich vykonávanie týmito orgánmi, s cieľom zistiť, či ich činnosť „vhodne chráni súkromie a občianske slobody a či je v súlade s príslušnými zákonmi, predpismi a politikami týkajúcimi sa ochrany súkromia a občianskych slobôd“. Bude takisto „prijímať a skúmať správy a iné informácie od úradníkov pre ochranu súkromia a úradníkov pre ochranu občianskych slobôd a, ak to bude vhodné, vypracuje pre nich odporúčania týkajúce sa ich činnosti“.

predpisov), k čomu sa vláda USA zaviazala. Okrem toho v rámci spolupráce bude ombudsman pre štít na ochranu osobných údajov informovaný o výsledku vyšetrovania a bude mať prostriedky, ktorými sa zaistí, aby získal všetky informácie potrebné na prípravu jeho odpovede.

- (121) A napokon, ombudsman pre štít na ochranu osobných údajov bude nezávislý, a teda nebude prijímať pokyny od spravodajských služieb USA ⁽¹⁷⁶⁾. To má veľký význam vzhľadom na to, že ombudsman bude musieť „potvrdiť“, že i) sťažnosť bola riadne vyšetrená a že ii) boli dodržané príslušné právne predpisy USA – okrem iného najmä obmedzenia a záruky uvedené v prílohe VI –, alebo v prípade ich porušenia, že toto porušenie bolo napravené. Na to, aby ombudsman pre štít na ochranu osobných údajov mohol poskytnúť toto nezávislé potvrdenie, bude musieť získať potrebné informácie týkajúce sa vyšetrovania s cieľom posúdiť presnosť odpovede na sťažnosť. Minister sa navyše zaviazal, že zaistí, aby tajomník ministra vykonával funkciu ombudsmana pre štít na ochranu osobných údajov objektívne a bez akéhokoľvek nevhodného vplyvu, ktorý môže mať vplyv na pripravované odpovede.
- (122) Celkovo sa týmto mechanizmom zaisťuje, že sťažnosti fyzických osôb sa budú dôkladne vyšetrovať a riešiť a že prinajmenšom v oblasti sledovania to bude zahŕňať nezávislé orgány dohľadu s potrebnými odbornými znalosťami a vyšetrovacími právomocami a ombudsmana, ktorý bude schopný vykonávať svoje funkcie bez nevhodného, predovšetkým politického, vplyvu. Fyzické osoby budú navyše môcť predložiť sťažnosti bez toho, aby museli preukázať, že boli predmetom sledovania, alebo o tom poskytnúť informácie ⁽¹⁷⁷⁾. Vzhľadom na tieto prvky je Komisia presvedčená o tom, že proti zneužívaniu existujú vhodné a účinné záruky.
- (123) Komisia na základe všetkých uvedených skutočností dospela k záveru, že USA zabezpečujú účinnú právnu ochranu pred zásahmi svojich spravodajských orgánov do základných práv osôb, ktorých údaje sa prenášajú z Únie do USA v rámci štítu na ochranu osobných údajov medzi EÚ a USA.
- (124) Komisia v tejto súvislosti berie na vedomie rozsudok Súdneho dvora vo veci *Schrems*, podľa ktorého „právna úprava, ktorá neupravuje nijakú možnosť fyzickej osoby podliehajúcej súdnej právomoci uplatniť právne prostriedky nápravy, aby mala prístup k osobným údajom, ktoré sa jej týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov, nerešpektuje podstatu obsahu základného práva na účinnú súdnu ochranu, ako je upravené článkom 47 Charty“ ⁽¹⁷⁸⁾. Posúdením Komisie sa potvrdilo, že takéto právne prostriedky nápravy sú v USA ustanovené, a to aj prostredníctvom zavedenia mechanizmu ombudsmana. Mechanizmom ombudsmana sa poskytuje nezávislý dohľad a vyšetrovacie právomoci. V rámci neustáleho monitorovania štítu na ochranu osobných údajov zo strany Komisie, okrem iného aj prostredníctvom každoročného spoločného preskúmania, ktoré bude takisto zahŕňať ombudsmana, sa účinnosť tohto mechanizmu bude opätovne posudzovať.

3.2. Prístup a použitie zo strany orgánov verejnej moci USA na účely presadzovania práva a verejného záujmu

- (125) Pokiaľ ide o zásahy do osobných údajov prenášaných v rámci štítu na ochranu osobných údajov medzi EÚ a USA na účely presadzovania práva, vláda USA (prostredníctvom ministerstva spravodlivosti) poskytla uistenie v súvislosti s platnými obmedzeniami a zárukami, ktoré podľa posúdenia Komisie preukazujú primeranú úroveň ochrany.

⁽¹⁷⁶⁾ Pozri Roman Zakharov/Rusko, rozsudok zo 4. decembra 2015 (Veľká komora), číslo žiadosti 47143/06, bod 275 („hoci v zásade je žiaduce zveriť kontrolu nad dohľadom sudcovi, dohľad zo strany mimosúdnych orgánov sa môže považovať za zlučiteľný s Dohovorom za predpokladu, že orgán dohľadu je nezávislý od orgánov vykonávajúcich sledovanie a sú mu zverené dostatočné a účinné právomoci dohľadu“).

⁽¹⁷⁷⁾ Pozri Kennedy/Spojené kráľovstvo, rozsudok z 18. mája 2010, č. žiadosti 26839/05, bod 167.

⁽¹⁷⁸⁾ Vec *Schrems*, bod 95. Ako vyplýva z bodov 91, 96 rozsudku, bod 95 sa týka úrovne ochrany zaručenej v právnom poriadku Únie, s ktorou musí byť úroveň ochrany v tretej krajine „v podstate rovnocenná“. Podľa bodov 73 a 74 rozsudku si to nevyžaduje, aby úroveň ochrany alebo prostriedky, ktoré tretia krajina využíva, museli byť identické, hoci prostriedky, ktoré sa majú použiť, sa musia v praxi preukázať ako účinné.

- (126) Podľa tejto informácie domové prehliadky a zaistenia zo strany orgánov presadzovania práva podľa štvrtého dodatku k ústave USA ⁽¹⁷⁹⁾ si predovšetkým ⁽¹⁸⁰⁾ vyžadujú, aby súd vydal príkaz na základe preukázania „pravdepodobnej príčiny“. V niekoľkých osobitne stanovených a výnimočných prípadoch, keď požiadavka na súdny príkaz neplatí ⁽¹⁸¹⁾, presadzovanie práva podlieha skúške „odôvodnenosti“ ⁽¹⁸²⁾. To, či sú domová prehliadka alebo zaistenie odôvodnené, „závisí od posúdenia na jednej strane miery, v akej zasahujú do súkromia fyzickej osoby, a na druhej strane miery, v akej sú nutné na presadenie oprávnených záujmov vlády“ ⁽¹⁸³⁾. Všeobecnejšie štvrtý dodatok zaručuje súkromie, dôstojnosť a chráni pred svojvoľnými a rušivými činmi úradníkov vlády ⁽¹⁸⁴⁾. Tieto koncepcie zodpovedajú zásadám nevyhnutnosti a proporcionality, ktoré obsahuje právo Únie. Ak orgány presadzovania práva už nepotrebnú používať zabavené veci ako dôkaz, mali by ich vrátiť ⁽¹⁸⁵⁾.
- (127) Hoci práva vyplývajúce zo štvrtého dodatku sa nevzťahujú na osoby, ktoré nie sú občanmi ani rezidentmi USA, tieto osoby sú ním napriek tomu nepriamo chránené, a to vzhľadom na skutočnosť, že osobné údaje majú v držbe spoločnosti v USA s tým účinkom, že orgány presadzovania práva musia v každom prípade žiadať o súdne povolenie (alebo aspoň dodržať požiadavku týkajúcu sa opodstatnenosti) ⁽¹⁸⁶⁾. Ďalšiu ochranu poskytujú osobitné zákonné orgány, ako aj usmernenia ministerstva spravodlivosti, ktoré obmedzujú prístup orgánov presadzovania práva k údajom z dôvodov, ktoré sú rovnocenné nevyhnutnosti a proporcionality (napr. požiadavkou, aby FBI použila čo najmenej obťažujúce vyšetrovacie metódy s ohľadom na ich vplyv na ochranu súkromia a občianskych slobôd) ⁽¹⁸⁷⁾. Podľa vyhlásení vlády USA sa rovnaká alebo vyššia ochrana vzťahuje na vyšetrovania v rámci presadzovania práva na úrovni štátu (pokiaľ ide o vyšetrovania vykonávané podľa zákonov štátu) ⁽¹⁸⁸⁾.
- (128) Hoci predchádzajúce povolenie súdu alebo veľkej poroty (vyšetrovací orgán súdu zostavený sudcom alebo magistrátnym sudcom) sa nevyžaduje vo všetkých prípadoch ⁽¹⁸⁹⁾, správne predvolania sú obmedzené na osobitné prípady a budú predmetom nezávislého súdneho preskúmania aspoň vtedy, keď sa vláda snaží o ich presadenie na súde ⁽¹⁹⁰⁾.
- ⁽¹⁷⁹⁾ Podľa štvrtého dodatku „právo osôb byť v bezpečí pred neodôvodnenými prehliadkami a zabaveniami, pokiaľ ide o osoby, domy, dokumenty a osobný majetok, sa nesmie porušiť a nesmú sa vydať žiadne príkazy okrem príkazov na základe pravdepodobnej príčiny, na základe prísahy alebo potvrdenia a v ktorých sa konkrétne opisuje miesto, ktoré sa má prehľadať, a osoby alebo veci, ktoré sú predmetom zabavenia.“ Príkazy na domovú prehliadku môžu vydávať iba (magistrátni) sudcovia. Federálne príkazy týkajúce sa kopírovania elektronicky uložených informácií sú ďalej upravené v pravidle 41 federálnych pravidiel trestného konania.
- ⁽¹⁸⁰⁾ Najvyšší súd opakovanne označil prehliadky bez príkazov za „mimoriadne“. Pozri napr. *Johnson/United States*, 333 U.S. 10, 14 (1948); *McDonald/United States*, 335 U.S. 451, 453 (1948); *Camara v. Municipal Court*, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp./United States*, 429 U.S. 338, 352-53, 355 (1977). Podobne Najvyšší súd pravidelne zdôrazňuje, že „najzákladnejším ústavným pravidlom v tejto oblasti je, že prehliadky vykonávané mimo súdneho konania bez predchádzajúceho súhlasu sudcu alebo magistrátneho sudcu, sú v zmysle štvrtého dodatku – samé o sebe neodôvodnené, a to okrem len niekoľkých osobitne stanovených a podrobne vymedzených výnimiek.“ Pozri napr. *Coolidge/New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp./United States*, 429 U.S. 338, 352-53, 358 (1977).
- ⁽¹⁸¹⁾ *Vec City of Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010).
- ⁽¹⁸²⁾ PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 107, s odkazom na *vec Maryland/King*, 133 S. Ct. 1958, 1970 (2013).
- ⁽¹⁸³⁾ PCLOB, Sec. 215 Report (Správa podľa odd. 215), s. 107, s odkazom na *vec Samson/California*, 547 U.S. 843, 848 (2006).
- ⁽¹⁸⁴⁾ *Vec City of Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.
- ⁽¹⁸⁵⁾ Pozri napr. *United States/Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).
- ⁽¹⁸⁶⁾ Pozri rozsudok *Roman Zakharov/Rusko*, zo 4. decembra 2015 (Veľká komora), číslo žiadosti 47143/06, bod 269, podľa ktorého „požiadavka ukázať povolenie na odpočúvanie poskytovateľovi komunikačných služieb pred získaním prístupu ku komunikácii osoby je jednou z dôležitých záruk pred zneužívaním zo strany orgánov presadzovania práva, ktorou sa zaisťuje, že vo všetkých prípadoch odpočúvania sa získa riadne povolenie.“
- ⁽¹⁸⁷⁾ Vyhlásenia ministerstva spravodlivosti (príloha VII), s. 4 s ďalšími odkazmi.
- ⁽¹⁸⁸⁾ Vyhlásenia ministerstva spravodlivosti (príloha VII), s. 2.
- ⁽¹⁸⁹⁾ Podľa informácií, ktoré Komisia dostala, a bez ohľadu na osobitné oblasti, ktoré pravdepodobne nie sú podstatné z hľadiska prenosu údajov v rámci štítu na ochranu osobných údajov medzi EÚ a USA (napr. vyšetrovania podvodov v oblasti zdravotnej starostlivosti, zneužívania detí alebo prípady kontrolovaných látok), sa to týka hlavne určitých orgánov podliehajúcich zákonu o ochrane súkromia v rámci elektronickej komunikácie (Electronic Communications Privacy Act – ECPA), konkrétne žiadostí o základné informácie o účastníkoch, komunikácii a zúčtovaní [18 U.S.C. § 2703 písm. c) body 1 a 2, napríklad adresa, typ/dĺžka služby] a o obsahu e-mailov starších ako 180 dní [18 U.S.C. § 2703 písm. a) a b)]. V druhom prípade to však dotknutej fyzickej osobe musí byť oznámené, a má teda príležitosť napadnúť žiadosť na súde. Pozri aj prehľad ministerstva spravodlivosti, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Prehľadávanie a zabavenie počítačov a získanie elektronických dôkazov pri vyšetrovaniach trestných činov), kapitola 3: *Stored Communications Act* (zákon o uloženej komunikácii), s. 115 – 138.
- ⁽¹⁹⁰⁾ Podľa vyhlásení vlády USA príjemcovia správnych predvolaní môžu tieto predvolania napadnúť na súde z dôvodu, že sú neopodstatnené, t. j. prehnané, obmedzujúce alebo neprimerane zťažujúce. Pozri vyhlásenia ministerstva spravodlivosti (príloha VII), s. 2.

- (129) To isté platí aj pre používanie správnych predvolaní na predloženie údajov na účely verejného záujmu. Podľa vyhlásení vlády USA sa navyše podobné významné obmedzenia uplatňujú aj v tom ohľade, že agentúry môžu žiadať o prístup len k tým údajom, ktoré sú relevantné pre záležitosti patriace do ich rozsahu právomocí, a musia dodržiavať zásadu opodstatnenosti.
- (130) V práve USA sa navyše stanovuje niekoľko možností súdnej nápravy pre fyzické osoby, a to voči orgánu verejnej moci alebo jednému z jeho úradníkov, ak tieto orgány spracovávajú osobné údaje. Tieto možnosti, ku ktorým patrí najmä zákon o správnom konaní (Administrative Procedure Act – APA), zákon o slobodnom prístupe k informáciám (Freedom of Information Act – FOIA) a zákon o súkromí v elektronickej komunikácii (Electronic Communications Privacy Act – ECPA), môžu využiť všetky fyzické osoby bez ohľadu na ich štátnu príslušnosť s výhradou akýchkoľvek uplatniteľných podmienok.
- (131) Vo všeobecnosti má v zmysle ustanovení zákona o správnom konaní ⁽¹⁹¹⁾ týkajúcich sa súdneho preskúmania „každá osoba, ktorá utrpí právnu krivdu v dôsledku činnosti agentúry, alebo ktorú činnosť agentúry nepriaznivo postihuje alebo poškodzuje“, nárok dožadovať sa súdneho preskúmania ⁽¹⁹²⁾. To zahŕňa možnosť požiadať súd, aby „činnosť agentúry, zistenia a závery, ktoré sa považujú za [...] svojvoľné, nevypočítateľné alebo za zneužitie právomoci, alebo inak v nesúlade so zákonom, vyhlásil za protiprávne a zrušil ich“ ⁽¹⁹³⁾.
- (132) Konkrétnejšie, v hlave II zákona o súkromí v elektronickej komunikácii ⁽¹⁹⁴⁾ sa uvádza systém zákonných práv v oblasti ochrany súkromia a ako takým sa ním upravuje prístup orgánov presadzovania práva k obsahu telefonickej, ústnej alebo elektronickej komunikácie, ktorú uchovávajú poskytovatelia služieb, ktorí sú tretími stranami ⁽¹⁹⁵⁾. Trestne sa ním postihuje nezákonný prístup (t. j. nie povolený súdom alebo inak prípustný) k tejto komunikácii a poskytuje sa ním možnosť nápravy pre dotknuté osoby prostredníctvom podania občianskoprávnej žaloby na federálnom súde USA o náhradu skutočnej škody a represívnu náhradu škody, ako aj spravodlivé alebo deklaratórne nápravné opatrenie voči štátnemu úradníkovi, ktorý vedome spáchal tieto nezákonné činy, alebo voči USA.
- (133) Takisto v zmysle zákona o slobodnom prístupe k informáciám (FOIA, 5 U.S.C. § 552) má každá osoba právo získať prístup k záznamom federálnej agentúry a po vyčerpaní správnych opravných prostriedkov si vymôcť toto právo na súde, pokiaľ tieto záznamy nie sú chránené pred zverejnením na základe výnimky alebo osobitného vylúčenia z presadzovania práva ⁽¹⁹⁶⁾.

⁽¹⁹¹⁾ 5 U.S.C. § 702.

⁽¹⁹²⁾ Predmetom súdneho preskúmania je vo všeobecnosti len „konečné“ konanie agentúry – a nie „predbežné, procesné alebo priebežné“ konanie agentúry. Pozri 5 U.S.C. § 704.

⁽¹⁹³⁾ 5 U.S.C. § 706 ods. 2 písm. A).

⁽¹⁹⁴⁾ 18 U.S.C. §§ 2701 – 2712.

⁽¹⁹⁵⁾ Zákomom ECPA sa ochraňuje komunikácia, ktorú uchovávajú dve určené triedy poskytovateľov sieťových služieb, konkrétne poskytovatelia: i) elektronických komunikačných služieb, ako je napríklad telefónia alebo e-mail; ii) diaľkových počítačových služieb, napríklad služby počítačového úložiska alebo služby spracovania.

⁽¹⁹⁶⁾ Tieto vylúčenia sú však presne vymedzené. Napríklad podľa 5 U.S.C. § 552 písm. b) bodu 7 sú práva v zmysle zákona FOIA vylúčené v prípade „záznamov alebo informácií zostavených na účely presadzovania práva, ale len v rozsahu, v akom by sa v súvislosti so zostavením týchto záznamov alebo informácií na účely presadzovania práva A) mohlo odôvodnene očakávať, že budú predstavovať zásah do konania na presadenie práva; B) zbavila osoba práva na spravodlivý proces alebo nezaujaté rozhodnutie; C) mohlo primerane očakávať, že budú predstavovať bezdôvodné narušenie súkromia; D) mohlo primerane očakávať, že sa v nich odhalí totožnosť dôverného zdroja, vrátane štátnej, miestnej alebo zahraničnej agentúry alebo orgánu alebo akejkoľvek súkromnej inštitúcie, ktorá poskytla informácie na dôvernom základe, a v prípade záznamu alebo informácií zostavených orgánom činným v trestnom konaní v priebehu vyšetrovania trestného činu alebo agentúrou vykonávajúcou zákonnú právomoc týkajúcu sa spravodajstva v oblasti národnej bezpečnosti, informácie poskytnuté dôverným zdrojom; E) odhalili techniky a postupy vyšetrovania alebo žaloby v oblasti presadzovania práva, alebo by sa odhalili usmernenia pre vyšetrovania alebo žaloby v oblasti presadzovania práva, keby sa dalo primerane očakávať, že na základe tohto odhalenia by hrozilo obchádzanie zákona; alebo F) mohlo primerane očakávať, že ohrozia život alebo telesnú bezpečnosť akejkoľvek fyzickej osoby.“ Zároveň, „vždy pri podaní žiadosti, ktorá zahŕňa prístup k záznamom (v súvislosti so zostavením ktorých by sa dalo primerane očakávať, že bude zasahovať do konania na presadenie práva) a – A) vyšetrovanie alebo konanie zahŕňa možné porušenie trestného práva; a B) existuje dôvod domnievať sa, že i) osoba, ktorá je predmetom vyšetrovania alebo konania, si nie je vedomá, že konanie prebieha; ii) v súvislosti s odhalením existencie záznamov by sa dalo primerane očakávať, že bude zasahovať do konania na presadenia práva, môže agentúra len počas takého obdobia, keď táto okolnosť pretrváva, považovať záznamy za také, ktoré nepodliehajú požiadavkám tohto oddielu.“ (5 U.S.C. § 552 písm. c) bod1).

- (134) Navyše niekoľko ďalších zákonov poskytuje fyzickým osobám právo podať žalobu na orgán verejnej moci USA alebo úradníka, pokiaľ ide o spracovanie ich osobných údajov, napríklad zákon o odpočúvaní ⁽¹⁹⁷⁾, zákon o počítačových podvodoch a zneužívaní ⁽¹⁹⁸⁾, federálny zákon o žalobe za ujmu ⁽¹⁹⁹⁾, zákon o práve na ochranu osobných finančných údajov ⁽²⁰⁰⁾ a zákon o náležitom podávaní informácií o úverovej schopnosti zákazníkov ⁽²⁰¹⁾.
- (135) Komisia preto dospela k záveru, že v USA existujú platné pravidlá, ktorých cieľom je obmedziť akékoľvek zásahy na účely presadzovania práva ⁽²⁰²⁾ alebo iného verejného záujmu do základných práv osôb, ktorých osobné údaje sa prenášajú z Únie do USA v rámci štítu na ochranu osobných údajov medzi EÚ a USA, na to, čo je nevyhnutne potrebné na dosiahnutie príslušného legitímneho cieľa, a ktoré zaisťujú účinnú právnu ochranu pred takými zásahmi.

4. PRIMERANÁ ÚROVEŇ OCHRANY V RÁMCI ŠTÍTU NA OCHRANU OSOBNÝCH ÚDAJOV MEDZI EÚ A USA

- (136) Na základe týchto zistení sa Komisia domnieva, že USA zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám v USA, ktoré osvedčili svoje dodržiavanie zásad, v rámci štítu na ochranu osobných údajov medzi EÚ a USA.
- (137) Komisia sa najmä domnieva, že zásady vydané Ministerstvom obchodu USA ako celok zabezpečujú úroveň ochrany osobných údajov, ktorá je v podstate rovnocenná ochrane zaručenej základnými zásadami stanovenými v smernici 95/46/ES.
- (138) Účinné uplatňovanie zásad je navyše zaručené povinnosťami týkajúcimi sa transparentnosti a tým, že štít na ochranu osobných údajov spravuje ministerstvo obchodu.
- (139) Komisia sa navyše domnieva, že dohľad a mechanizmy nápravy, ktoré poskytuje štít na ochranu osobných údajov, ako celok umožňujú v praxi odhaľovať a trestať porušenia zásad ochrany súkromia organizáciami zapojenými do štítu na ochranu osobných údajov a poskytujú právne prostriedky nápravy, prostredníctvom ktorých môže dotknutá osoba získať prístup k osobným údajom, ktoré sa jej týkajú, a domôcť sa opravy alebo vymazania týchto údajov.
- (140) A napokon, na základe dostupných informácií o právnom poriadku USA vrátane vyhlásení a záväzkov vlády USA sa Komisia domnieva, že akékoľvek zásahy orgánov verejnej moci USA do základných práv osôb, ktorých údaje sa prenášajú z Únie do USA v rámci štítu na ochranu osobných údajov na účely národnej bezpečnosti, presadzovania práva alebo iných verejných záujmov, a následné obmedzenia organizácií, ktoré osvedčili svoje dodržiavanie zásad, s ohľadom na to, ako dodržiavajú zásady, budú obmedzené na to, čo je nevyhnutne potrebné na dosiahnutie príslušného legitímneho cieľa, a že existuje účinná právna ochrana pred takými zásahmi.

⁽¹⁹⁷⁾ 18 U.S.C. §§ 2510 a nasl. V zmysle zákona o odpočúvaní (18 U.S.C. § 2520) môže fyzická osoba, ktorej telefonická, ústna alebo elektronická komunikácia sa zachytáva, zverejňuje alebo zámerne používa, podať občianskoprávnu žalobu za porušenie zákona o odpočúvaní, pričom za istých okolností môže podať žalobu aj na konkrétno štátneho úradníka alebo na USA. Zber adresných informácií a iných neobsahových informácií (napríklad IP adresa, adresa odosielateľa/príjemcu v e-maile), je uvedený aj v kapitole záznamníky zdrojov a cieľov elektronickej komunikácie v hlave 18 (18 U.S.C. §§ 3121 – 3127 a žaloba v občianskoprávnom konaní § 2707).

⁽¹⁹⁸⁾ 18 U.S.C. § 1030. V zmysle zákona o počítačových podvodoch a zneužívaní môže osoba podať žalobu na akúkoľvek osobu, pokiaľ ide o úmyselný neoprávnený prístup (alebo prekročenie oprávneného prístupu) s cieľom získať informácie od finančnej inštitúcie, z počítačového systému vlády USA alebo iného uvedeného počítača, pričom za istých okolností možno žalovať aj konkrétno štátneho úradníka.

⁽¹⁹⁹⁾ 28 U.S.C. §§ 2671 a nasl. V zmysle federálneho zákona o žalobe za ujmu môže osoba za istých okolností podať žalobu na USA, pokiaľ ide o „nedbalý alebo nezákonný akt alebo omyl akéhokoľvek zamestnanca štátu, ktorý koná v rozsahu pôsobnosti svojej funkcie alebo zamestnania.“

⁽²⁰⁰⁾ 12 U.S.C. §§ 3401 a nasl. V zmysle zákona o práve na ochranu osobných finančných údajov môže osoba za istých okolností podať žalobu na USA, pokiaľ ide o získanie alebo zverejnenie chránených finančných záznamov v rozpore so zákonom. Prístup vlády k chráneným finančným záznamom je vo všeobecnosti zakázaný, pokiaľ vláda nepodá žiadosť na základe právoplatného predvolania alebo príkazu na prehliadku alebo, pričom toto ustanovenie podlieha obmedzeniam, formálnu písomnú žiadosť a fyzickej osobe, o ktorej informácie sa žiada, nebude doručené oznámenie o takejto žiadosti.

⁽²⁰¹⁾ 15 U.S.C. §§ 1681 – 1681x. V zmysle zákona o náležitom podávaní informácií o úverovej schopnosti zákazníkov môže osoba podať žalobu na akúkoľvek osobu, ktorá nesplní požiadavky (predovšetkým potrebu právoplatného povolenia) týkajúce sa zhromažďovania, šírenia a použitia informácií o úverovej schopnosti zákazníkov, pričom za istých okolností možno podať žalobu na vládnu agentúru.

⁽²⁰²⁾ Súdny dvor uznal, že presadzovanie práva predstavuje legitímny politický cieľ. Pozri spojené veci C-293/12 a C-594/12, Digital Rights Ireland a i., EU:C:2014:238, bod 42. Pozri aj článok 8 ods. 2 EDLP a rozsudok Európskeho súdu pre ľudské práva vo veci Weber and Saravia/Nemecko, číslo žiadosti 54934/00, bod 104.

- (141) Komisia dospela k záveru, že sú tým splnené normy článku 25 smernice 95/46/ES vykladaného v duchu Charty základných práv Európskej únie, ako to vysvetlil Súdny dvor najmä v rozsudku vo veci Schrems.

5. ČINNOSŤ ORGÁNOV NA OCHRANU ÚDAJOV A INFORMÁCIE POSKYTOVANÉ KOMISII

- (142) Súdny dvor v rozsudku vo veci Schrems objasnil, že Komisia nemá právomoc obmedziť právomoci orgánov pre ochranu osobných údajov vyplývajúce z článku 28 smernice 95/46/ES (vrátane právomoci pozastaviť prenosy údajov), ak osoba, ktorá podáva žalobu podľa tohto ustanovenia, spochybňuje zlučiteľnosť rozhodnutia Komisie o primeranosti s ochranou základného práva na súkromie a ochranu údajov ⁽²⁰³⁾.
- (143) Aby bolo možné účinne kontrolovať fungovanie štítu na ochranu osobných údajov, členské štáty by mali informovať Komisiu o príslušných opatreniach prijatých orgánmi pre ochranu osobných údajov.
- (144) Súdny dvor ďalej konštatoval, že v súlade s článkom 25 ods. 6 druhým pododsekom smernice 95/46/ES členské štáty a ich orgány musia prijať opatrenia potrebné na dosiahnutie súladu s aktmi inštitúcií Únie, lebo na tieto opatrenia sa v zásade vzťahuje prezumpcia zákonnosti, a majú preto právne účinky dovtedy, kým neboli derogované, zrušené v konaní o žalobe o neplatnosť alebo vyhlásené za neplatné v nadväznosti na návrh na začatie prejudiciálneho konania alebo námietku nezákonnosti. Rozhodnutie Komisie o primeranosti prijaté podľa článku 25 ods. 6 smernice 95/46/ES je preto záväzné pre všetky orgány členských štátov, ktoré sú jeho adresátmi, vrátane ich nezávislých orgánov dohľadu ⁽²⁰⁴⁾. Keď taký orgán prijme sťažnosť spochybňujúcu súlad rozhodnutia Komisie o primeranosti s ochranou základného práva na súkromie a ochranu údajov a domnieva sa, že predložené námietky sú dôvodné, vnútroštátne právo mu musí poskytnúť právny prostriedok nápravy umožňujúci predložiť tieto námietky vnútroštátnemu súdu, ktorý v prípade pochybností musí prerušiť konanie a podať návrh na začatie prejudiciálneho konania na Súdnom dvore ⁽²⁰⁵⁾.

6. PRAVIDELNÉ PRESKÚMANIE ZISTENIA O PRIMERANOSTI

- (145) Vzhľadom na to, že úroveň ochrany poskytovaná právnym poriadkom USA môže podliehať zmenám, Komisia bude po prijatí tohto rozhodnutia pravidelne skúmať, či sú zistenia o primeranosti úrovne ochrany poskytovanej USA v rámci štítu na ochranu osobných údajov medzi EÚ a USA stále skutkovo a právne odôvodnené. Toto preskúmanie sa v každom prípade vyžaduje vtedy, keď Komisia získa akékoľvek informácie vedúce k dôvodným pochybnostiam v tomto ohľade ⁽²⁰⁶⁾.
- (146) Z tohto dôvodu bude Komisia priebežne monitorovať celkový rámec pre prenos osobných údajov vytvorený štítom na ochranu osobných údajov medzi EÚ a USA, ako aj dodržiavanie vyhlásení a záväzkov uvedených v dokumentoch priložených k tomuto rozhodnutiu orgánmi USA. S cieľom uľahčiť tento proces sa USA zaviazali, že budú informovať Komisiu o dôležitom vývoji v práve USA, ak bude relevantný pre štít na ochranu osobných údajov v oblasti ochrany osobných údajov a obmedzení a záruk vzťahujúcich sa na prístup k osobným údajom zo strany orgánov verejnej moci. Toto rozhodnutie bude okrem toho podliehať každoročnému spoločnému preskúmaniu, ktoré sa bude týkať všetkých aspektov fungovania štítu na ochranu osobných údajov medzi EÚ a USA vrátane uplatňovania výnimiek zo zásad súvisiacich s národnou bezpečnosťou a presadzovaním práva. Okrem toho keďže záver o primeranosti môže byť ovplyvnený aj právnym vývojom v práve Únie, Komisia posúdi úroveň ochrany poskytovanú štítom na ochranu osobných údajov po nadobudnutí účinnosti všeobecného nariadenia o ochrane údajov.
- (147) Na účely vykonania každoročného spoločného preskúmania uvedeného v prílohách I, II a VI sa Komisia stretne s ministerstvom obchodu a FTC, ktoré v prípade potreby doplnia ďalšie ministerstvá a agentúry zapojené do vykonávania opatrení štítu na ochranu osobných údajov, a v prípade záležitostí týkajúcich sa národnej bezpečnosti aj so zástupcami ODNI, ďalších zložiek spravodajských služieb a ombudsmanom. Na tomto stretnutí sa budú môcť zúčastniť aj orgány pre ochranu osobných údajov z EÚ a zástupcovia pracovnej skupiny zriadenej podľa článku 29.

⁽²⁰³⁾ Vec Schrems, bod 40 a nasl., 101 – 103.

⁽²⁰⁴⁾ Vec Schrems, body 51, 52 a 62.

⁽²⁰⁵⁾ Vec Schrems, bod 65.

⁽²⁰⁶⁾ Vec Schrems, bod 76.

- (148) V rámci každoročného spoločného preskúmania bude Komisia požadovať, aby ministerstvo obchodu poskytlo podrobné informácie o všetkých dôležitých aspektoch fungovania štítu na ochranu osobných údajov medzi EÚ a USA vrátane žiadostí, ktoré ministerstvu obchodu postúpili orgány pre ochranu osobných údajov, a výsledkov *ex officio* preskúmaní dodržiavania predpisov. Komisia bude takisto žiadať o vysvetlenia prípadných otázok alebo záležitostí týkajúcich sa štítu na ochranu osobných údajov medzi EÚ a USA a jeho fungovania vyplývajúcich z dostupných informácií vrátane správ na účely zabezpečenia transparentnosti predkladaných podľa zákona USA o slobode, verejných správ národných spravodajských orgánov USA, orgánov pre ochranu osobných údajov, skupín pre ochranu súkromia, správ z médií alebo akýchkoľvek iných možných zdrojov. S cieľom uľahčiť prácu Komisie v tomto ohľade by navyše členské štáty mali informovať Komisiu o prípadoch, keď opatrenia orgánov zodpovedných za zabezpečenie dodržiavania zásad v USA nezabezpečili ich dodržiavanie, a o všetkých náznakoch, že opatrenia orgánov verejnej moci USA zodpovedných za národnú bezpečnosť alebo prevenciu, vyšetrovanie, odhaľovanie alebo stíhanie trestných činov nezabezpečujú požadovanú úroveň ochrany.
- (149) Komisia na základe každoročného spoločného preskúmania vypracuje verejnú správu, ktorú predloží Európskemu parlamentu a Rade.

7. POZASTAVENIE ROZHODNUTIA O PRIMERANOSTI

- (150) Ak na základe kontrol alebo akýchkoľvek iných dostupných informácií Komisia dospeje k záveru, že úroveň ochrany, ktorú poskytuje štít na ochranu osobných údajov, už nemožno považovať za v podstate rovnocennú s úrovňou v Únii, alebo ak sa vyskytnú jasné náznaky, že v USA už nie je zabezpečený účinné dodržiavanie zásad alebo že opatrenia orgánov verejnej moci USA zodpovedných za národnú bezpečnosť alebo prevenciu, vyšetrovanie, odhaľovanie alebo stíhanie trestných činov nezabezpečujú požadovanú úroveň ochrany, bude o tom informovať ministerstvo obchodu a požiada, aby sa v stanovenej primeranej lehote prijali vhodné opatrenia na urýchléné riešenie prípadného nedodržania zásad. Ak po uplynutí stanovenej lehoty orgány USA uspokojivo nepreukázu, že štít na ochranu osobných údajov medzi EÚ a USA aj naďalej zabezpečuje účinné dodržiavanie zásad a primeranú úroveň ochrany, Komisia začne konanie vedúce k čiastočnému alebo úplnému pozastaveniu alebo zrušeniu tohto rozhodnutia ⁽²⁰⁷⁾. Prípadne môže Komisia navrhnúť zmenu tohto rozhodnutia, napríklad tým, že obmedzí rozsah pôsobnosti zistenia o primeranosti iba na prenosy údajov podliehajúce dodatočným podmienkam.
- (151) Komisia začne konanie o pozastavení alebo zrušení najmä v prípade:
- a) náznakov, že orgány USA nedodržiavajú vyhlásenia a záväzky uvedené v dokumentoch priložených k tomuto rozhodnutiu, a to aj pokiaľ ide o podmienky a obmedzenia prístupu orgánov verejnej moci USA k osobným údajom prenášaným v rámci štítu na ochranu osobných údajov na účely presadzovania práva, národnej bezpečnosti a iné účely verejného záujmu;
 - b) neschopnosti účinne riešiť sťažnosti dotknutých osôb z EÚ; Komisia v tejto súvislosti vezme do úvahy všetky okolnosti, ktoré majú vplyv na možnosť dotknutých osôb z EÚ vymáhať ich práva, najmä dobrovoľný záväzok spoločností v USA, ktoré osvedčili svoje dodržiavanie zásad, spolupracovať s orgánmi pre ochranu osobných údajov a riadiť sa ich radami;
 - c) že ombudsman pre štít na ochranu osobných údajov včas neposkytne primerané odpovede na žiadosti dotknutých osôb z EÚ.
- (152) Komisia takisto zváži začatie konania vedúceho k zmene, pozastaveniu alebo zrušeniu tohto rozhodnutia, ak v kontexte každoročného spoločného preskúmania fungovania štítu na ochranu osobných údajov medzi EÚ a USA alebo v inom kontexte ministerstvo obchodu alebo iné ministerstvá alebo agentúry zapojené do vykonávania štítu na ochranu osobných údajov, prípadne, ak ide o záležitosti týkajúce sa národnej bezpečnosti, predstavitelia spravodajských služieb USA alebo ombudsman neposkytnú informácie alebo vysvetlenia potrebné na posúdenie dodržiavania zásad, účinnosti postupov vybavovania sťažností, prípadne v súvislosti so znížením

⁽²⁰⁷⁾ Od dátumu uplatňovania všeobecného nariadenia o ochrane údajov bude Komisia využívať svoju právomoc prijať na základe riadne odôvodnených vážnych a naliehavých dôvodov vykonávací akt, ktorým pozastaví toto rozhodnutie a ktorý bude platiť okamžite bez jeho predchádzajúceho predloženia príslušnému komitologickému výboru a zostane v platnosti počas obdobia najviac šesť mesiacov.

požadovanej úrovne ochrany v dôsledku opatrení národných spravodajských orgánov USA, najmä v dôsledku zberu osobných údajov a/alebo prístupu k nim, ktorý sa neobmedzuje na to, čo je nevyhnutne potrebné a primerané. Komisia v tomto ohľade vezme do úvahy to, do akej miery možno príslušné informácie získať z iných zdrojov, okrem iného prostredníctvom správ od spoločností v USA, ktoré osvedčili svoje dodržiavanie zásad, ktoré sú povolené podľa zákona USA o slobode.

- (153) Pracovná skupina pre ochranu jednotlivcov so zreteľom na spracovanie osobných údajov zriadená podľa článku 29 smernice 95/46/ES uverejnila svoje stanovisko k úrovni ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA ⁽²⁰⁸⁾, ktoré sa zohľadnilo pri príprave tohto rozhodnutia.
- (154) Európsky parlament prijal uznesenie o transatlantických tokoch údajov ⁽²⁰⁹⁾.
- (155) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru zriadeného podľa článku 31 ods. 1 smernice 95/46/ES,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

1. Na účely článku 25 ods. 2 smernice 95/46/ES Spojené štáty zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie organizáciám v USA v rámci štítu na ochranu osobných údajov medzi EÚ a USA.
2. Štít na ochranu osobných údajov medzi EÚ a USA tvoria zásady vydané Ministerstvom obchodu USA 7. júla 2016, ktoré sú uvedené v prílohe II, a oficiálne vyhlásenia a záväzky obsiahnuté v dokumentoch uvedených v prílohách I, III až VII.
3. Na účely odseku 1 sa osobné údaje prenášajú v rámci štítu na ochranu osobných údajov medzi EÚ a USA, keď sa prenášajú z Únie organizáciám v USA, ktoré sú zahrnuté do „zoznamu organizácií zapojených do štítu na ochranu osobných údajov“, ktorý vedie a sprístupňuje verejnosti Ministerstvo obchodu USA v súlade s oddielmi I a III zásad stanovených v prílohe II.

Článok 2

Toto rozhodnutie nemá vplyv na uplatňovanie ustanovení smernice 95/46/ES okrem ustanovení článku 25 ods. 1, ktoré sa týkajú spracovania osobných údajov v členských štátoch, a najmä na článok 4 tejto smernice.

Článok 3

Keď príslušné orgány členských štátov uplatnia svoje právomoci podľa článku 28 ods. 3 smernice 95/46/ES, dôsledkom čoho je pozastavenie alebo trvalý zákaz tokov údajov organizácii v USA, ktorá je uvedená v zozname organizácií zapojených do štítu na ochranu osobných údajov v súlade s oddielmi I a III zásad stanovených v prílohe II, príslušný členský štát o tom v záujme ochrany fyzických osôb v súvislosti so spracovaním ich osobných údajov, bezodkladne informuje Komisiu.

Článok 4

1. Komisia bude priebežne monitorovať fungovanie štítu na ochranu osobných údajov medzi EÚ a USA s cieľom posúdiť, či USA aj naďalej zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných na jeho základe z Únie organizáciám v USA.

⁽²⁰⁸⁾ Stanovisko 01/2016 k návrhu rozhodnutia o primeranosti štítu na ochranu osobných údajov medzi EÚ a USA, prijaté 13. apríla 2016.

⁽²⁰⁹⁾ Uznesenie Európskeho parlamentu o transatlantických tokoch údajov z 26. mája 2016 [(2016/2727(RSP))]

2. Členské štáty a Komisia sa budú navzájom informovať o prípadoch, keď sa zdá, že vládne orgány v USA so zákonnou právomocou presadzovať dodržiavanie zásad stanovených v prílohe II neposkytujú účinné mechanizmy odhaľovania a dohľadu umožňujúce identifikovať a v praxi postihovať porušovanie zásad.

3. Členské štáty a Komisia sa budú navzájom informovať o všetkých náznakoch, že zásahy orgánov verejnej moci USA zodpovedných za národnú bezpečnosť, presadzovanie práva alebo iné verejné záujmy do práv fyzických osôb na ochranu osobných údajov presahujú rámec toho, čo je nevyhnutne potrebné, a/alebo že neexistuje účinná právna ochrana pred takými zásahmi.

4. Komisia do jedného roka odo dňa oznámenia tohto rozhodnutia členským štátom a potom každý rok vyhodnotí zistenie uvedené v článku 1 ods. 1 na základe všetkých dostupných informácií vrátane informácií, ktoré získa v rámci každoročného spoločného preskúmania uvedeného v prílohách I, II a VI.

5. Komisia oznámi všetky relevantné zistenia výboru zriadenému podľa článku 31 smernice 95/46/ES.

6. Komisia predloží návrh opatrení v súlade s postupom uvedeným v článku 31 ods. 2 smernice 95/46/ES s cieľom pozastaviť, zmeniť alebo zrušiť toto rozhodnutie alebo obmedziť jeho rozsah pôsobnosti, keď, okrem iného, existujú náznaky:

- že orgány verejnej moci USA nedodržiavajú vyhlásenia a záväzky uvedené v dokumentoch priložených k tomuto rozhodnutiu, a to aj pokiaľ ide o podmienky a obmedzenia prístupu orgánov verejnej moci USA k osobným údajom prenášaným v rámci štítu na ochranu osobných údajov medzi EÚ a USA na účely presadzovania práva, národnej bezpečnosti a iné účely verejného záujmu,
- systematickej neschopnosti účinne riešiť sťažnosti dotknutých osôb z EÚ alebo
- že ombudsman pre štít na ochranu osobných údajov systematicky neposkytuje včasné a primerané odpovede na žiadosti dotknutých osôb z EÚ, ako sa vyžaduje v oddiele 4 písm. e) prílohy III.

Komisia predloží tieto návrhy opatrení aj v prípade, že nedostatočná spolupráca s orgánmi USA zabezpečujúcimi fungovanie štítu na ochranu osobných údajov medzi EÚ a USA bráni Komisii v stanovení, či je ovplyvnené zistenie podľa článku 1 ods. 1.

Článok 5

Členské štáty prijímú všetky opatrenia potrebné na dosiahnutie súladu s týmto rozhodnutím.

Článok 6

Toto rozhodnutie je určené členským štátom.

V Bruseli 12. júla 2016

Za Komisiu
Věra JOUROVÁ
členka Komisie

PRÍLOHA 1

List ministerky obchodu USA Penny Pritzkerovej

7. júla 2016

Vážená pani Věra Jourová
Komisárka pre spravodlivosť, spotrebiteľov a rodovú rovnosť
Európska komisia
Rue de la Loi/Weststraat 200
1049 Brusel
Belgicko

Vážená pani komisárka Jourová,

v mene Spojených štátov amerických si Vám dovoľujem zaslať súbor dokumentov týkajúcich sa štítu na ochranu osobných údajov medzi EÚ a USA, ktorý je výsledkom dvoch rokov plodných diskusií medzi našimi tímami. Spolu s ďalšími materiálmi, ktoré má Komisia k dispozícii z verejných zdrojov, predstavuje veľmi dobré východisko pre nové posúdenie primeranosti ochrany zo strany Európskej komisie ⁽¹⁾.

Môžeme byť spoločne pyšní na zlepšenia tohto rámca. Štít na ochranu osobných údajov vychádza zo zásad, ktoré sa tešia silnej konsenzuálnej podpore na oboch brehoch Atlantického oceánu a my sme dosiahli posilnenie ich uplatňovania. Naša spoločná práca nám poskytuje reálnu príležitosť zlepšiť ochranu osobných údajov na celom svete.

Súbor dokumentov týkajúcich sa štítu na ochranu osobných údajov zahŕňa zásady štítu, ako aj list (priložený ako príloha 1) Útvaru pre správu medzinárodného obchodu (ITA) Ministerstva obchodu USA, ktoré je poverené správou a riadením programu. V liste sú opísané záväzky, ktoré naše ministerstvo prijalo s cieľom zabezpečiť účinné fungovanie štítu. Súčasťou súboru dokumentov je aj príloha 2, ktorá obsahuje ďalšie záväzky Ministerstva obchodu USA týkajúce sa nového arbitrážneho modelu, ktorý je k dispozícii v rámci štítu na ochranu osobných údajov.

Vydala som pokyny svojim zamestnancom, aby využili všetky potrebné prostriedky na rýchle a úplné vykonanie rámca štítu na ochranu osobných údajov a zabezpečenie včasného splnenia záväzkov uvedených v prílohe 1 a prílohe 2.

Súbor dokumentov týkajúcich sa štítu na ochranu osobných údajov zahŕňa aj dokumenty ďalších úradov Spojených štátov amerických, konkrétne:

- list Federálnej obchodnej komisie, v ktorom sa opisuje spôsob, akým komisia presadzuje štít na ochranu osobných údajov,
- list Ministerstva dopravy USA, v ktorom sa opisuje spôsob, akým uvedené ministerstvo presadzuje štít na ochranu osobných údajov,
- dva listy, ktoré vypracoval Úrad riaditeľa národnej spravodajskej služby (ODNI), týkajúce sa záruk a obmedzení uplatniteľných na orgány národnej bezpečnosti USA,
- list Ministerstva zahraničných vecí USA a sprievodné memorandum, v ktorých sa opisuje záväzok Ministerstva zahraničných vecí zriadiť novú funkciu ombudsmana pre štít na ochranu osobných údajov, na ktorého sa bude možné obrátiť s otázkami týkajúcimi sa postupov signálového spravodajstva USA a
- list, ktorý vypracovalo Ministerstvo spravodlivosti USA, týkajúci sa záruk a obmedzení prístupu vlády USA na účely presadzovania práva a verejného záujmu.

Ubezpečujeme Vás, že Spojené štáty americké pristupujú k týmto záväzkom so všetkou vážnosťou.

⁽¹⁾ Ak sa rozhodnutie Komisie o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA uplatní aj na Island, Lichtenštajnsko a Nórsko, súbor dokumentov týkajúcich sa štítu na ochranu osobných údajov sa bude vzťahovať na Európsku úniu, aj na uvedené tri krajiny.

Do 30 dní od konečného schválenia určenia primeranosti ochrany bude celý súbor dokumentov týkajúcich sa štítu na ochranu osobných údajov doručený na uverejnenie do *Federálneho registra USA*.

Tešíme sa na budúcu spoluprácu s Vami pri vykonávaní štítu na ochranu osobných údajov a na spoločný začiatok novej etapy tohto procesu.

S úctou
Penny Pritzker

Príloha 1

List úradujúceho tajomníka pre medzinárodný obchod Kena Hyatta

Vážená pani Věra Jourová
Komisárka pre spravodlivosť, spotrebiteľov a rodovú rovnosť
Európska komisia
Rue de la Loi/Weststraat 200
1049 Brusel
Belgicko

Vážená pani komisárka Jourová,

v mene Útvary pre správu medzinárodného obchodu si Vám dovoľujem zaslať opis posilnenej ochrany osobných údajov, ktorú poskytuje rámec štítu na ochranu osobných údajov medzi EÚ a USA („štít na ochranu osobných údajov“ alebo „rámec“), ako aj záväzkov, ktoré prijalo Ministerstvo obchodu USA („ministerstvo“) s cieľom zabezpečiť účinné fungovanie štítu na ochranu osobných údajov. Dokončenie tohto historicky významného procesu znamená dôležitý medzník pre ochranu osobných údajov aj pre podniky na oboch brehoch Atlantického oceánu. Ponúka fyzickým osobám z EÚ záruku ochrany ich údajov a dáva im k dispozícii opravné prostriedky na riešenie prípadných problémov. Je zárukou istoty, ktorá pomôže rastu transatlantického hospodárstva, tým, že zabezpečí, aby tisíce európskych a amerických podnikov mohli naďalej cezhranične investovať a podnikáť v našich dvoch krajinách. Štít na ochranu osobných údajov je výsledkom viac ako dvojročnej náročnej práce a spolupráce s Vami – našimi kolegami v Európskej komisii („Komisia“). Tešíme sa na ďalšiu spoluprácu s Komisiou pri zabezpečení riadneho fungovania štítu.

Spolupracovali sme s Komisiou pri príprave štítu na ochranu osobných údajov s cieľom umožniť organizáciám so sídlom v USA, aby splnili požiadavky na primeranú ochranu osobných údajov vyplývajúce z práva EÚ. Nový rámec bude prínosný pre fyzické osoby i podniky vo viacerých ohľadoch. Po prvé, prináša dôležitý súbor opatrení v oblasti ochrany osobných údajov pre údaje fyzických osôb z EÚ. Vyžaduje sa v ňom, aby zúčastnené organizácie z USA vypracovali vyhovujúce podmienky ochrany súkromia, aby sa verejne zaviazali, že budú dodržiavať zásady štítu na ochranu osobných údajov, čo umožní presadzovať ich záväzok podľa práva USA, aby každoročne opätovne osvedčovali ministerstvu, že dodržiavajú tieto zásady, aby umožnili fyzickým osobám z EÚ bezplatné a nezávislé riešenie sporov a aby podliehali právomoci Federálnej obchodnej komisie, ministerstva dopravy alebo iného orgánu presadzovania práva. Po druhé, štít na ochranu osobných údajov umožní tisícom spoločností v Spojených štátoch amerických a pobočiek európskych spoločností v USA získavať osobné údaje z Európskej únie, čím sa uľahčia toky údajov podporujúce transatlantický obchod. Transatlantický obchodný vzťah je už dnes najväčším obchodným vzťahom na svete, pričom tvorí polovicu celosvetového hospodárskeho výstupu a takmer jeden bilión dolárov v rámci obchodu s tovarom a službami, vďaka čomu existujú milióny pracovných miest na oboch stranách Atlantického oceánu. Podniky, ktoré sú závislé od transatlantických tokov údajov, pochádzajú zo všetkých priemyselných odvetví a zahŕňajú jednak veľké spoločnosti uvedené v zozname 500 najúspešnejších podnikov sveta zostavenom časopisom Fortune a jednak mnoho malých a stredných podnikov. Transatlantické toky údajov umožňujú organizáciám v USA spracúvať údaje potrebné v súvislosti s ponukou tovaru, služieb a pracovných príležitostí fyzickým osobám v Európe. Štít na ochranu osobných údajov podporuje spoločné zásady ochrany osobných údajov, odstraňuje rozdiely medzi našimi právnymi prístupmi a zároveň pomáha pri dosahovaní obchodných a ekonomických cieľov Európy aj USA.

Rozhodnutie spoločnosti o predložení osvedčenia podľa tohto nového rámca síce bude dobrovoľné, ale v okamihu verejného prijatia záväzku dodržiavať zásady štítu na ochranu osobných údajov bude možné presadzovať tento záväzok podľa práva USA, a to zo strany Federálnej obchodnej komisie alebo ministerstva dopravy (podľa toho, ktorý orgán má jurisdikciu v súvislosti s danou organizáciou zapojenou do štítu na ochranu osobných údajov).

Zlepšenia vyplývajúce zo zásad štítu na ochranu osobných údajov

Výsledný štít na ochranu osobných údajov posilňuje ochranu osobných údajov prostredníctvom nasledujúcich opatrení:

- požiadavka na poskytnutie doplňujúcich informácií fyzickým osobám stanovená v rámci zásady oznámenia vrátane vyhlásenia o zapojení organizácie do štítu na ochranu osobných údajov, vyhlásenia o práve fyzickej osoby na prístup k jeho osobným údajom a určenia príslušného nezávislého orgánu na riešenie sporov,
- posilnenie ochrany osobných údajov, ktoré sa prenášajú od organizácie zapojenej do štítu na ochranu osobných údajov prevádzkovateľovi, ktorý je treťou stranou, prostredníctvom požiadavky, aby strany prenosu údajov uzavreli zmluvu, v ktorej stanovujú, že prenášané údaje je možné spracúvať len na obmedzené a presne určené účely v súlade so súhlasom poskytnutým jednotlivcom a že príjemca údajov zabezpečí rovnakú úroveň ochrany osobných údajov, akú si vyžadujú zásady,

- posilnenie ochrany osobných údajov, ktoré sa prenášajú od organizácie zapojenej do štítu na ochranu osobných údajov zástupcovi, ktorý je treťou stranou, vrátane požiadavky, aby organizácia zapojená do štítu na ochranu osobných údajov: prijala primerané a vhodné opatrenia s cieľom zabezpečiť, aby zástupca účinne spracoval osobné údaje prenesené spôsobom, ktorý je v súlade so záväzkami organizácie vyplývajúcimi zo zásad, na základe oznámenia prijala primerané a vhodné opatrenia s cieľom zastaviť a napraviť neoprávnené spracovanie a na požiadanie poskytla ministerstvu zhrnutie alebo reprezentatívnu kópiu príslušných ustanovení o ochrane osobných údajov zo zmluvy s daným zástupcom,
- stanovenie zodpovednosti organizácie zapojenej do štítu na ochranu osobných údajov za spracovanie osobných údajov, ktoré získa v rámci štítu a následne prenesie tretej strane konajúcej v jej mene ako zástupca, ako aj zodpovednosti organizácie zapojenej do štítu na ochranu osobných údajov vyplývajúcej zo zásad za to, že jej zástupca spracúva uvedené osobné údaje spôsobom, ktorý je v rozpore so zásadami, okrem prípadov, keď organizácia preukáže, že nie je zodpovedná za udalosť, ktorá viedla k ujme,
- objasnenie toho, že organizácie zapojené do štítu na ochranu osobných údajov musia obmedziť osobné údaje na tie, ktoré sú relevantné na účely spracovania,
- požiadavka na organizáciu, aby každoročne osvedčovala ministerstvu svoj záväzok uplatňovať zásady na údaje získané v čase, keď bola zapojená do štítu na ochranu osobných údajov, pokiaľ svoje zapojenie do štítu ukončí a vyberie si možnosť, že bude uvedené údaje naďalej uchovávať,
- požiadavka na poskytnutie jednotlivcom bezplatných nezávislých mechanizmov nápravy,
- požiadavka na organizácie a ich vybrané nezávislé mechanizmy nápravy, aby rýchlo reagovali na otázky a žiadosti ministerstva týkajúce sa informácií súvisiacich so štítom na ochranu osobných údajov,
- požiadavka na organizácie, aby urýchlene reagovali na sťažnosti týkajúce sa dodržiavania zásad, postúpené orgánmi členských štátov EÚ prostredníctvom ministerstva a
- požiadavka na organizáciu zapojenú do štítu na ochranu osobných údajov, aby uverejnila všetky relevantné oddiely každej správy o dodržiavaní predpisov alebo hodnotiacej správy predloženej Federálnej obchodnej komisii, ktoré súvisia so štítom na ochranu osobných údajov, pokiaľ bude v súvislosti s danou organizáciou vydaný uznesenie Federálnej obchodnej komisie alebo súdny príkaz týkajúci sa nedodržiavania zásad.

Správa štítu na ochranu osobných údajov a dohľad nad ním zo strany ministerstva obchodu

Ministerstvo znova opakuje svoj záväzok viesť a sprístupniť verejnosti oficiálny zoznam organizácií v USA, ktoré ministerstvu predložili osvedčenie a zaviazali sa dodržiavať zásady („zoznam organizácií zapojených do štítu na ochranu osobných údajov“). Ministerstvo bude aktualizovať zoznam organizácií zapojených do štítu na ochranu osobných údajov a odstraňovať z neho tie organizácie, ktoré dobrovoľne opustia štít, každoročne nepredložia osvedčenie v súlade s postupmi ministerstva alebo v prípade ktorých sa potvrdí, že trvale nedodržiavajú zásady. Ministerstvo tiež povedie a sprístupní verejnosti oficiálny zoznam organizácií v USA, ktoré v minulosti ministerstvu osvedčili svoje dodržiavanie zásad, ale boli vyradené zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov vrátane tých organizácií, ktoré boli zo zoznamu vyradené z dôvodu trvalého nedodržiavania zásad. Ministerstvo uvedie dôvod odstránenia jednotlivých organizácií zo zoznamu.

Ministerstvo sa ďalej zaväzuje, že posilní správu štítu na ochranu osobných údajov a dohľad nad ním. Konkrétne ministerstvo:

Bude poskytovať doplňujúce informácie na webovej lokalite štítu na ochranu osobných údajov

- povedie zoznam organizácií zapojených do štítu na ochranu osobných údajov, ako aj zoznam organizácií, ktoré v minulosti osvedčili svoje dodržiavanie zásad, ale v súčasnosti už nemajú nárok na využívanie výhod vyplývajúcich zo štítu,
- na viditeľnom mieste vysvetlí, že všetky organizácie vyradené zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov stratili nárok na využívanie výhod vyplývajúcich zo štítu, musia však naďalej uplatňovať zásady pri tých osobných údajoch, ktoré získali v období, keď boli do štítu zapojené, a to po celý čas uchovávania týchto informácií a
- uvedie odkaz na zoznam prípadov Federálnej obchodnej komisie, ktoré súvisia so štítom na ochranu osobných údajov, vedený na webovej lokalite Federálnej obchodnej komisie.

Bude overovať požiadavky na osvedčenie samotnou organizáciou

- pred dokončením osvedčovania samotnou organizáciou (alebo každoročného opätovného osvedčovania) a zaradením organizácie do zoznamu organizácií zapojených do štítu na ochranu osobných údajov ministerstvo overí, či organizácia:
 - poskytla požadované kontaktné informácie,
 - opísala svoju činnosť so zreteľom na osobné údaje získavané z EÚ,
 - uviedla, na aké osobné údaje sa vzťahuje jej osvedčenie,
 - ak má vlastnú verejne prístupnú webovú lokalitu, či uviedla adresu webovej lokality, na ktorej sú dostupné podmienky ochrany súkromia, a či sú tieto podmienky dostupné na uvedenej webovej adrese, alebo (pokiaľ organizácia nemá verejnú webovú lokalitu), či uviedla, na akom mieste sú podmienky ochrany súkromia k dispozícii verejnosti,
 - zahrnula do príslušných podmienok ochrany súkromia vyhlásenie, že dodržiava zásady, a, ak sú podmienky ochrany súkromia k dispozícii on-line, či uviedla hypertextový odkaz na webovú lokalitu ministerstva týkajúcu sa štítu na ochranu osobných údajov,
 - určila osobitný orgán zriadený zákonom, ktorý je oprávnený vypočítať prípadné sťažnosti voči danej organizácii týkajúce sa možných nečestných alebo klamlivých praktík a porušenia zákonov alebo právnych predpisov upravujúcich ochranu súkromia (a ktorý je uvedený v zásadách alebo v budúcom dodatku k zásadám),
 - ak si organizácia zvolila možnosť, že splní požiadavky uvedené v písmene a) bode i) a iii) zásady nápravy, presadzovania a zodpovednosti a zaviazala sa spolupracovať s príslušnými orgánmi EÚ na ochranu osobných údajov, či uviedla svoj úmysel spolupracovať s orgánmi na ochranu osobných údajov pri vyšetrowaní a riešení sťažností predložených v rámci štítu na ochranu osobných údajov, a najmä reagovať na ich otázky, pokiaľ dotknuté osoby z EÚ podali svoje sťažnosti priamo príslušným národným orgánom na ochranu osobných údajov,
 - uviedla program v oblasti ochrany osobných údajov, ktorého je členom,
 - uviedla spôsob overenia súladu so zásadami (napr. interne, treťou stranou),
 - uviedla (v rámci osvedčovania samotnou organizáciou a vo svojich podmienkach ochrany súkromia) nezávislý mechanizmus nápravy, ktorý je k dispozícii na vyšetrowanie a riešenie sťažností,
 - zahrnula do svojich príslušných podmienok ochrany súkromia (ak sú tieto podmienky k dispozícii on-line) hypertextový odkaz na webovú lokalitu alebo formulár na predkladanie sťažností v rámci nezávislého mechanizmu nápravy, ktorý je k dispozícii na vyšetrowanie nevybavených sťažností a
 - ak organizácia uviedla, že má v úmysle prijímať informácie o ľudských zdrojoch prenesené z EÚ na použitie v rámci pracovnoprávného pomeru, či vyjadrila svoj záväzok spolupracovať s orgánmi na ochranu osobných údajov a plniť ich požiadavky pri riešení sťažností na jej činnosť súvisiacu s uvedenými údajmi, či poskytla ministerstvu kópiu svojich podmienok ochrany súkromia v oblasti ľudských zdrojov a či uviedla, kde sú podmienky ochrany súkromia k dispozícii na nahliadnutie pre dotknutých zamestnancov,
- spolupracovať s nezávislými mechanizmami nápravy s cieľom overiť, či sa organizácia skutočne zaregistrovala v príslušnom mechanizme uvedenom pri osvedčovaní, ak sa takáto registrácia vyžaduje.

Zvýši úsilie pri kontrole organizácií, ktoré boli odstránené zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov

- oznamovať organizáciám, ktoré boli vyradené zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov z dôvodu „trvalého nedodržiavania zásad“, že nie sú oprávnené uchovávať informácie zozbierané v rámci štítu na ochranu osobných údajov a
- zasielať dotazníky organizáciám, ktoré nepredložili osvedčenie o svojom dodržiavaní zásad alebo ktoré dobrovoľne opustili štít na ochranu osobných údajov s cieľom overiť, či osobné údaje, ktoré získali v čase svojho zapojenia do štítu na ochranu osobných údajov, vrátia, odstránia alebo na ne budú naďalej uplatňovať zásady, a pokiaľ budú osobné údaje uchovávať, overovať, či bola určená osoba, ktorá bude v rámci organizácie trvale fungovať ako kontaktná osoba pre otázky súvisiace so štítom na ochranu osobných údajov.

Bude vyhľadávať nepravdivé tvrdenia o zapojení do štítu a ich riešenie

- skúmať podmienky ochrany súkromia organizácií, ktoré sa v minulosti zapojili do štítu na ochranu osobných údajov, ale boli vyradené zo zoznamu organizácií zapojených do štítu s cieľom vyhľadať všetky nepravdivé tvrdenia o zapojení do štítu,
- priebežne, keď organizácia: a) opustí štít, b) nepredloží opätovné osvedčenie o svojom dodržiavaní zásad alebo c) je vyradená zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov z dôvodu „trvalého nedodržiavania zásad“, overovať *ex officio*, či organizácia odstránila zo všetkých relevantných uverejnených podmienok ochrany súkromia všetky odkazy na štít na ochranu osobných údajov, z ktorých by vyplývalo, že sa naďalej aktívne zapája do štítu a má nárok na využívanie výhod, ktoré z neho vyplývajú. Keď ministerstvo zistí, že takéto odkazy neboli odstránené, upozorní organizáciu, že danú vec prípadne postúpi príslušnému úradu na účely presadenia práva, pokiaľ organizácia bude naďalej tvrdiť, že má osvedčenie v rámci štítu na ochranu osobných údajov. Ak organizácia neodstráni odkaz, ani nepredloží osvedčenie o svojom dodržiavaní zásad štítu na ochranu osobných údajov, ministerstvo postúpi danú vec *ex officio* Federálnej obchodnej komisii, ministerstvu dopravy alebo inému príslušnému orgánu presadzovania práva, resp. vo vhodných prípadoch prijme opatrenia na presadenie práva v súvislosti s certifikačnou značkou štítu na ochranu osobných údajov,
- prijme ďalšie opatrenia na odhalenie nepravdivých tvrdení o zapojení do štítu na ochranu osobných údajov a nevhodného používania certifikačnej značky štítu okrem iného prostredníctvom internetového vyhľadávania s cieľom zistiť, kde sa zobrazujú certifikačné značky štítu na ochranu osobných údajov a odkazy na štít v podmienkach ochrany súkromia jednotlivých organizácií,
- rýchle reagovať na všetky problémy, ktoré zistí v priebehu *ex officio* monitorovania nepravdivých tvrdení o zapojení do štítu na ochranu osobných údajov a zneužívania certifikačnej značky vrátane varovania organizácií, ktoré nepravdivo vyhlasujú, že sú zapojené do štítu vyššie opísaným spôsobom,
- prijímať ďalšie primerané nápravné opatrenia vrátane uplatnenia právnej nápravy, ktorú je ministerstvo oprávnené uplatniť, a postúpenia vecí Federálnej obchodnej komisii, ministerstvu dopravy alebo inému príslušnému orgánu presadzovania práva a
- urýchlene preskúmať a riešiť sťažnosti na nepravdivé tvrdenia o zapojení do štítu, ktoré ministerstvo dostane.

Ministerstvo bude skúmať podmienky ochrany súkromia organizácií s cieľom účinnejšie zisťovať a riešiť nepravdivé tvrdenia o zapojení do štítu na ochranu osobných údajov. Zameria sa predovšetkým na podmienky ochrany súkromia tých organizácií, platnosť osvedčenia ktorých uplynula, pretože opätovne neosvedčili svoje dodržiavanie zásad. Ministerstvo bude vykonávať uvedené preskúmania s cieľom overiť, či tieto organizácie odstránili zo všetkých relevantných uverejnených podmienok ochrany súkromia všetky odkazy, z ktorých by vyplývalo, že sa naďalej aktívne zapájajú do štítu na ochranu osobných údajov. Výsledkom tohto druhu preskúmaní bude určenie organizácií, ktoré neodstránili odkazy na štít a ich upozornenie formou listu kancelárie vedúceho právneho odboru ministerstva s varovaním pred možnými opatreniami v rámci presadzovania práva, pokiaľ odkazy nebudú odstránené. Ministerstvo prijme nadväzujúce opatrenia s cieľom zabezpečiť, aby tieto organizácie buď odstránili nevhodné odkazy, alebo opakovane osvedčili svoje dodržiavanie zásad. Ministerstvo sa okrem toho zameria na zisťovanie nepravdivých tvrdení o zapojení do štítu na ochranu osobných údajov zo strany organizácií, ktoré do štítu nikdy neboli zapojené a prijme voči týmto organizáciám podobné nápravné opatrenia.

Bude vykonávať pravidelné *ex officio* preskúmania súladu a hodnotenia programu

- priebežne monitorovať účinné dodržiavanie zásad okrem iného prostredníctvom zasielania podrobných dotazníkov zapojeným organizáciám s cieľom určiť problémy, ktoré by si mohli vyžiadať následné nadväzujúce opatrenia. Takéto preskúmania súladu sa uskutočnia predovšetkým vtedy, keď: a) ministerstvo dostane konkrétne opodstatnené sťažnosti na dodržiavanie zásad zo strany organizácie; b) organizácia neodpovie uspokojivo na žiadosti ministerstva o informácie súvisiace so štítom na ochranu osobných údajov alebo c) existuje spoľahlivý dôkaz, že organizácia neplní svoje záväzky, ktoré prijala v rámci štítu na ochranu osobných údajov. Ministerstvo podľa potreby konzultuje preskúmania súladu s príslušnými orgánmi na ochranu osobných údajov a
- pravidelne hodnotí správu programu štítu na ochranu osobných údajov a dohľad nad ním s cieľom zabezpečiť primeranosť monitorovania v záujme riešenia nových problémov bezprostredne po ich vzniku.

Ministerstvo rozšírilo zdroje, ktoré sa budú venovať správe štítu na ochranu osobných údajov a dohľadu nad ním vrátane zdvojnásobenia počtu zamestnancov zodpovedných za správu programu a dohľad nad ním. Naďalej budeme vynakladať primerané prostriedky na snahy o zabezpečenie účinného monitorovania a správy programu.

Prispôsobí webovú lokalitu štítu na ochranu osobných údajov konkrétnym adresátom

Ministerstvo prispôsobí webovú lokalitu štítu na ochranu osobných údajov so zreteľom na tri skupiny adresátov: fyzické osoby z EÚ, podniky z EÚ a podniky z USA. Zahŕnutie obsahu zameraného priamo na fyzické osoby a podniky z EÚ v mnohých smeroch uľahčí dosiahnutie transparentnosti. Pokiaľ ide o fyzické osoby z EÚ, na webovej lokalite budú zreteľne vysvetlené: 1. práva, ktoré štít na ochranu osobných údajov poskytuje fyzickým osobám z EÚ, 2. mechanizmy nápravy dostupné fyzickým osobám z EÚ v prípade, že sú presvedčení o porušení záväzku organizácie, že bude dodržiavať zásady a 3. spôsoby vyhľadávania informácií týkajúcich sa osvedčovania samotnou organizáciou organizácie v rámci programu štítu na ochranu osobných údajov. Pokiaľ ide o podniky z EÚ, webová lokalita uľahčí overenie nasledujúcich skutočností: 1. či organizácia má nárok na využívanie výhod vyplývajúcich zo štítu na ochranu osobných údajov; 2. druh informácií, na ktoré sa vzťahuje osvedčenie organizácie v rámci štítu na ochranu osobných údajov; 3. podmienky ochrany súkromia, ktoré sa uplatňujú na zahrnuté informácie a 4. spôsob, ktorý organizácia používa na overenie dodržiavania zásad.

Zintenzívni spoluprácu s orgánmi pre ochranu osobných údajov

Ministerstvo v záujme zintenzívnenia spolupráce s orgánmi na ochranu osobných údajov určí kontaktnú osobu, ktorá bude pôsobiť ako prostredník vo vzťahoch s orgánmi na ochranu osobných údajov. Ak je orgán na ochranu osobných údajov presvedčený o tom, že organizácia nedodržiava zásady okrem iného aj na základe sťažnosti podanej fyzickou osobou z EÚ, môže sa obrátiť na poverenú kontaktnú osobu ministerstva a požiadať o ďalšiu kontrolu danej organizácie. Kontaktná osoba bude tiež prijímať podnety týkajúce sa organizácií, ktoré nepravdivo tvrdia, že sú zapojené do štítu na ochranu osobných údajov, hoci nikdy neosvedčili svoje dodržiavanie zásad. Kontaktná osoba bude pomáhať orgánom na ochranu osobných údajov pri vyhľadávaní informácií súvisiacich s osvedčovaním samotnou organizáciou konkrétnej organizácie alebo jej zapojením do programu v minulosti a bude odpovedať na žiadosti orgánov na ochranu osobných údajov týkajúce sa dodržiavania osobitných požiadaviek štítu na ochranu osobných údajov. Po druhé, ministerstvo poskytne orgánom na ochranu osobných údajov materiál týkajúci sa štítu na ochranu osobných údajov, aby ho začlenili do svojich vlastných webových lokalít v záujme zvýšenia transparentnosti pre fyzické osoby a podniky z EÚ. Lepšia informovanosť o štíte na ochranu osobných údajov a právach a povinnostiach, ktoré z neho vyplývajú, by mala uľahčiť zisťovanie problémov bezprostredne po ich vzniku a pomôcť pri ich následnom primeranom riešení.

Uľahčí riešenie sťažností týkajúcich sa nedodržiavania zásad

Ministerstvo bude prostredníctvom poverenej kontaktnej osoby prijímať sťažnosti týkajúce sa nedodržiavania zásad organizáciou zapojenou do štítu na ochranu osobných údajov, ktoré mu postúpi orgán na ochranu osobných údajov. Ministerstvo vynaloží maximálne úsilie na uľahčenie riešenia sťažnosti s organizáciou zapojenou do štítu. Do 90 dní od doručenia sťažnosti poskytne orgánu pre ochranu osobných údajov aktuálne informácie. S cieľom uľahčiť podávanie sťažností ministerstvo pripraví štandardný formulár, ktorý budú orgány na ochranu osobných údajov posielat poverenej kontaktnej osobe na ministerstve. Poverená kontaktná osoba bude sledovať všetky podnety od orgánov na ochranu osobných údajov doručené na ministerstvo a v rámci ročného preskúmania opísaného nižšie vypracuje správu, v ktorej súhrnne zanalyzuje sťažnosti doručené za celý rok.

Bude prijímať arbitrážne postupy a vyberať rozhodcov po porade s Komisiou

Ministerstvo splní svoje záväzky vyplývajúce z prílohy I a uverejní postupy po dosiahnutí dohody.

Mechanizmus spoločného preskúmania fungovania štítu na ochranu osobných údajov

Ministerstvo obchodu, Federálna obchodná komisia a ďalšie príslušné úrady sa budú každoročne stretávať so zástupcami Komisie, zainteresovanými orgánmi na ochranu osobných údajov a príslušnými zástupcami pracovnej skupiny zriadenej podľa článku 29 a na týchto stretnutiach poskytne aktuálne informácie o štíte na ochranu osobných údajov. Súčasťou každoročných stretnutí bude diskusia o aktuálnych problémoch súvisiacich s fungovaním, vykonávaním a presadzovaním štítu na ochranu osobných údajov, ako aj s dohľadom nad ním vrátane podnetov, ktoré ministerstvo dostane od orgánov na ochranu osobných údajov, výsledkov *ex officio* preskúmaní dodržiavania predpisov a prípadných diskusií o príslušných zmenách právnych predpisov. Prvé ročné preskúmanie a podľa potreby následné preskúmania budú zahŕňať aj dialóg o ďalších témach, ako je napríklad automatizované prijímanie rozhodnutí, vrátane aspektov týkajúcich sa podobností a rozdielov v prístupoch EÚ a USA.

Aktualizácia právnych predpisov

Ministerstvo vynaloží primerané úsilie na informovanie Komisie o vecných zmenách v práve USA, ktoré sú relevantné z hľadiska štítu na ochranu osobných údajov v oblasti ochrany osobných údajov a obmedzení a zabezpečení vzťahujúcich sa na prístup k osobným údajom zo strany orgánov USA a na ich následné použitie.

Výnimka týkajúca sa národnej bezpečnosti

Pokiaľ ide o obmedzenia pri dodržiavaní zásad štítu na ochranu osobných údajov súvisiace s národnou bezpečnosťou, generálny právny zástupca Úradu riaditeľa národnej spravodajskej služby Robert Litt zaslal dva listy adresované Justinovi Antonipillaiovi a Tedovi Deanovi z ministerstva obchodu, ktoré sme Vám postúpili. V týchto listoch sa obšírne píše okrem iného o politikách, zárukách a obmedzeniach vzťahujúcich sa na činnosti signálového spravodajstva uskutočňované USA. V uvedených listoch sa ďalej opisuje transparentnosť spravodajských služieb v tejto oblasti. Informácie uvedené v listoch ubezpečujú Komisiu posudzujúcu rámec štítu na ochranu osobných údajov o tom, že program bude riadne fungovať v súlade so stanovenými zásadami. Chápeme, že informácie zverejnené spravodajskými službami v budúcnosti možno spolu s ďalšími informáciami použijete ako podklad pre každoročné preskúmanie rámca štítu na ochranu osobných údajov.

Na základe zásad do štítu na ochranu osobných údajov a sprievodných listov a materiálov, vrátane záväzkov ministerstva týkajúcich sa správy a dohľadu nad rámcom štítu na ochranu osobných údajov, predpokladáme, že Komisia dospeje k záveru, že rámec štítu na ochranu osobných údajov medzi EÚ a USA zaručuje primeranú ochranu na účely práva EÚ a že budú pokračovať prenosy údajov z Európskej únie organizáciám, ktoré sú zapojené do štítu.

S úctou

Ken Hyatt

Príloha 2

Arbitrážny model

PRÍLOHA I

V tejto prílohe I sú uvedené podmienky, podľa ktorých sú organizácie zapojené do štítu na ochranu osobných údajov povinné rozhodovať o nárokoch podľa zásady nápravy, presadzovania práva a zodpovednosti. Možnosť záväzného rozhodcovského konania opísaná nižšie sa vzťahuje na určité „zostatkové“ pohľadávky týkajúce sa údajov v rámci štítu na ochranu osobných údajov medzi EÚ a USA. Zmyslom tejto možnosti je zabezpečiť rýchly, nezávislý a spravodlivý mechanizmus, podľa rozhodnutia jednotlivca, na riešenie údajných porušení zásad, ktoré neboli vyriešené prostredníctvom žiadnych iných mechanizmov štítu na ochranu osobných údajov.

A. Rozsah

Táto možnosť rozhodcovského konania je k dispozícii pre jednotlivcov na určenie, či organizácia zapojená do štítu na ochranu osobných údajov v prípade zostatkových pohľadávok porušila svoje záväzky voči jednotlivcovi v súvislosti so zásadami a či takéto porušenie ostalo úplne alebo čiastočne nenapravené. Táto možnosť je dostupná len na tieto účely. Táto možnosť nie je k dispozícii napríklad v prípade výnimiek zo zásad ⁽¹⁾ alebo v prípade tvrdení o neprimeranosti štítu na ochranu osobných údajov.

B. Dostupné prostriedky nápravy

Podľa tejto možnosti rozhodcovského konania má výbor pre štít na ochranu osobných údajov (zložený z jedného alebo troch rozhodcov, podľa dohody strán) právomoc nariadiť konkrétnu, nepeňažnú spravodlivú náhradu (ako napríklad prístup, opravu, vymazanie alebo vrátenie predmetných údajov jednotlivca) potrebnú pre nápravu porušenia zásad, ktorá sa týka výhradne jednotlivca. Toto sú jediné právomoci arbitrážneho výboru týkajúce sa nápravných prostriedkov. Pri zvažovaní prostriedkov nápravy musí arbitrážny výbor zohľadniť iné prostriedky nápravy, ktoré už boli uložené inými mechanizmami v rámci štítu na ochranu osobných údajov. Nie sú k dispozícii žiadne náhrady škody, nákladov, poplatkov alebo iné prostriedky nápravy. Každá strana znáša svoje vlastné náklady na právneho zástupcu.

C. Predarbitrážne požiadavky

Jednotlivec, ktorý sa rozhodne uplatniť možnosť rozhodcovského konania, musí pred začiatkom arbitrážneho nároku vykonať tieto kroky: 1. predložiť údajné porušenie zásad priamo organizácii a poskytnúť jej možnosť vyriešiť problém v lehote stanovenej v oddiele III.11 písm. d) bode i) zásad; 2. využiť nezávislý mechanizmus nápravy podľa zásad, ktorý je jednotlivcovi bezplatne k dispozícii a 3. predložiť tento problém svojmu orgánu na ochranu údajov, ktorý ho postúpi ministerstvu obchodu, a poskytnúť ministerstvu obchodu príležitosť vynaložiť maximálne úsilie na vyriešenie problému v časovom rámci stanovenom v liste správy zahraničného obchodu z ministerstva obchodu, a to bez akýchkoľvek nákladov pre jednotlivca.

Táto možnosť rozhodcovského konania sa nesmie uplatniť, ak to isté údajné porušenie zásad 1. bolo už predtým predmetom záväzného rozhodcovského konania; 2. bolo predmetom právoplatného rozsudku vyneseného v súdnom konaní, v ktorom bol jednotlivec jednou zo strán, alebo 3. bolo predtým vysporiadané oboma stranami. Táto možnosť sa okrem toho nemôže uplatniť, ak orgán EÚ na ochranu údajov 1. má právomoc podľa oddielov III.5 alebo III.9 zásad alebo 2. má právomoc vyriešiť údajné porušenie priamo s organizáciou. Právomoc DPA na riešenie rovnakého nároku voči prevádzkovateľovi v EÚ nebráni uplatneniu tejto možnosti rozhodcovského konania voči odlišnej právnickej osobe, ktorá nie je viazaná právomocou DPA.

D. Záväzný charakter rozhodnutí

Rozhodnutie jednotlivca uplatniť túto možnosť záväzného rozhodcovského konania je úplne dobrovoľné. Arbitrážne rozhodnutia budú záväzné pre všetky strany rozhodcovského konania. Keď sa raz uplatní, jednotlivec sa vzdáva možnosti požadovať náhradu za to isté údajné porušenie v inom fóre, s výnimkou prípadu, že ak nepeňažná spravodlivá náhrada nie je úplne uspokojivým nápravným prostriedkom pre takéto porušenie, uplatnenie rozhodcovského konania zo strany jednotlivca nebude brániť nároku na náhradu škody, ktorý je inak dostupný na súdoch.

⁽¹⁾ Oddiel I.5 zásad.

E. Preskúmanie a výkon

Jednotlivci a organizácie zapojené do štítu na ochranu osobných údajov budú môcť požiadať o súdne preskúmanie a výkon arbitrážnych rozsudkov podľa práva USA v rámci zákona o federálnej arbitráži ⁽¹⁾. Akékoľvek takéto prípady sa musia predložiť na federálny okresný súd, ktorého územné pokrytie zahŕňa hlavné miesto podnikania organizácie zapojenej do štítu na ochranu osobných údajov.

Účelom tejto možnosti rozhodcovského konania je riešiť individuálne spory a arbitrážne rozhodnutia nemajú plniť funkciu presvedčivého alebo záväzného precedensu vo veciach týkajúcich sa ostatných strán vrátane budúcich rozhodcovských konaní na súdoch EÚ alebo USA alebo konaní Federálnej obchodnej komisie.

F. Arbitrážny výbor

Strany si zvolia rozhodcov z príslušného zoznamu opísaného nižšie.

Ministerstvo obchodu USA a Európska komisia v súlade s platnými právnymi predpismi vypracujú zoznam aspoň 20 rozhodcov na základe nezávislosti, integrity a odborných znalostí. V súvislosti s týmto postupom sa uplatňujú tieto pravidlá:

Rozhodcovia:

1. zostanú uvedení na zozname počas obdobia 3 rokov, ak nenastanú výnimočné okolnosti alebo príčiny, s možnosťou predĺženia o ďalšie 3 roky;
2. nebudú sa riadiť žiadnymi pokynmi ani nebudú spojení so žiadnou stranou alebo organizáciou zapojenou do štítu na ochranu osobných údajov, ani USA, EÚ alebo ktorýmkoľvek členským štátom EÚ, ani so žiadnym iným vládny orgánom, orgánom verejnej moci alebo orgánom na presadzovanie práva a
3. musia byť oprávnení vykonávať advokátsku prax v USA a byť odborníkmi v oblasti práva USA na ochranu súkromia s odbornými znalosťami zákonov EÚ z oblasti ochrany údajov.

G. Rozhodcovské konania

Ministerstvo obchodu a Európska komisia sa v súlade s platnými právnymi predpismi do 6 mesiacov od prijatia rozhodnutia o primeranosti dohodnú o prijatí existujúceho zaužívaného súboru rozhodcovských konaní USA (ako napríklad AAA alebo JAMS) s cieľom riadiť konania pred výborom pre štít na ochranu osobných údajov, na základe týchto podmienok:

1. Jednotlivec môže začať záväzné rozhodcovské konanie za predpokladu, že sú splnené predarbitrážne podmienky uvedené vyššie, dorúčením „oznámenia“ organizácii. Toto oznámenie musí obsahovať zhrnutie krokov, ktoré boli prijaté podľa časti C s cieľom vyriešiť nárok, opis údajného porušenia a na základe rozhodnutia jednotlivca aj akékoľvek podkladové dokumenty a materiály a/alebo diskusiu o právnych predpisoch týkajúcich sa údajného nároku.

⁽¹⁾ V kapitole 2 zákona o federálnej arbitráži (ďalej len „FAA“) sa stanovuje, že „rozhodcovská dohoda alebo rozhodcovské rozhodnutie, ktoré vyplývajú z právneho vzťahu, či už zmluvného alebo nie, ktorý sa považuje za obchodnú zmluvu, vrátane transakcie, alebo dohodu opísanú v [oddiele 2 zákona FAA], patrí do rozsahu pôsobnosti dohovoru [o uznaní a výkone cudzích rozhodcovských rozhodnutí z 10. júna 1958, 21 U.S.T. 2519, T.I.A.S. č. 6997 (ďalej len „Newyorský dohovor“)]“ (9 U.S.C. § 202). V zákone FAA sa ďalej stanovuje, že „dohoda alebo rozhodnutie, ktoré vyplýva z takéhoto vzťahu, ktorý je výlučne medzi občanmi Spojených štátov, sa považuje za nepatriacu do rozsahu pôsobnosti [Newyorského] dohovoru, pokiaľ takýto vzťah nezahŕňa majetok nachádzajúci sa v zahraničí, neplánuje sa výkon alebo presadzovanie práva v zahraničí alebo nemá žiadny iný primeraný vzťah s jedným alebo viacerými cudzími štátmi“ (tamtiež). Podľa kapitoly 2, „ktorákoľvek strana rozhodcovského konania môže podať návrh na ktorýkoľvek súd, ktorý má podľa tejto kapitoly jurisdikciu, na príkaz potvrdzujúci rozhodnutie voči ktorejkoľvek inej strane rozhodcovského konania. Súd potvrdí rozhodnutie, pokiaľ nezistí jediný dôvod odmietnutia alebo odkladu uznania či výkonu rozhodnutia uvedeného v spomínanom [Newyorskom] dohovore“ (tamtiež, § 207). V kapitole 2 sa ďalej stanovuje, že „okresné súdy Spojených štátov... majú pôvodnú jurisdikciu rozhodovať o... žalobe alebo konaní [podľa Newyorského dohovoru], a to bez ohľadu na spornú časť“ (tamtiež, § 203).

V kapitole 2 sa tiež stanovuje, že „kapitola 1 sa vzťahuje na žaloby a konania zahrnuté v tejto kapitole, pokiaľ daná kapitola nie je v rozpore s touto kapitolou alebo [Newyorským] dohovorom ratifikovaným Spojenými štátmi“ (tamtiež, § 208). V kapitole 1 sa stanovuje, že „písomné ustanovenie v... zmluve, ktoré potvrdzuje obchodnú transakciu na urovanie sporu vyplývajúceho z takejto zmluvy alebo transakcie prostredníctvom rozhodcovského konania, alebo odmietnutie vykonať celú alebo ktorúkoľvek časť z neho, alebo písomnej dohody na predloženie existujúceho sporu vyplývajúceho z takejto zmluvy, transakcie alebo odmietnutia rozhodcovského konania, je platné, neodvolateľné a vymáhateľné s výnimkou prípadov existujúcich podľa zákona a vlastného kapitálu pre zrušenie akejkoľvek zmluvy“ (tamtiež, § 2). V kapitole 1 sa ďalej stanovuje, že „ktorákoľvek strana rozhodcovského konania sa môže obrátiť na určený súd v súvislosti s príkazom na potvrdenie rozhodnutia, následkom čoho súd udeliť takýto príkaz, pokiaľ sa rozhodnutie nezruší, nezmení alebo neopraví, ako sa to stanovuje v oddieloch 10 a 11 [zákona FAA]“ (tamtiež, § 9).

2. Vypracujú sa postupy, aby sa zaistilo, že to isté údajné porušenie jednotlivca nebude spojené s duplicitnými prostriedkami nápravy alebo konaniami.
3. Súbežne s rozhodcovským konaním môže prebiehať činnosť Federálnej obchodnej komisie.
4. Na týchto rozhodcovských konaniach sa nesmie zúčastniť žiadny zástupca USA, EÚ alebo ktoréhokoľvek členského štátu EÚ alebo iného vládneho orgánu, orgánu verejnej moci alebo orgánu na presadzovanie práva, pričom DPA v EÚ môžu na žiadosť jednotlivca z EÚ poskytovať pomoc jedine v rámci vypracovania oznámenia, ale DPA v EÚ nesmú mať prístup k zisteniam alebo akýmkoľvek iným materiálom týkajúcim sa týchto rozhodcovských konaní.
5. Rozhodcovské konanie prebieha v Spojených štátoch a jednotlivec si môže vybrať spôsob účasti prostredníctvom videokonferencie alebo telefónu, ktoré sa jednotlivcovi poskytnú bezplatne. Nebude sa vyžadovať osobná účasť.
6. Jazykom rozhodcovského konania bude angličtina, pokiaľ sa strany nedohodnú inak. Na základe odôvodnenej žiadosti a pri zohľadnení skutočností, či jednotlivca zastupuje advokát, sa jednotlivcovi na arbitrážnom vypočutí bezplatne poskytnú tlmočnické služby, ako aj preklad arbitrážnych materiálov, pokiaľ výbor nezistí, že za okolností špecifického rozhodcovského konania by to viedlo k neprimeraným alebo neúmerným nákladom.
7. S materiálmi, ktoré sa predložili rozhodcom, sa bude zaobchádzať dôverne a budú sa používať jedine v súvislosti s rozhodcovským konaním.
8. V prípade potreby sa môže povoliť individuálne sprístupnenie zistení, s ktorými budú strany zaobchádzať dôverne a ktoré sa budú používať jedine v súvislosti s rozhodcovským konaním.
9. Rozhodcovské konanie sa ukončí do 90 dní od doručenia oznámenia samotnej organizácii, pokiaľ sa strany nedohodnú inak.

H. Náklady

Rozhodcovia by mali vykonať primerané kroky s cieľom minimalizovať náklady alebo poplatky za rozhodcovské konania.

Ministerstvo obchodu na základe platných právnych predpisov uľahčí po konzultácii s Európskou komisiou zriadenie fondu, do ktorého budú musieť organizácie zapojené do štítu na ochranu osobných údajov odvádzať ročné príspevky, ktoré budú sčasti založené na veľkosti organizácie a ktoré pokryjú náklady rozhodcovského konania, vrátane poplatkov za rozhodcu, až do maximálnych súm („stropov“). Fond bude spravovať tretia strana, ktorá bude pravidelne podávať správy o operáciách fondu. Ministerstvo obchodu a Európska komisia budú v rámci ročného preskúmania hodnotiť činnosť fondu, ako aj potrebu prispôsobiť sumu príspevkov alebo stropov, a okrem iného zväžia počet, náklady a načasovanie rozhodcovských konaní, pričom vzájomne chápu, že organizácie zapojené do štítu na ochranu osobných údajov sa nebudú neprimerane finančne zaťažovať. Náklady na právneho zástupcu nie sú pokryté v tomto ustanovení ani v rámci žiadneho fondu podľa tohto ustanovenia.

PRÍLOHA II

**ZÁSADY RÁMCA ŠTÍTU NA OCHRANU OSOBNÝCH ÚDAJOV MEDZI EÚ A USA VYDANÉ
MINISTERSTVOM OBCHODU USA**

I. PREHEAD

1. Napriek tomu, že Spojené štáty a Európska únia sledujú rovnaký cieľ zvyšovania ochrany súkromia, Spojené štáty majú odlišný prístup k ochrane súkromia než Európska únia. Spojené štáty uplatňujú odvetvový prístup založený na kombinácii právnych predpisov, regulácie a samoregulácie. Vzhľadom na tieto rozdiely a s cieľom poskytnúť organizáciám v Spojených štátoch spoľahlivý mechanizmus prenosu osobných údajov z Európskej únie do Spojených štátov a zároveň zabezpečiť, aby dotknuté osoby z EÚ mohli naďalej využívať účinné záruky a ochranu, ako to vyžadujú európske právne predpisy vzhľadom na spracovanie ich osobných údajov, ktoré boli prenesené do krajín mimo EÚ, ministerstvo obchodu vydalo z titulu svojej zákonnej právomoci posilňovať, podporovať a rozvíjať medzinárodný obchod (15 U.S.C. § 1512) tieto zásady štítu na ochranu osobných údajov vrátane doplnkových zásad (ďalej spoločne len „zásady“). Tieto zásady boli vypracované na základe konzultácií s Európskou komisiou, predstaviteľmi priemyslu a inými zainteresovanými stranami v záujme uľahčenia obchodu medzi Spojenými štátmi a Európskou úniou. Sú určené výlučne pre organizácie v USA, ktoré získavajú osobné údaje z Európskej únie, aby mohli splniť požiadavky štítu na ochranu osobných údajov a získať tak prospech z rozhodnutia Európskej komisie o primeranosti⁽¹⁾. Tieto zásady nemajú vplyv na uplatňovanie vnútroštátnych ustanovení, ktorými sa vykonáva smernica 95/46/ES (ďalej len „smernica“) a ktoré sa vzťahujú na spracúvanie osobných údajov v členských štátoch. Týmto zásadami sa tiež neobmedzujú povinnosti týkajúce sa ochrany súkromia, ktoré sa inak uplatňujú podľa práva Spojených štátov.
2. Aby sa organizácia mohla na účely prenosov osobných údajov z EÚ opierať o štít na ochranu osobných údajov, musí ministerstvu obchodu (alebo jeho zástupcovi) (ďalej len „ministerstvo“) osvedčiť svoje dodržiavanie zásad. Hoci sú rozhodnutia organizácií o zapojení do štítu na ochranu osobných údajov úplne dobrovoľné, účinné dodržiavanie jeho zásad je povinné: organizácie, ktoré poskytnú ministerstvu osvedčenie o svojom dodržiavaní zásad a verejne vyhlásia svoj záväzok dodržiavať zásady, musia postupovať v úplnom súlade s týmito zásadami. Ak sa organizácia chce zapojiť do štítu na ochranu osobných údajov, musí a) podliehať vyšetrovacím právomociam a právomociam presadzovania práva Federálnej obchodnej komisie (ďalej len „FTC“), ministerstva alebo iného zákonom zriadeného orgánu, čo účinne zabezpečí dodržiavanie zásad (v budúcnosti možno zákonom zriadené orgány Spojených štátov uznané EÚ uviesť v prílohe); b) verejne vyhlásiť, že sa zaväzuje dodržiavať zásady; c) zverejniť svoje podmienky ochrany súkromia v súlade s týmito zásadami a d) v plnej miere ich vykonávať. Nedodržiavanie zásad zo strany organizácie je postihnutelné podľa oddielu 5 zákona o Federálnej obchodnej komisii, ktorý zakazuje nekalé a klamlivé konanie v rámci obchodu alebo s vplyvom na obchod [15 U.S.C. § 45 a)], alebo podľa iných právnych predpisov a nariadení, ktorými sa zakazuje takéto konanie.
3. Ministerstvo obchodu bude viesť a sprístupní verejnosti oficiálny zoznam organizácií v USA, ktoré osvedčili ministerstvu svoje dodržiavanie zásad a vyhlásili svoj záväzok dodržiavať zásady („zoznam organizácií zapojených do štítu na ochranu osobných údajov“). Výhody vyplývajúce zo štítu na ochranu osobných údajov sú zabezpečené od dátumu, keď ministerstvo pridá organizáciu do zoznamu organizácií zapojených do štítu na ochranu osobných údajov. Ministerstvo vyradí organizáciu zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov, ak organizácia dobrovoľne opustí štít na ochranu osobných údajov alebo ak nedokončí svoje každoročné opätovné osvedčovanie ministerstvu. Vyradenie organizácie zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov znamená, že organizácia už nemôže mať prospech z rozhodnutia Európskej komisie o primeranosti a nemôže získavať osobné informácie z EÚ. Organizácia musí naďalej uplatňovať zásady vo vzťahu k osobným informáciám, ktoré získala počas účasti v štíte na ochranu osobných údajov, a potvrdiť ministerstvu každý rok svoj záväzok pokračovať v tomto konaní dovtedy, kým bude uchovávať takéto informácie; inak musí organizácia tieto informácie vrátiť alebo vymazať alebo zabezpečiť ich „primeranú“ ochranu iným povoleným spôsobom. Ministerstvo vyradí zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov také organizácie, ktoré trvale nedodržiavali zásady; takéto organizácie nesplňajú podmienky na využívanie výhod vyplývajúcich zo štítu na ochranu osobných údajov a musia vrátiť alebo vymazať osobné informácie, ktoré získali v rámci štítu na ochranu osobných údajov.
4. Ministerstvo bude takisto viesť a sprístupňovať verejnosti oficiálny zoznam organizácií Spojených štátov, ktoré predtým ministerstvu osvedčili svoje dodržiavanie zásad, ale boli vyradené zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov. Ministerstvo poskytne jasné varovanie, že tieto organizácie nie sú zapojené do štítu na ochranu osobných údajov; že vyradenie zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov znamená, že takéto organizácie nemôžu tvrdiť, že dodržiavajú zásady štítu na ochranu osobných

⁽¹⁾ Ak sa rozhodnutie Komisie o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA uplatní aj na Island, Lichtenštajnsko a Nórsko, súbor dokumentov týkajúcich sa štítu na ochranu osobných údajov sa bude vzťahovať na Európsku úniu, aj na uvedené tri krajiny. Všetky odkazy na EÚ a jej členské štáty sa teda budú chápať tak, že zahŕňajú aj Island, Lichtenštajnsko a Nórsko.

údajov a nesmú poskytovať žiadne vyhlásenia ani vykonávať zavádzajúce postupy, ktoré by naznačovali ich zapojenie do štítu na ochranu osobných údajov; a že takéto organizácie už nie sú oprávnené využívať výhody plynúce z rozhodnutia Európskej komisie o primeranosti, čo by im umožnilo získavať osobné informácie z EÚ. Organizácii, ktorá naďalej tvrdí, že je zapojená do štítu na ochranu osobných údajov alebo robí iné nepravdivé vyhlásenia týkajúce sa štítu na ochranu osobných údajov po tom, ako bola vyradená zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov, môžu hroziť opatrenia na presadzovanie práva zo strany FTC, ministerstva dopravy alebo iných orgánov presadzovania práva.

5. Dodržiavanie týchto zásad môže byť obmedzené: a) na mieru potrebnú na splnenie požiadaviek národnej bezpečnosti, verejného záujmu alebo presadzovania práva; b) zákonmi, nariadeniami vlády alebo judikatúrou, ktoré stanovujú protichodné povinnosti alebo výslovné oprávnenia, za predpokladu, že pri vykonávaní každého takéhoto oprávnenia môže organizácia preukázať, že jej nedodržiavanie zásad je obmedzené do tej miery, ktorá je potrebná na splnenie nadradených oprávnených záujmov, na ktoré má takéto oprávnenie slúžiť, alebo c) ak účinok určitej smernice alebo právnych predpisov členského štátu umožňuje výnimky alebo odchýlky, za predpokladu, že takéto výnimky alebo odchýlky sa uplatňujú v porovnateľných súvislostiach. V súlade s cieľom zvyšovania ochrany súkromia by sa organizácie mali snažiť vykonávať tieto zásady v úplnosti a transparentne, čo tiež znamená, že by v rámci svojich podmienok ochrany súkromia mali uviesť, v akých prípadoch sa budú pravidelne uplatňovať výnimky zo zásad povolené na základe vyššie uvedeného písmena b). Z tých istých dôvodov sa predpokladá, že tam, kde je v súlade so zásadami a/alebo s právom USA možná voľba medzi určitými alternatívami, si organizácie podľa možnosti zvolia vyššiu úroveň ochrany.
6. Organizácie sú povinné uplatňovať zásady na všetky osobné údaje prenesené v rámci štítu na ochranu osobných údajov po tom, ako sa doňho zapoja. Organizácia, ktorá sa rozhodne rozšíriť výhody vyplývajúce zo štítu na ochranu osobných údajov na osobné informácie o ľudských zdrojoch prenášané z Európskej únie v súvislosti s pracovnoprávnymi vzťahmi musí túto skutočnosť uviesť pri poskytovaní osvedčenia o svojom dodržiavaní zásad ministerstvu a musí spĺňať požiadavky stanovené v doplnkovej zásade týkajúcej sa osvedčenia samotnou organizáciou.
7. Na otázky výkladu zásad a súladu so zásadami a príslušnými pravidlami ochrany súkromia, ktoré uplatňujú organizácie zapojené do štítu na ochranu osobných údajov, sa uplatňuje právo USA, s výnimkou prípadov, keď sa organizácie zaviazali spolupracovať s európskymi orgánmi pre ochranu osobných údajov (ďalej ako „DPA“). Pokiaľ nie je stanovené inak, všetky ustanovenia zásad sa uplatňujú tam, kde sú relevantné.
8. Vymedzenie pojmov:
 - a) „Osobné údaje“ a „osobné informácie“ sú údaje o identifikovanej alebo identifikovateľnej fyzickej osobe patriace do rámca pôsobnosti smernice, ktoré získava organizácia v Spojených štátoch od Európskej únie a ktoré sú v akejkoľvek forme zaznamenané.
 - b) „Spracovanie“ osobných údajov je akákoľvek operácia alebo súbor operácií, ktoré sa vykonávajú na osobných údajoch, či už automatizovanými prostriedkami, alebo bez automatizovaných prostriedkov, ako je zber, zaznamenávanie, usporiadanie, uchovávanie, úprava alebo pozmeňovanie, vyhľadávanie údajov, nahliadanie do nich, ich používanie, oznamovanie, šírenie a vymazanie alebo zničenie.
 - c) „Prevádzkovateľ“ je osoba alebo organizácia, ktorá sama alebo v spojení s inými určí účely a prostriedky spracovania osobných údajov.
9. Dňom nadobudnutia účinnosti zásad je deň konečného schválenia rozhodnutia Európskej komisie o primeranosti ochrany.

II. ZÁSADY

1. Oznámenie

- a) Organizácia musí informovať fyzické osoby o:
 - i) svojom zapojení do štítu na ochranu osobných údajov a poskytnúť hypertextový odkaz na zoznam organizácií zapojených do štítu na ochranu osobných údajov alebo jeho webovú adresu;
 - ii) druhoch zhromažďovaných osobných údajov a, ak je to vhodné, o subjektoch alebo dcérskych spoločnostiach organizácie, ktoré tiež dodržiavajú zásady;

- iii) svojom záväzku dodržiavať zásady v súvislosti so všetkými osobnými údajmi získanými z EÚ na základe štítu na ochranu osobných údajov,
 - iv) účeloch, na ktoré zhromažďuje a používa osobné informácie o nich;
 - v) spôsobe kontaktovania organizácie v prípade akýchkoľvek otázok alebo sťažností vrátane akýchkoľvek príslušných prevádzkárni v EÚ, ktoré môžu odpovedať na takéto otázky alebo sťažnosti;
 - vi) druhu alebo totožnosti tretích strán, ktorým poskytuje osobné informácie, ako o účeloch tohto konania;
 - vii) práve fyzických osôb na prístup k ich osobným údajom;
 - viii) možnostiach a prostriedkoch, ktoré daná organizácia poskytuje fyzickým osobám, ak chcú obmedziť využívanie a zverejňovanie svojich osobných údajov,
 - ix) nezávislom orgáne na riešenie sporov, ktorého úlohou je vybavovanie sťažností a bezplatné poskytovanie nápravy pre fyzické osoby, a či ide o: 1. výbor vytvorený orgánmi pre ochranu osobných údajov, 2. poskytovateľa alternatívneho riešenia sporov so sídlom v EÚ alebo 3. poskytovateľa alternatívneho riešenia sporov so sídlom v Spojených štátoch;
 - x) skutočnosti, že podlieha vyšetrovacím a donucovacím právomociam FTC, ministerstva dopravy alebo ktoréhokoľvek iného zákonom zriadeného štatutárneho orgánu Spojených štátov,
 - xi) možnosti jednotlivca využiť za určitých podmienok možnosť záväzného rozhodcovského konania;
 - xii) požiadavke na zverejnenie osobných informácií v reakcii na oprávnené žiadosti orgánov verejnej moci, vrátane plnenia požiadaviek národnej bezpečnosti alebo presadzovania práva, a
 - xiii) jej zodpovednosti v prípadoch ďalších prenosov tretím stranám.
- b) Toto oznámenie musí byť poskytnuté v jasnom a zrozumiteľnom jazyku vtedy, keď sa od fyzických osôb po prvýkrát požaduje poskytnutie osobných informácií danej organizácii alebo čo najskôr po tom, ako je to možné, ale v každom prípade pred tým, než daná organizácia využije takéto informácie na účel iný ako ten, na ktorý boli tieto informácie pôvodne zhromaždené alebo spracúvané prenášajúcou organizáciou alebo pred tým, než daná organizácia poskytne tieto informácie po prvýkrát tretej strane.

2. Možnosť voľby

- a) Organizácia musí fyzickým osobám ponúknuť možnosť rozhodnúť sa (možnosť vyjadriť nesúhlas), či sa ich osobné informácie i) môžu poskytnúť tretej strane alebo ii) môžu využiť na účel, ktorý sa podstatne odlišuje od účelu (účelov) na ktorý (ktoré) boli tieto informácie pôvodne zhromaždené alebo následne schválené danými fyzickými osobami. Fyzickým osobám sa musia poskytnúť jasné, zreteľné a ľahko dostupné mechanizmy na uskutočnenie takejto voľby.
- b) Odchyľne od predchádzajúceho odseku nie je potrebné poskytnúť možnosť voľby, keď sa údaje zverejnia tretej strane, ktorá koná ako zástupca a plní úlohu (úlohy) v mene organizácie a podľa jej pokynov. Organizácia však musí so zástupcom vždy uzavrieť zmluvu.
- c) Čo sa týka citlivých informácií (t. j. osobných informácií týkajúcich sa liečebnej starostlivosti alebo zdravotného stavu, rasového alebo etnického pôvodu, politických názorov, náboženskej viery alebo svetonázoru, členstva v odboroch alebo informácií týkajúcich sa sexuálneho života fyzickej osoby), organizácie musia od fyzických osôb získať výslovný súhlas (možnosť vyjadriť súhlas), ak sa príslušné informácie majú i) poskytnúť tretej strane alebo ii) využiť na účel iný ako ten, na ktorý boli tieto informácie pôvodne zhromaždené alebo následne schválené fyzickými osobami prostredníctvom uskutočnenia voľby vyjadrením súhlasu. Organizácia by mala navyše zaobchádzať s akýmkoľvek osobnými informáciami získanými od tretej strany ako s citlivými, ak ich tretia strana označí ako citlivé a zaobchádza s nimi ako s citlivými.

3. **Zodpovednosť za ďalší prenos**

- a) Aby mohli organizácie preniesť osobné informácie tretej strane, ktorá koná ako prevádzkovateľ, musia postupovať v súlade so zásadami oznámenia a možnosťou voľby. Organizácie musia takisto uzavrieť zmluvu s prevádzkovateľom, ktorý je treťou stranou, v ktorej sa stanoví, že takéto údaje sa môžu spracovávať výhradne na obmedzené a konkrétne účely v súlade so súhlasom a že príjemca zabezpečí rovnakú úroveň ochrany ako tieto zásady a oznámi organizácii, ak prijme rozhodnutie, že už ďalej nemôže plniť túto povinnosť. V zmluve musí byť stanovené, že po prijatí takeého rozhodnutia prevádzkovateľ tretej strany ukončí spracúvanie alebo prijme iné primerané a vhodné opatrenia na nápravu.
- b) Aby mohla organizácia preniesť osobné údaje tretej strane, ktorá koná ako zástupca, musí: i) preniesť takéto údaje len na obmedzené a konkrétne účely; ii) zistiť, či je zástupca povinný zabezpečiť prinajmenšom rovnakú úroveň ochrany súkromia, ako sa vyžaduje podľa zásad; iii) prijať primerané a vhodné opatrenia na zabezpečenie toho, že zástupca bude účinne spracúvať osobné informácie prenesené spôsobom, ktorý je v súlade s povinnosťami organizácie podľa zásad; iv) požadovať od sprostredkovateľa, aby oznámil organizácii, ak prijme rozhodnutie, že už ďalej nemôže plniť svoju povinnosť zabezpečiť rovnakú úroveň ochrany, ako sa vyžaduje podľa zásad; v) na základe oznámenia prijať, a to aj v prípade bodu iv), primerané a vhodné opatrenia na zastavenie a nápravu neoprávneného spracovania a vi) poskytnúť ministerstvu na vyžiadanie zhrnutie alebo reprezentatívnu kópiu príslušných ustanovení o ochrane súkromia zo zmluvy uzavretej s týmto zástupcom.

4. **Bezpečnosť**

- a) Organizácie vytvárajúce, uchovávajúce, využívajúce alebo rozširujúce osobné informácie musia uskutočniť primerané a vhodné opatrenia, aby zabránili strate týchto informácií, ich zneužitiu a neoprávnenému prístupu k nim, ich zverejňovaniu, zmene a zničeniu, pričom zohľadnia riziká spojené so spracovaním a povahou osobných údajov.

5. **Integrita údajov a obmedzenie účelu**

- a) Osobné informácie musia byť v súlade so zásadami obmedzené na informácie, ktoré sú relevantné na účely spracovania ⁽¹⁾. Organizácia nesmie spracúvať osobné informácie spôsobom, ktorý je nezlučiteľný s účelmi, na ktoré boli zhromaždené alebo následne odsúhlasené príslušným jednotlivcom. V miere nevyhnutnej na tieto účely musí organizácia prijať primerané opatrenia, aby zaistila spoľahlivosť osobných údajov na zamýšľaný účel, ich presnosť, úplnosť a aktuálnosť. Organizácia musí dodržiavať zásady po celý čas, čo takéto informácie uchováva.
- b) Informácie sa môžu uchovávať vo forme, ktorá identifikuje alebo umožňuje identifikáciu ⁽²⁾ jednotlivca, iba dovtedy, kým slúžia na účely spracovania v zmysle bodu 5 písm. a). Táto povinnosť nebráni organizáciám spracúvať osobné informácie počas dlhšieho obdobia, a to na také obdobie a v takom rozsahu, aby takéto spracovanie primerane slúžilo na účely archivovania vo verejnom záujme, novinárskej práce, literatúry a umenia, vedeckého alebo historického výskumu a štatistickej analýzy. V týchto prípadoch sa na takéto spracovanie vzťahujú iné zásady a ustanovenia rámca. Organizácie by mali prijať primerané a vhodné opatrenia na plnenie tohto ustanovenia.

6. **Prístup**

- a) Fyzické osoby musia mať prístup k svojim osobným informáciám, ktoré uchováva určitá organizácia, a musia mať možnosť opraviť, zmeniť alebo vypustiť určité informácie, ak sú tieto informácie nepresné alebo boli spracované v rozpore so zásadami, s výnimkou prípadov, keď by zataženie alebo výdavky súvisiace s poskytnutím prístupu neboli v danom prípade úmerné ohrozeniu súkromia dotknutej osoby alebo keď by boli poškodené práva osôb iných ako príslušnej fyzickej osoby.

⁽¹⁾ V závislosti od okolností môžu byť príkladom zlučiteľných účelov spracovania také účely, ktoré primerane slúžia v oblasti vzťahov so zákazníkmi, posudzovania súladu a právnych aspektov, vykonávania auditu, bezpečnosti a predchádzania podvodom, ochrany alebo obhajovania zákonných práv organizácie, alebo iné účely, ktoré sú v súlade s primeranými očakávaniami v súvislosti so zhromažďovaním údajov.

⁽²⁾ V tejto súvislosti sa jednotlivec považuje za „identifikovateľného“, ak vzhľadom na prostriedky identifikácie, ktoré sa s primeranou pravdepodobnosťou použijú (pri zohľadnení, okrem iného, nákladov a času potrebného na identifikáciu a technológie dostupnej v čase spracovania), a formu, v akej sa údaje uchovávajú, by organizácia alebo tretia strana mohla jednotlivca primerane identifikovať, ak by mala prístup k jeho údajom.

7. Náprava, presadzovanie a zodpovednosť

- a) Účinná ochrana súkromia musí zahŕňať spoľahlivé mechanizmy zabezpečujúce dodržiavanie týchto zásad, prostriedky nápravy pre fyzické osoby dotknuté nedodržiavaním zásad, ako aj dôsledky pre príslušnú organizáciu v prípade nedodržiavania zásad. Takéto mechanizmy musia prinajmenšom zahŕňať:
- i) ľahko dostupné nezávislé mechanizmy nápravy, prostredníctvom ktorých sa vyšetrujú a urýchlene riešia sťažnosti a spory fyzických osôb bez toho, aby im vznikli akékoľvek náklady a s odkazom na zásady, a priznávajú sa náhrady, ak sa tak stanovuje v platných právnych predpisoch alebo iniciatívach súkromného sektora;
 - ii) následné postupy na overenie toho, či sú osvedčenia a tvrdenia organizácií o ich postupoch v oblasti ochrany súkromia pravdivé a či sa postupy v oblasti ochrany súkromia vykonávajú tak, ako sú prezentované, a to najmä v prípadoch nedodržiavania zásad; a
 - iii) povinnosti napraviť problémy, ktoré vznikli v dôsledku nedodržiavania zásad organizáciami vyhlasujúcimi, že zásady dodržiavajú, a vyvodenie dôsledkov pre takéto organizácie. Sankcie musia byť dostatočne prísne, aby zabezpečili dodržiavanie zásad organizáciami.
- b) Organizácie a ich vybrané nezávislé mechanizmy nápravy budú rýchlo reagovať na otázky a žiadosti ministerstva o informácie týkajúce sa štítu na ochranu osobných údajov. Všetky organizácie musia pohotovo reagovať na sťažnosti týkajúce sa dodržiavania zásad, ktoré postúpia orgány členského štátu EÚ prostredníctvom ministerstva. Organizácie, ktoré sa rozhodli spolupracovať s DPA, vrátane organizácií, ktoré spracúvajú údaje o ľudských zdrojoch, musia v súvislosti s vyšetrovaním a vybavovaním sťažností odpovedať priamo takýmto orgánom.
- c) Organizácie sú povinné riešiť sťažnosti a dodržiavať podmienky stanovené v prílohe I za predpokladu, že jednotlivец sa dovoľoval záväzného rozhodcovského konania tým, že doručil príslušnej organizácii oznámenie podľa postupov a podmienok stanovených v prílohe I.
- d) V kontexte ďalšieho prenosu je organizácia zapojená do štítu na ochranu osobných údajov zodpovedná za spracovanie osobných informácií, ktoré získa v rámci štítu na ochranu osobných údajov a následne ich prenesie tretej strane, ktorá koná v jej mene ako zástupca. Organizácia zapojená do štítu na ochranu osobných údajov zostane zodpovedná podľa zásad, ak jej zástupca spracúva takéto osobné informácie spôsobom, ktorý je v rozpore so zásadami, pokiaľ organizácia nepreukáže, že nie je zodpovedná za skutočnosť, ktorá spôsobila škodu.
- e) Keď organizácia podlieha príkazu FTC alebo súdnemu príkazu, ktorý je založený na nedodržiavaní zásad, zverejní akékoľvek relevantné časti štítu na ochranu osobných údajov týkajúce sa akejkoľvek správy o dodržiavaní zásad alebo hodnotiacej správy FTC, pokiaľ je to zlučiteľné s požiadavkami dôvernosti. Ministerstvo zriadilo vyhradené kontaktné miesto, na ktoré sa DPA môžu obrátiť v prípade akýchkoľvek problémov s dodržiavaním zásad zo strany organizácií zapojených do štítu na ochranu osobných údajov. Federálna obchodná Komisia sa bude prioritne zaoberať sťažnosťami na nedodržiavanie zásad postúpenými ministerstvom a orgánmi členských štátov EÚ a bude si v súvislosti s týmito sťažnosťami včas vymieňať informácie s orgánmi postupujúceho štátu, a to v rámci existujúcich obmedzení týkajúcich sa dôvernosti údajov.

III. DOPLNKOVÉ ZÁSADY

1. Citlivé údaje

- a) Organizácia nemusí získať výslovný súhlas (možnosť vyjadriť súhlas) v súvislosti s citlivými údajmi, ak je spracovanie:
- i) vykonávané v životne dôležitom záujme dotknutej osoby alebo inej osoby;
 - ii) potrebné na uplatnenie právnych nárokov alebo na obhajobu;
 - iii) nevyhnutné na účely poskytnutia zdravotnej starostlivosti alebo stanovenia diagnózy;
 - iv) vykonávané v priebehu zákonnej činnosti nadácie, združenia alebo akéhokoľvek iného neziskového subjektu majúceho politický, filozofický, náboženský alebo odborársky cieľ a pod podmienkou, že sa spracúvanie týka výlučne členov príslušného subjektu alebo osôb, ktoré sú s ním v pravidelnom kontakte v súvislosti s jeho cieľmi a že sa údaje neposkytnú tretej strane bez súhlasu dotknutých osôb;

- v) nevyhnutné na plnenie povinností príslušnej organizácie v oblasti pracovného práva alebo
- vi) vykonávané v súvislosti s údajmi, ktoré príslušná fyzická osoba preukázateľne zverejnila.

2. Výnimky pre novinárov

- a) Vzhľadom na ústavnú ochranu slobody tlače v USA a výnimku stanovenú v smernici s ohľadom na novinárske účely, ak sa práva na slobodnú tlač zakotvené v Prvom dodatku k Ústave Spojených štátov stretávajú so záujmami v oblasti ochrany súkromia, musí sa vyvážením týchto záujmov so zreteľom na činnosť osôb alebo organizácií v Spojených štátoch riadiť Prvým dodatkom.
- b) Osobné informácie zhromažďované s cieľom uverejnenia v tlači, vysielania rozhlasom alebo televíziou alebo iných foriem verejného oznámenia novinárskeho materiálu, bez ohľadu na to, či sa použijú alebo nie, ani informácie nájdené v už uverejnenom materiáli rozšírenom z mediálnych archívov, nepodliehajú požiadavkám zásad štítu na ochranu osobných údajov.

3. Druhotná zodpovednosť

- a) Poskytovatelia internetových služieb, telekomunikační prevádzkovatelia ani iné organizácie nenesú zodpovednosť podľa zásad štítu na ochranu osobných údajov, ak v mene inej organizácie len prenášajú, presmerovávajú, prepájajú alebo dočasne ukladajú informácie. Podobne ako je to v prípade samotnej smernice, štít na ochranu osobných údajov nezakladá druhotnú zodpovednosť. Pokiaľ určitá organizácia len ďalej odovzdáva údaje prenášané tretími stranami a nerozhoduje o účeloch a prostriedkoch spracúvania týchto osobných údajov, nie je zodpovedná.

4. Vykonávanie hĺbkovej analýzy a auditov

- a) Činnosť audítorov a investičných bankárov môže zahŕňať spracúvanie osobných údajov bez súhlasu alebo vedomia jednotlivca. Je to povolené v rámci zásad oznámenia, možnosti voľby a prístupu a za okolností, ktoré sú opísané nižšie.
- b) Verejné akciové spoločnosti a súkromné akciové spoločnosti vrátane organizácií zapojených do štítu na ochranu osobných údajov sa pravidelne podrobia auditom. Takéto audity, najmä také, ktoré sú zamerané na potenciálne protiprávne konanie, môžu byť ohrozené, ak sa predčasne zverejnia. Podobne aj organizácie zapojené do štítu na ochranu osobných údajov sa v prípade možného zlúčenia alebo prevzatia budú musieť podrobiť hĺbkovej analýze alebo ju samé vykonať. To bude často zahŕňať zhromažďovanie a spracúvanie osobných údajov, ako napríklad informácií o vedúcich pracovníkoch a iných kľúčových zamestnancoch. Predčasné zverejnenie by mohlo zabrániť transakcii alebo dokonca porušiť platné predpisy o cenných papieroch. Investiční bankári, právni zástupcovia zapojení do hĺbkovej analýzy, alebo audítori vykonávajúci audit môžu spracúvať informácie bez vedomia jednotlivca len v rozsahu potrebnom a počas obdobia potrebného na to, aby splnili zákonné požiadavky alebo požiadavky verejného záujmu a za iných okolností, za ktorých by uplatňovaním týchto zásad boli dotknuté oprávnené záujmy príslušnej organizácie. Tieto oprávnené záujmy zahŕňajú monitorovanie dodržiavania právnych záväzkov organizáciou a legitímnu účtovnícku činnosť a potrebu zachovania dôvernosti v súvislosti s prípadnými akvizíciami, fúziami, spoločnými podnikmi alebo inými podobnými transakciami vykonávanými investičnými bankármi alebo audítormi.

5. Úloha orgánov pre ochranu osobných údajov

- a) Organizácie budú plniť svoj záväzok spolupracovať s orgánmi Európskej únie pre ochranu osobných údajov (DPA), ako je uvedené nižšie. Podľa zásad štítu na ochranu osobných údajov sa musia organizácie Spojených štátov, ktoré získavajú osobné údaje z EÚ, zaviazat, že budú uplatňovať účinné mechanizmy na zabezpečenie dodržiavania zásad štítu na ochranu osobných údajov. Konkrétne, ako je to stanovené v zásade nápravy, presadzovania a zodpovednosti, musia zapojené organizácie: a) i) poskytnúť možnosť nápravy pre fyzické osoby, ktorých sa údaje týkajú; a) ii) zabezpečiť následné postupy umožňujúce overiť, či sú ich osvedčenia a tvrdenia o postupoch v oblasti ochrany súkromia pravdivé a a) iii) plniť povinnosť napraviť problémy, ktoré vznikli v dôsledku nedodržiavania zásad a prijať príslušné sankcie za porušenie týchto zásad. Organizácia môže spĺňať písmeno a) body i) a iii) zásady nápravy, presadzovania a zodpovednosti, ak dodržiava požiadavky stanovené v tejto časti pre spoluprácu s DPA.

- b) Organizácia sa zaväzuje k spolupráci s DPA tým, že v rámci osvedčenia o svojom dodržiavaní štítu na ochranu osobných údajov poskytne ministerstvu obchodu (pozri doplnkovú zásadu týkajúcu sa osvedčenia vydávaného samotnou organizáciou) vyhlásenie o tom, že:
- i) sa rozhodla splniť požiadavku v písmene a) bodoch i) a iii) zásady štítu na ochranu osobných údajov týkajúcu sa nápravy, presadzovania a zodpovednosti tým, že sa zaviazala spolupracovať s DPA;
 - ii) bude spolupracovať s DPA pri vyšetrowaní a riešení sťažností vznesených na základe štítu na ochranu osobných údajov a
 - iii) bude dodržiavať všetky odporúčania poskytnuté DPA, ak budú DPA toho názoru, že daná organizácia musí prijať osobitné opatrenia s cieľom dodržiavať zásady štítu na ochranu osobných údajov, vrátane nápravných alebo kompenzačných opatrení v prospech fyzických osôb dotknutých akýmkoľvek nedodržiavaním zásad a poskytne DPA písomné potvrdenie, že sa takéto opatrenia vykonali.
- c) Fungovanie výborov DPA
- i) Spolupráca zo strany DPA bude zabezpečená vo forme informácií a odporúčaní nasledujúcim spôsobom:
 - 1. Odporúčania zo strany DPA sa budú poskytovať prostredníctvom neformálneho výboru DPA ustanoveného na úrovni Európskej únie, ktorý okrem iného pomôže zabezpečiť harmonizovaný a jednotný prístup.
 - 2. Výbor bude príslušným organizáciám v Spojených štátoch poskytovať odporúčania ohľadom nevyriešených sťažností fyzických osôb týkajúcich sa zaobchádzania s osobnými informáciami, ktoré boli prenesené z EÚ v rámci štítu na ochranu osobných údajov. Cieľom týchto odporúčaní bude zabezpečiť, aby sa zásady štítu na ochranu osobných údajov uplatňovali správne, pričom tieto odporúčania budú zahŕňať všetky opravné prostriedky vo vzťahu k príslušnej fyzickej osobe (fyzickým osobám), ktoré budú DPA považovať za primerané.
 - 3. Výbor bude takéto odporúčania poskytovať na základe žiadostí príslušných organizácií a/alebo sťažností obdržaných priamo od fyzických osôb na organizácie, ktoré sa zaviazali spolupracovať s DPA na účely štítu na ochranu osobných údajov, pričom bude takéto fyzické osoby povzbudzovať a podľa potreby im pomáhať, aby najskôr využili vnútropodnikové mechanizmy na vybavovanie sťažností, ktoré daná organizácia poskytuje.
 - 4. Odporúčania budú poskytnuté až po tom, čo obe strany sporu mali primeranú možnosť vyjadriť sa a predložiť všetky dôkazy, ktoré chceli. Výbor sa bude snažiť poskytnúť odporúčania tak rýchlo, ako mu to umožňuje táto požiadavka ohľadom náležitého postupu. Vo všeobecnosti sa výbor bude snažiť poskytnúť odporúčania do 60 dní od doručenia sťažnosti alebo žiadosti a podľa možnosti rýchlejšie.
 - 5. Výbor zverejní výsledky svojho posúdenia sťažností, ktoré mu boli predložené, ak to bude považovať za vhodné.
 - 6. Poskytnutie odporúčania prostredníctvom výboru nezakladá vo vzťahu k výboru alebo vo vzťahu k jednotlivým DPA žiadnu zodpovednosť.
 - ii) Ako bolo uvedené vyššie organizácie, ktoré sa rozhodnú pre tento spôsob riešenia sporov sa musia zaviazat, že budú dodržiavať odporúčania poskytnuté zo strany DPA. Ak sa určitá organizácia nepodrobí odporúčaniam do 25 dní odo dňa jeho vydania a neposkytne žiadne uspokojujúce vysvetlenie omeškania, výbor oznámi svoj zámer byť predložiť danú záležitosť Federálnej obchodnej komisii, ministerstvu dopravy alebo inému federálnemu alebo štátnemu orgánu USA so zákonnými právomocami v záujme prijatia opatrení na presadenie odporúčaní v prípadoch podvodu alebo nepravdivého vyhlásenia, alebo svoj zámer rozhodnúť o tom, že dohoda o spolupráci bola závažným spôsobom porušená, a preto sa musí považovať za neplatnú. V poslednom prípade výbor informuje ministerstvo obchodu, aby sa mohol náležite upraviť zoznam organizácií zapojených do štítu na ochranu osobných údajov. Akékoľvek nesplnenie záväzku spolupracovať s DPA, ako aj nedodržanie zásad štítu na ochranu osobných údajov, bude žalovateľné ako klamlivá praktika podľa oddielu 5 zákona o Federálnej obchodnej komisii alebo podľa iného podobného právneho predpisu.
- d) Organizácia, ktorá má záujem o rozšírenie výhod vyplývajúcich zo štítu na ochranu osobných údajov na údaje týkajúce sa ľudských zdrojov prenášané z EÚ v súvislosti s pracovnoprávnymi vzťahmi, sa musí zaviazat, že vo vzťahu k takýmto údajom bude spolupracovať s DPA (pozri doplnkovú zásadu týkajúcu sa údajov o ľudských zdrojoch),

- e) Organizácie, ktoré sa rozhodnú pre túto možnosť, budú musieť platiť ročný poplatok určený na pokrytie prevádzkových nákladov výboru a môžu byť dodatočne požiadané, aby uhradili akékoľvek potrebné výdavky na preklad súvisiace s posudzovaním, ktoré výbor uskutočňuje vo vzťahu k žiadostiam alebo sťažnostiam týkajúcim sa týchto organizácií. Ročný poplatok neprekročí 500 USD a pre menšie spoločnosti bude nižší.

6. Osvedčenie vydávané samotnou organizáciou

- a) Výhody vyplývajúce zo štítu na ochranu osobných údajov sú zabezpečené od dátumu, keď ministerstvo doplní organizáciu do zoznamu organizácií zapojených do štítu na ochranu osobných údajov po tom, ako organizácia poskytla osvedčenie o svojom dodržiavaní zásad štítu na ochranu osobných údajov a ministerstvo potvrdilo úplnosť tohto osvedčenia.
- b) S cieľom poskytnutia osvedčenia o svojom dodržiavaní zásad štítu na ochranu osobných údajov musí organizácia ministerstvu poslať list podpísaný vedúcim pracovníkom spoločnosti v mene danej organizácie pripájajúcej sa k štítu na ochranu osobných údajov, ktorý obsahuje prinajmenšom nasledujúce informácie:
- i) názov organizácie, poštovú adresu, e-mailovú adresu, telefónne a faxové čísla;
 - ii) opis činnosti danej organizácie s ohľadom na osobné informácie získavané od EÚ a
 - iii) opis podmienok ochrany súkromia danej organizácie vo vzťahu k takýmto osobným informáciám, vrátane:
 1. ak má organizácia webovú lokalitu, príslušnú internetovú stránku, kde sú k dispozícii podmienky ochrany súkromia, alebo ak organizácia nemá verejnú webovú lokalitu, kde sú verejnosti sprístupnené podmienky ochrany súkromia;
 2. dňa, kedy nadobúda účinnosť vykonávanie týchto pravidiel;
 3. kontaktného orgánu pre vybavovanie sťažností, žiadostí o prístup a akýchkoľvek iných záležitostí vyplývajúcich z uplatňovania štítu na ochranu osobných údajov;
 4. osobitného zákonom zriadeného orgánu, v ktorého právomoci je vypočutie sťažností voči danej organizácii, čo sa týka možných nekalých alebo klamlivých praktík a porušení zákonov alebo iných právnych predpisov upravujúcich ochranu súkromia (a ktorý je uvedený v zásadách alebo v budúcom zozname pripojenom k zásadám);
 5. názvu akéhokoľvek programu v oblasti ochrany súkromia, ktorého je daná organizácia členom;
 6. spôsobu overovania (napr. vnútri podniku, treťou stranou) (pozri doplnkovú zásadu týkajúcu sa overovania); a
 7. nezávislého mechanizmu nápravy, ktorý je dostupný s cieľom vyšetrovania nevyriešených sťažností.
- c) Tam, kde má organizácia záujem o to, aby výhody vyplývajúce zo štítu na ochranu osobných údajov zahŕňali informácie o ľudských zdrojoch prenášané z EÚ na využitie v súvislosti s pracovnoprávnymi vzťahmi, môže tak urobiť, ak existuje štatutárny orgán s právomocou vypočúvať sťažnosti voči danej organizácii vyplývajúce z informácií o ľudských zdrojoch, ktorý je uvedený v zásadách alebo v budúcom zozname pripojenom k zásadám. Daná organizácia musí túto skutočnosť okrem toho uviesť vo svojom osvedčení o dodržiavaní zásad a musí vyhlásiť, že sa zaväzuje spolupracovať s príslušným orgánom alebo orgánmi EÚ v súlade s doplnkovými zásadami týkajúcimi sa údajov o ľudských zdrojoch, resp. úlohy orgánov pre ochranu osobných údajov, a že bude dodržiavať odporúčania poskytnuté týmito orgánmi. Organizácia musí tiež ministerstvu poslať kópiu svojich podmienok ochrany súkromia v oblasti ľudských zdrojov a poskytnúť informácie o dostupnosti podmienok ochrany súkromia k nahliadnutiu pre dotknutých zamestnancov.
- d) Ministerstvo bude viesť zoznam organizácií zapojených do štítu na ochranu osobných údajov, ktoré predložili úplné osvedčenia o dodržiavaní zásad a ktorým tak prináležia výhody vyplývajúce zo štítu na ochranu osobných údajov, a tento zoznam bude aktualizovať na základe každoročne predkladaných osvedčení a oznámení prijatých podľa doplnkovej zásady týkajúcej sa riešenia sporov a presadzovania práva. Takéto osvedčenia o dodržiavaní zásad sa musia predkladať najmenej raz ročne; v opačnom prípade bude organizácia vyradená zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov a už viac nebude môcť využívať výhody vyplývajúce zo štítu na ochranu osobných údajov. Zoznam organizácií zapojených do štítu na ochranu osobných údajov a osvedčenia organizácií o dodržiavaní zásad budú verejne sprístupnené. Všetky organizácie, ktoré ministerstvo zaradi do zoznamu organizácií zapojených do štítu na ochranu osobných údajov, musia tiež vo svojich príslušných uverejnených vyhláseniach o podmienkach ochrany súkromia uviesť, že dodržiavajú zásady štítu na ochranu osobných údajov. V prípade dostupnosti na internete musia podmienky ochrany

súkromia organizácie obsahovať hypertextový odkaz na webovú lokalitu štítu na ochranu osobných údajov vytvorenú ministerstvom alebo formulár na predkladanie sťažností v rámci nezávislého mechanizmu nápravy, pomocou ktorého sa vyšetrujú nevyriešené sťažnosti.

- e) Podmienky ochrany súkromia platia hneď po osvedčení. Keďže zásady ovplyvnia obchodné vzťahy s tretími stranami, organizácie, ktoré poskytnú osvedčenie v rámci štítu na ochranu osobných údajov v priebehu prvých dvoch mesiacov po dátume účinnosti rámca, musia uviesť existujúce obchodné vzťahy s tretími stranami do súladu so zásadou zodpovednosti za ďalší prenos, a to čo najskôr, ale každopádne najneskôr do deviatich mesiacov od dátumu, keď osvedčia svoje dodržiavanie zásad štítu na ochranu osobných údajov. Počas tohto prechodného obdobia, keď organizácie prenášajú údaje tretej strane, i) uplatňujú zásady oznámenia a možnosti voľby a ii) ak sa osobné údaje prenášajú tretej strane, ktorá koná ako zástupca, presvedčia sa, či je zástupca povinný zabezpečiť prinajmenšom rovnakú úroveň ochrany, aká sa vyžaduje podľa zásad.
- f) Organizácia musí dodržiavať zásady štítu na ochranu osobných údajov v prípade všetkých osobných údajov získaných z EÚ na základe štítu na ochranu osobných údajov. Záväzok dodržiavať zásady štítu na ochranu osobných údajov nie je časovo obmedzený vo vzťahu k údajom získavaným v priebehu obdobia, v ktorom daná organizácia využíva výhody vyplývajúce zo štítu na ochranu osobných údajov. Záväzok organizácie znamená, že bude vo vzťahu k takýmto údajom naďalej uplatňovať zásady tak dlho ako ich bude uchovávať, využívať alebo poskytovať, a to dokonca aj vtedy, ak následne štít na ochranu osobných údajov z akýchkoľvek dôvodov opustí. Organizácia, ktorá opustí štít na ochranu osobných údajov, ale chce si ponechať takéto údaje, musí ministerstvo každoročne uisťovať o svojom záväzku pokračovať v uplatňovaní zásad alebo poskytovaní „primeranej“ ochrany daných informácií iným povoleným spôsobom (napríklad prostredníctvom zmluvy, ktorá úplne zodpovedá požiadavkám príslušných štandardných zmluvných ustanovení prijatých Európskou komisiou); inak musí organizácia dané informácie vrátiť alebo vymazať. Organizácia, ktorá opustí štít na ochranu osobných údajov, musí z akýchkoľvek príslušných podmienok ochrany súkromia odstrániť všetky odkazy na štít na ochranu osobných údajov, ktoré naznačujú aktívnu účasť organizácie v štíte na ochranu osobných údajov a jej nárok na využívanie príslušných výhod.
- g) Organizácia, ktorá v dôsledku fúzie alebo prevzatia prestane existovať ako samostatná právnická osoba, o tom musí vopred informovať ministerstvo. V tomto oznámení by tiež malo byť uvedené, či nadobúdajúca spoločnosť alebo spoločnosť vzniknutá v dôsledku fúzie i) bude podľa práva upravujúceho prevzatie alebo fúziu naďalej viazaná zásadami štítu na ochranu osobných údajov alebo ii) sa rozhodne poskytnúť osvedčenie o svojom dodržiavaní zásad štítu na ochranu osobných údajov alebo poskytnúť iné záruky, ako napríklad písomnú dohodu, ktorá zabezpečí dodržiavanie zásad štítu na ochranu osobných údajov. Pokiaľ neplatí ani i) ani ii), musia byť všetky osobné údaje získané v rámci štítu na ochranu osobných údajov okamžite vymazané.
- h) Ak organizácia z akýchkoľvek dôvodov opustí štít na ochranu osobných údajov, musí odstrániť všetky vyhlásenia, ktoré naznačujú jej pokračujúce zapojenie do štítu na ochranu osobných údajov alebo jej nárok na využívanie výhod vyplývajúcich zo štítu na ochranu osobných údajov. Ak organizácia používa certifikačnú značku štítu na ochranu osobných údajov medzi EÚ a USA, musí sa táto značka tiež odstrániť. Akékoľvek nepravdivé vyhlásenie pre verejnosť ohľadom dodržiavania zásad štítu na ochranu osobných údajov organizáciou môže byť žalovateľné zo strany Federálnej obchodnej komisie alebo iného príslušného vládneho orgánu. Nepravdivé vyhlásenia pre ministerstvo môžu byť žalovateľné podľa zákona o nepravdivých vyhláseniach (18 U.S.C. § 1001).

7. Overovanie

- a) Organizácie musia zabezpečiť následné postupy na overenie toho, či sú ich osvedčenia a tvrdenia o postupoch v oblasti ochrany súkromia na základe štítu na ochranu osobných údajov pravdivé a či sa tieto postupy ochrany súkromia vykonávajú tak, ako sa prezentuje, a v súlade so zásadami štítu na ochranu osobných údajov.
- b) Aby organizácia splnila požiadavky na overovanie stanovené v zásade nápravy, presadzovania a zodpovednosti, musí takéto osvedčenia a tvrdenia overovať buď prostredníctvom posudzovania dodržiavania zásad vykonaného samotnou organizáciou, alebo externým posudzovateľom.
- c) Pri posudzovaní vykonávanom samotnou organizáciou sa musí takýmto overením zistiť, že zverejnené podmienky ochrany súkromia danej organizácie týkajúce sa osobných informácií získavaných z EÚ sú presné, úplné, oznámené na viditeľnom mieste, vykonávané v úplnosti a prístupné. Malo by sa tiež preukázať, že podmienky ochrany súkromia zodpovedajú zásadám štítu na ochranu osobných údajov; že fyzické osoby sú informované o všetkých mechanizmoch vybavovania sťažností dostupných v rámci organizácie a o nezávislých mechanizmoch, prostredníctvom ktorých môžu podávať sťažnosti; že organizácia zaviedla postupy odbornej prípravy zamestnancov v oblasti vykonávania podmienok ochrany súkromia a postihovania zamestnancov v prípade nedodržania týchto podmienok a že daná organizácia zaviedla interné postupy s cieľom vykonávania pravidelného objektívneho posudzovania dodržiavania toho, čo bolo uvedené vyššie. Vyhlásenie osvedčujúce

posúdenie vykonané samotnou organizáciou musí byť podpísané vedúcim pracovníkom alebo iným oprávneným zástupcom danej organizácie najmenej raz za rok a musí byť na požiadanie sprístupnené fyzickým osobám alebo v súvislosti s vyšetrovaním alebo sťažnosťou ohľadom nedodržiavania zásad.

- d) V prípade, že sa organizácia rozhodne pre posúdenie dodržiavania zásad externým posudzovateľom, pri takomto posúdení sa musí preukázať, že jej podmienky ochrany súkromia týkajúce sa osobných informácií získavaných z EÚ sú v súlade so zásadami štítu na ochranu osobných údajov, že sa dodržiavajú a že fyzické osoby sú informované o mechanizmoch, prostredníctvom ktorých môžu podávať sťažnosti. Spôsoby posudzovania môžu bez obmedzenia zahŕňať audit, náhodné kontroly, používanie „návnad“ alebo prípadne využívanie technologických nástrojov. Vyhlásenie osvedčujúce, že bolo úspešne ukončené posúdenie dodržiavania zásad vykonané externým posudzovateľom, musí byť podpísané buď posudzovateľom, alebo vedúcim pracovníkom alebo iným oprávneným zástupcom danej organizácie najmenej raz za rok a malo by byť na požiadanie sprístupnené fyzickým osobám alebo v súvislosti s vyšetrovaním alebo sťažnosťou ohľadom dodržiavania zásad.
- e) Organizácie musia uchovávať záznamy o dodržiavaní svojich postupov v oblasti ochrany súkromia na základe štítu na ochranu osobných údajov a musia ich na požiadanie sprístupniť, v súvislosti s vyšetrovaním alebo sťažnosťou ohľadom nedodržiavania postupov, nezávislému orgánu zodpovednému za vyšetrovanie sťažností alebo orgánu, ktorý je príslušný rozhodovať v prípadoch nekalých a klamlivých praktík. Organizácie tiež musia rýchlo reagovať na otázky a iné žiadosti ministerstva o informácie týkajúce sa dodržiavania zásad zo strany organizácie.

8. Prístup

a) Zásada prístupu v praxi

- i) Podľa zásad štítu na ochranu osobných údajov je právo na prístup k osobným informáciám základom ochrany súkromia. Konkrétne umožňuje fyzickým osobám overovať správnosť informácií, ktoré sa o nich uchovávajú. Podľa zásady prístupu majú fyzické osoby právo:
1. získať od organizácie potvrdenie o tom, či organizácia spracúva alebo nespracúva osobné údaje, ktoré sa ich týkajú⁽¹⁾;
 2. získať takéto údaje, aby si mohli overiť ich presnosť a zákonnosť spracovania, a
 3. dať tieto údaje opraviť, zmeniť alebo vymazať, ak sú nepresné alebo sa spracovali v rozpore so zásadami.
- ii) Fyzické osoby nemusia odôvodňovať svoje žiadosti o prístup k svojim vlastným údajom. Pri reagovaní na žiadosti fyzických osôb o prístup by sa organizácie mali predovšetkým riadiť dôvodom (dôvodmi), ktoré viedli k príslušným žiadostiam. Napríklad, ak je žiadosť o prístup nejasná alebo rozsahom všeobecná, organizácia môže s jednotlivcom nadviazať dialóg, aby lepšie pochopila motiváciu danej žiadosti a lokalizovala zodpovedajúce informácie. Organizácia sa môže zaujímať o to, s ktorou organizačnou súčasťou (súčasťami) danej organizácie príslušný jednotlivec komunikoval a/alebo o povahu informácií alebo ich využitie, ktoré sú predmetom žiadosti o prístup.
- iii) V súlade so základnou povahou prístupu k osobným informáciám by sa organizácie mali vždy v dobrej viere snažiť poskytnúť prístup. Napríklad, ak je potrebné určité informácie chrániť a dajú sa ľahko oddeliť od iných osobných informácií, ktorých sa týka žiadosť o prístup, organizácia by mala oddeliť chránené informácie a mala by sprístupniť ostatné informácie. Ak organizácia rozhodne, že v niektorom konkrétnom prípade by sa mal prístup obmedziť, mala by fyzickej osobe požadujúcej prístup poskytnúť vysvetlenie, prečo sa takto rozhodla, a mala by mu udať kontaktné miesto, na ktoré sa môže obrátiť v prípade ďalších otázok.

b) Zaťaženie alebo výdavky súvisiace s poskytnutím prístupu

- i) Právo na prístup k osobným údajom sa môže vo výnimočných prípadoch obmedziť, ak by boli porušené legitímne práva osôb iných než daná fyzická osoba, alebo v prípadoch, keď by zaťaženie alebo výdavky súvisiace s poskytnutím prístupu boli v danom prípade neúmerné rizikám pre súkromie fyzickej osoby. Výdavky a zaťaženie sú významnými faktormi a mali by sa brať do úvahy, ale nie sú určujúce pri rozhodovaní o tom, či je poskytnutie prístupu opodstatnené.

⁽¹⁾ Organizácia by mala odpovedať na žiadosti fyzických osôb týkajúce sa účelov spracovania, kategórií príslušných osobných údajov a príjemcov či kategórií príjemcov, ktorým sa osobné údaje poskytujú.

- ii) Napríklad, ak sa dané osobné informácie využívajú na prijatie rozhodnutí, ktoré sa významným spôsobom dotknú danej fyzickej osoby (napríklad zamietnutie alebo priznanie dôležitých výhod, ako je napríklad poistné, hypotéka alebo práca), potom by organizácia v súlade s ostatnými ustanoveniami doplnkových zásad mala tieto informácie poskytnúť dokonca aj vtedy, ak je toto poskytnutie relatívne zložité alebo nákladné. Ak požadované osobné informácie nie sú citlivé alebo sa nevyužívajú na prijatie rozhodnutí, ktoré sa významným spôsobom dotknú danej fyzickej osoby, ale sú ľahko dostupné a ich poskytnutie nie je nákladné, organizácia by mala poskytnúť prístup k takýmto informáciám.

c) Dôverné obchodné informácie

- i) Dôverné obchodné informácie sú informácie, vo vzťahu ku ktorým určitá organizácia podnikla kroky na ich ochranu pred zverejnením, pretože takéto zverejnenie by zvýhodnilo konkurenta na trhu. Organizácie môžu zamietnuť alebo obmedziť prístup, pokiaľ by sa poskytnutím úplného prístupu odhalili ich vlastné dôverné obchodné informácie, ako napríklad marketingové odhady alebo kategorizácie vypracované danou organizáciou alebo dôverné obchodné informácie inej organizácie, na ktoré sa vzťahuje zmluvná povinnosť utajenia.
- ii) Ak je možné dôverné obchodné informácie ľahko oddeliť od iných osobných informácií, ktorých sa týka žiadosť o prístup, daná organizácia by mala oddeliť dôverné obchodné informácie a mala by sprístupniť nedôverné informácie.

d) Organizácia databáz

- i) Prístup je možné poskytnúť tak, že organizácia sprístupní relevantné osobné informácie fyzickej osobe, pričom sa nevyžaduje, aby organizácia poskytla fyzickej osobe prístup k svojej databáze.
- ii) Prístup k osobným informáciám sa musí poskytnúť len vtedy, ak organizácia dané informácie uchováva. Samotná zásada prístupu nezakladá povinnosť uchovávať, udržiavať, reorganizovať alebo reštrukturalizovať súbory s osobnými informáciami.

e) Prípady obmedzenia prístupu

- i) Keďže organizácie sa musia vždy v dobrej viere snažiť poskytnúť fyzickým osobám prístup k ich osobným údajom, okolnosti, za ktorých môžu takýto prístup obmedziť, sú obmedzené, a akékoľvek dôvody na obmedzenie prístupu musia byť konkrétne uvedené. Rovnako ako na základe smernice môže organizácia obmedziť prístup k informáciám, pokiaľ je pravdepodobné, že takéto sprístupnenie je v rozpore s ochranou dôležitých protikladných verejných záujmov, ako je napríklad národná bezpečnosť; obrana; alebo verejná bezpečnosť. Okrem toho, ak sa osobné informácie spracúvajú výlučne na účely výskumu alebo štatistiky, môže byť prístup zamietnutý. Iné dôvody na zamietnutie alebo obmedzenie prístupu k osobným informáciám sú:
 - 1. ovplyvnenie výkonu alebo presadzovania práva alebo občianskoprávneho konania, vrátane prevencie, vyšetrovania alebo odhaľovania trestných činov, alebo práva na spravodlivý proces;
 - 2. sprístupnenie, pri ktorom by sa porušili legitímne práva alebo dôležité záujmy iných osôb;
 - 3. porušovanie zákonnej alebo inej profesionálnej výsady alebo povinnosti;
 - 4. ovplyvňovanie vyšetrovania bezpečnosti pri práci alebo konania vo veci pracovných sťažností alebo v súvislosti s plánovaním zmien v obsadzovaní funkcií v rámci určitej spoločnosti a s reorganizáciou určitej spoločnosti; alebo
 - 5. porušenie potrebnej dôvernosti v súvislosti s monitorovaním, kontrolou alebo regulačnými funkciami súvisiacimi s dobrým hospodárskym alebo finančným riadením, alebo porušovanie dôvernosti budúcich alebo prebiehajúcich rokovaní s účasťou organizácie.
- ii) Organizácia, ktorá si nárokuje výnimku má povinnosť preukázať jej nevyhnutnosť a uviesť dôvody na obmedzenie prístupu a kontaktné miesto, na ktoré sa môžu fyzické osoby obrátiť v prípade ďalších otázok.

f) Právo na získanie potvrdenia a účtovanie poplatkov na pokrytie nákladov súvisiacich s poskytnutím prístupu

- i) Jednotlivec má právo získať potvrdenie o tom, či daná organizácia má alebo nemá osobné údaje, ktoré sa ho týkajú. Jednotlivec má tiež právo získať takéto osobné údaje, ktoré sa ho týkajú. Organizácia môže účtovať poplatok, ktorý nie je neprimerane vysoký.
- ii) Účtovanie poplatku môže byť opodstatnené napríklad v prípade zjavne neprimeraných žiadostí o prístup, najmä z dôvodu ich opakujúceho sa charakteru.
- iii) Prístup nemôže byť zamietnutý z dôvodu nákladov, ak príslušný jednotlivec ponúka zaplatať náklady.

g) Opakované alebo obťažujúce žiadosti o prístup

Organizácia môže primerane obmedziť počet prípadov, v ktorých sa v rámci určitého časového obdobia vyhovie žiadostiam určitého jednotlivca o prístup. Pri stanovovaní takýchto obmedzení by organizácia mala zohľadniť také faktory ako frekvencia, s akou sa informácie aktualizujú, účel, na ktorý sa dané údaje využívajú, a povaha daných informácií.

h) Podvodné žiadosti o prístup

Organizácia nemusí poskytnúť prístup k osobným informáciám, pokiaľ jej nie sú predložené dostatočné informácie, ktoré jej umožnia potvrdiť totožnosť osoby, ktorá podáva žiadosť.

i) Časový rámec na odpovede

Organizácie by mali odpovedať na žiadosti o prístup v primeranej lehote, vhodným spôsobom a vo forme, ktorá je pre fyzickú osobu zrozumiteľná. Organizácia, ktorá pravidelne poskytuje údaje dotknutým osobám, môže splniť žiadosť jednotlivca o prístup prostredníctvom pravidelného zverejňovania, ak by to nespôsobilo nadmerné oneskorenie.

9. Údaje o ľudských zdrojoch

a) Rozsah pôsobnosti štítu na ochranu osobných údajov

- i) Ak organizácia z EÚ prenáša osobné informácie o svojich zamestnancoch (bývalých alebo súčasných) zhromaždené v súvislosti s pracovnoprávnym vzťahom do materskej, sesterskej alebo nesesterskej spoločnosti, ktorá poskytuje služby v Spojených štátoch a ktorá je zapojená do štítu na ochranu osobných údajov, na daný prenos sa vzťahujú výhody vyplývajúce zo štítu na ochranu osobných údajov. V takýchto prípadoch zhromažďovanie informácií a ich spracúvanie pred prenosom podlieha vnútroštátnym právnym predpisom krajiny EÚ, v ktorej boli dané informácie zhromaždené, a musia byť rešpektované akékoľvek podmienky alebo obmedzenia vo vzťahu k prenosu týchto informácií stanovené týmito predpismi.
- ii) Zásady štítu na ochranu osobných údajov sú relevantné len vtedy, keď sa prenášajú individuálne identifikované alebo identifikovateľné záznamy alebo keď sa poskytuje prístup k takýmto záznamom. Štatistické výkazy založené na súhrnných údajoch o zamestnancoch, ktoré neobsahujú žiadne osobné údaje, a využívanie anonymizovaných údajov nepredstavujú ohrozenie súkromia.

b) Uplatňovanie zásad oznámenia a možnosti voľby

- i) Organizácia v USA, ktorá získala informácie týkajúce sa zamestnancov z EÚ v rámci štítu na ochranu osobných údajov, môže tieto informácie poskytnúť tretím stranám alebo ich využívať na rôzne účely len v súlade so zásadami oznámenia a možnosti voľby. Napríklad v prípade, že chce organizácia využiť osobné informácie zhromaždené v rámci pracovnoprávného vzťahu na účely nesúvisiace s pracovnoprávnymi vzťahmi, ako napríklad na marketingovú komunikáciu, daná organizácia v USA musí pred tým, než tak urobí, poskytnúť dotknutým fyzickým osobám možnosť voľby, pokiaľ tieto fyzické osoby už nedali svoj súhlas na využitie daných informácií na takéto účely. Také použitie musí byť zlučiteľné s účelmi, na ktoré boli osobné informácie zhromaždené alebo následne schválené daným jednotlivcom. Navyše, takáto možnosť voľby sa nesmie použiť na obmedzenie pracovných príležitostí alebo na represívne konanie voči takýmto zamestnancom.

- ii) Treba podotknúť, že určité všeobecne uplatniteľné podmienky na prenos z niektorých členských štátov EÚ môžu vylučovať iné možnosti využitia takýchto informácií dokonca aj po prenose mimo EÚ a takéto podmienky sa budú musieť rešpektovať.
- iii) Navyše, zamestnávateľia by mali vynaložiť primerané úsilie na to, aby vyhověli preferenciám zamestnancov, pokiaľ ide o ochranu súkromia. To by napríklad mohlo znamenať obmedzenie prístupu k osobným údajom, anonymizovanie určitých údajov alebo pridelenie kódov alebo pseudonymov v prípadoch, keď sa na účely riadenia nevyhnutne nevyžadujú skutočné mená.
- iv) Organizácia nemusí poskytnúť oznámenie a možnosť voľby v miere a v lehote potrebnej na to, aby nebola dotknutá schopnosť organizácie uskutočňovať povýšenia, menovania alebo prijímať iné podobné pracovno-právne rozhodnutia.

c) Uplatňovanie zásady prístupu

Doplňková zásada týkajúca sa prístupu poskytuje usmernenie, pokiaľ ide o dôvody, ktoré môžu opodstatňovať zamietnutie alebo obmedzenie prístupu na požiadanie v súvislosti s ľudskými zdrojmi. Zamestnávateľia v Európskej únii musia prirodzene dodržiavať miestne právne predpisy a zabezpečiť, aby mali zamestnanci v rámci Európskej únie prístup k takýmto informáciám, tak ako to vyžaduje právo v ich domovských krajinách bez ohľadu na to, na akom mieste sa údaje spracúvajú a uchovávajú. Podľa zásad štítu na ochranu osobných údajov sa vyžaduje, aby organizácia, ktorá spracúva takéto údaje v Spojených štátoch, spolupracovala pri poskytovaní takéhoto prístupu buď priamo, alebo prostredníctvom zamestnávateľa v EÚ.

d) Presadzovanie

- i) Pokiaľ sa osobné informácie využívajú len v rámci pracovnoprávných vzťahov, prvotnú zodpovednosť za údaje vo vzťahu k zamestnancovi nesie organizácia v EÚ. To znamená, že ak európski zamestnanci podajú sťažnosti týkajúce sa porušovania ich práv na ochranu údajov a nie sú spokojní s výsledkami interného posúdenia, konania o sťažnosti a odvolacieho konania (alebo iného postupu na predkladanie sťažností uplatniteľného podľa kolektívnej zmluvy), tieto sťažnosti by sa mali podať na štátny alebo národný orgán pre ochranu osobných údajov alebo na úrad práce, v rámci jurisdikcie ktorých daný zamestnanec pracuje. Týka sa to aj prípadov, keď je za údajné nesprávne zaobchádzanie s osobnými informáciami spomínaných zamestnancov zodpovedná organizácia v USA, ktorá získala dané informácie od zamestnávateľa, čo znamená, že ide o údajné porušenie zásad štítu na ochranu osobných údajov. Toto bude najúčinnjší spôsob riešenia často sa prekrývajúcich práv a povinností ukladaných miestnym pracovným právom a pracovnými dohodami, ako aj právom v oblasti ochrany údajov.
- ii) Organizácia v USA, ktorá sa zapája do štítu na ochranu osobných údajov a ktorá využíva údaje z EÚ týkajúce sa ľudských zdrojov prenášané z Európskej únie v súvislosti s pracovnoprávnym vzťahom a ktorá si praje, aby sa na takéto prenosi vzťahoval štít na ochranu osobných údajov, sa preto musí zaviazat, že v takýchto prípadoch bude spolupracovať pri vyšetrovaniach príslušných orgánov EÚ a že bude dodržiavať odporúčania týchto orgánov.

e) Uplatňovanie zásady zodpovednosti za ďalší prenos

Pokiaľ ide o príležitostné prevádzkové potreby organizácie zapojenej do štítu na ochranu osobných údajov týkajúce sa pracovnoprávných vzťahov so zreteľom na osobné údaje prenášané v rámci štítu na ochranu osobných údajov, ako je napríklad rezervácia leteniek, hotelovej izby alebo poistné krytie, prenosi osobných údajov malého počtu zamestnancov prevádzkovateľom sa môžu vykonávať bez uplatňovania zásady prístupu alebo bez uzavretia zmluvy s prevádzkovateľom, ktorý je treťou stranou, ako sa to vyžaduje v iných prípadoch podľa zásady zodpovednosti za ďalší prenos, ak organizácia zapojená do štítu na ochranu osobných údajov dodržala zásady oznámenia a možnosti voľby.

10. Povinné uzavretie zmlúv pre ďalšie prenosi

a) Zmluvy o spracovaní údajov

- i) Ak sa osobné údaje prenášajú z EÚ do Spojených štátov len na účely spracúvania, zmluva sa bude vyžadovať bez ohľadu na zapojenie spracovateľa do štítu na ochranu osobných údajov.

- ii) Od prevádzkovateľov v Európskej únii sa vždy vyžaduje, aby v prípade, že sa prenos vykonáva len s cieľom spracúvania údajov, uzavreli zmluvu, a to bez ohľadu na to, či sa operácia spracúvania vykonáva v rámci EÚ alebo mimo nej a bez ohľadu na zapojenie spracovateľa do štítu na ochranu osobných údajov. Účelom zmluvy je zabezpečiť, že spracovateľ:

1. koná len na základe pokynov prevádzkovateľa;
2. zabezpečuje zavedenie vhodných technických a organizačných opatrení na ochranu osobných údajov pred náhodným alebo nezákonným zničením, náhodnou stratou, zmenou, neoprávneným zverejnením alebo sprístupnením, a vie, či je povolený ďalší prenos a
3. vzhľadom na povahu spracúvania pomáha prevádzkovateľovi pri odpovedaní fyzickým osobám, ktoré uplatňujú svoje práva na základe zásad.

- iii) Keďže organizácie zapojené do štítu na ochranu osobných údajov poskytujú primeranú ochranu osobných informácií, zmluvy s organizáciami zapojenými do štítu na ochranu osobných údajov týkajúce sa výlučne spracúvania údajov si nevyžadujú predchádzajúci súhlas (alebo takýto súhlas poskytnú členské štáty automaticky), ktorý by sa vyžadoval v prípade zmlúv s príjemcami údajov, ktorí sa nezapájajú do štítu na ochranu osobných údajov alebo iným spôsobom neposkytujú primeranú ochranu osobných informácií.

b) Prenosy v rámci kontrolovanej skupiny spoločností alebo subjektov

Keď sa osobné informácie prenášajú medzi dvoma prevádzkovateľmi v rámci kontrolovanej skupiny spoločností alebo subjektov, podľa zásady týkajúcej sa zodpovednosti za ďalší prenos sa vždy nevyžaduje uzavretie zmluvy. Prevádzkovatelia v rámci kontrolovanej skupiny spoločností alebo subjektov môžu založiť svoje prenosy na iných nástrojoch, ako napríklad na záväzných firemných pravidlách EÚ alebo iných vnútrogrupinových nástrojoch (napr. programy dodržiavania predpisov a kontroly), a zabezpečiť tak kontinuitu ochrany osobných informácií podľa zásad. V prípade takýchto prenosov zostáva organizácia zapojená do štítu na ochranu osobných údajov zodpovedná za dodržiavanie zásad.

c) Prenosy medzi prevádzkovateľmi

V prípade prenosov medzi prevádzkovateľmi nemusí byť prijímajúci prevádzkovateľ organizáciou zapojenou do štítu na ochranu osobných údajov ani nemusí mať nezávislý mechanizmus nápravy. Organizácia zapojená do štítu na ochranu osobných údajov musí uzavrieť zmluvu s prijímajúcim prevádzkovateľom, ktorý je treťou stranou, ktorá zabezpečuje rovnakú úroveň ochrany, aká je dostupná na základe štítu na ochranu osobných údajov, pričom sa nevyžaduje, aby prevádzkovateľ, ktorý je treťou stranou, bol organizáciou zapojenou do štítu na ochranu osobných údajov alebo mal nezávislý mechanizmus nápravy, za predpokladu, že poskytne rovnocenný mechanizmus.

11. Riešenie sporov a presadzovanie práva

- a) Zásada nápravy, presadzovania a zodpovednosti stanovuje požiadavky na presadzovanie štítu na ochranu osobných údajov. Spôsob plnenia požiadaviek písm. a) bodu ii) tejto zásady je stanovený v doplnkovej zásade týkajúcej sa overovania. Táto doplnková zásada sa týka písm. a) bodov i) a iii), v ktorých sa vyžadujú nezávislé mechanizmy nápravy. Tieto mechanizmy môžu mať rôznu podobu, musia však spĺňať požiadavky zásady nápravy, presadzovania a zodpovednosti. Organizácie tieto požiadavky splnia nasledujúcim spôsobom: i) dodržiavaním programov ochrany súkromia vypracovaných súkromným sektorom, ktoré začleňujú do svojich pravidiel zásady štítu na ochranu osobných údajov a ktoré zahŕňujú účinné mechanizmy presadzovania toho druhu, ktorý je opísaný v zásade nápravy, presadzovania a zodpovednosti; ii) podrobením sa zákonným alebo regulačným dozorným orgánom, ktoré zabezpečujú vybavovanie sťažností fyzických osôb a riešenie sporov; alebo iii) tým, že sa zaviazu spolupracovať s orgánmi pre ochranu osobných údajov so sídlom v Európskej únii alebo s ich oprávnenými zástupcami.
- b) Vymenovanie vyššie uvedených spôsobov má ilustratívny a nie obmedzujúci charakter. Súkromný sektor môže zaviesť ďalšie mechanizmy na zabezpečenie presadzovania, pokiaľ tieto mechanizmy budú spĺňať požiadavky zásady nápravy, presadzovania a zodpovednosti a doplnkových zásad. Treba upozorniť na to, že požiadavky

zásady nápravy, presadzovania a zodpovednosti dopĺňajú požiadavky, podľa ktorých musí byť samoregulačné úsilie vymáhateľné podľa oddielu 5 zákona o Federálnej obchodnej komisii, ktorý zakazuje nekalé a klamlivé konanie, alebo podľa podobného právneho predpisu či nariadenia, ktoré zakazuje takúto činnosť.

- c) S cieľom pomôcť zabezpečiť dodržiavanie záväzkov vyplývajúcich zo štítu na ochranu osobných údajov a podporiť správu programu, organizácie aj ich nezávislé mechanizmy nápravy musia ministerstvu na požiadanie poskytnúť informácie týkajúce sa štítu na ochranu osobných údajov. Organizácie musia navyše pohotovo odpovedať na sťažnosti týkajúce sa ich dodržiavania zásad, postúpené DPA prostredníctvom ministerstva. V rámci takejto odpovede by sa malo riešiť, či je sťažnosť opodstatnená, a ak áno, ako organizácia naprávi daný problém. Ministerstvo bude chrániť dôvernosc prijatých informácií v súlade s právom USA.

d) Mechanizmy nápravy

- i) Spotrebiteľia by mali byť nabádaní k tomu, aby pred tým, než sa obrátia na nezávislé mechanizmy nápravy, podali svoje prípadné sťažnosti príslušnej organizácii. Organizácie musia spotrebiteľom odpovedať do 45 dní od prijatia sťažnosti. To, či je určitý mechanizmus nápravy nezávislý, je faktická otázka, ktorú možno zodpovedať najmä preukázaním nestrannosti, transparentnej štruktúry a financovania, ako aj preukázaním predchádzajúcej činnosti. Podľa zásady nápravy, presadzovania a zodpovednosti, musí byť mechanizmus nápravy dostupný pre fyzické osoby ľahko prístupný a bezplatný. Subjekty pre riešenie sporov by mali prešetriť každú sťažnosť, ktorú dostanú od fyzických osôb, pokiaľ tieto sťažnosti nie sú očividne nepodložené alebo neodôvodnené. To však nevylučuje možnosť, že organizácia prevádzkujúca mechanizmus nápravy zavedie požiadavky súvisiace s oprávnenosťou podania sťažnosti, takéto požiadavky však musia byť transparentné a odôvodnené (napríklad požiadavka na vylúčenie sťažností, ktoré nepatria do rámca pôsobnosti daného programu alebo patria na posúdenie inému fóru) a ich výsledkom by nemalo byť narušenie záväzku ohľadom prešetrovania oprávnených sťažností. Okrem toho by mechanizmy nápravy mali fyzickým osobám poskytovať úplné a ľahko dostupné informácie o tom, ako prebieha postup riešenia sporov v prípade, že podajú sťažnosť. Takéto informácie by mali zahŕňať upozornenie na postupy daného mechanizmu v oblasti ochrany súkromia, a to v súlade so zásadami štítu na ochranu osobných údajov. Mechanizmy nápravy by tiež mali spolupracovať na vypracovaní nástrojov, ako napríklad štandardných formulárov na podávanie sťažností, aby tak uľahčili proces riešenia sťažností.
- ii) Nezávislé mechanizmy nápravy musia na svojich verejných webových lokalitách uvádzať informácie týkajúce sa zásad štítu na ochranu osobných údajov a služieb, ktoré poskytujú v rámci štítu na ochranu osobných údajov. Tieto informácie musia zahŕňať: 1. informácie o požiadavkách zásad štítu na ochranu osobných údajov týkajúcich sa nezávislých mechanizmov nápravy alebo odkaz na tieto požiadavky; 2. odkaz na webovú lokalitu ministerstva pre štít na ochranu osobných údajov; 3. vysvetlenie, že ich služby riešenia sporov v rámci štítu na ochranu osobných údajov sú pre fyzické osoby bezplatné; 4. opis spôsobu, akým možno podať sťažnosť týkajúcu sa štítu na ochranu osobných údajov; 5. časový rámec, v ktorom sa spracúvajú sťažnosti týkajúce sa štítu na ochranu osobných údajov a 6. opis škály možných nápravných opatrení.
- iii) Nezávislé mechanizmy nápravy musia zverejňovať výročnú správu so súhrnnými štatistickými údajmi o svojich službách riešenia sporov. Výročná správa musí uvádzať: 1. celkový počet sťažností týkajúcich sa štítu na ochranu osobných údajov prijatých počas vykazovaného roku; 2. typy prijatých sťažností; 3. spôsob merania kvality riešenia sporov, ako napríklad dĺžku obdobia potrebného na spracovanie sťažností a 4. výsledky prijatých sťažností, najmä počet a typy nápravných opatrení alebo uložených sankcií.
- iv) Ako sa stanovuje v prílohe I, fyzické osoby majú k dispozícii možnosť rozhodcovského konania, prostredníctvom ktorého sa v prípade zvyšných nárokov určí, či organizácia zapojená do štítu na ochranu osobných údajov porušila záväzky ktoré má voči fyzickej osobe na základe zásad a či takéto porušenie ostane úplne alebo čiastočne nenapravené. Táto možnosť je dostupná len na tieto účely. Táto možnosť nie je dostupná napríklad v prípade výnimiek zo zásad ⁽¹⁾ alebo v prípade tvrdení o neprimeranosti štítu na ochranu osobných údajov. Podľa tejto možnosti rozhodcovského konania má výbor pre štít na ochranu osobných údajov (zložený z jedného alebo troch rozhodcov, podľa dohody strán) právomoc nariadiť spravodlivú nepenažnú náhradu (ako napríklad prístup, opravu, vymazanie alebo vrátenie predmetných údajov fyzickej osobe) pre konkrétnu fyzickú osobu potrebnú na nápravu porušenia zásad, ktorá sa týka výhradne danej fyzickej osoby. Fyzické osoby a organizácie zapojené do štítu na ochranu osobných údajov budú môcť požiadať o súdne preskúmanie a výkon arbitrážnych rozsudkov podľa práva USA na základe federálneho zákona o rozhodcovskom konaní.

⁽¹⁾ Oddiel I.5 zásad.

e) Nápravné opatrenia a sankcie

Výsledkom akýchkoľvek nápravných opatrení stanovených orgánom na riešenie sporov by malo byť to, že daná organizácia v možnom rozsahu zvráti alebo napraviť nedodržiavanie zásad a to, že ďalšie spracúvanie údajov danou organizáciou bude v súlade so zásadami a v prípadoch, kde je to vhodné, bude ukončené spracúvanie osobných údajov fyzickej osoby, ktorá podala sťažnosť. Sankcie musia byť dostatočne prísne, aby sa zabezpečilo dodržiavanie zásad danou organizáciou. Rozsah sankcií rôzneho stupňa prísnosti umožní orgánom na riešenie sporov primerane reagovať na rozličné stupne nedodržiavania zásad. Sankcie by mali zahŕňať uverejnenie zisteného nedodržiavania zásad, ako aj požiadavku vymazania údajov za určitých okolností⁽¹⁾. Iné sankcie by mohli zahŕňať pozastavenie a odobratie oprávnenia používať pečiatku, kompenzáciu pre fyzické osoby za straty spôsobené v dôsledku nedodržiavania zásad a príkazné opatrenia. Orgány súkromného sektora na riešenie sporov a samoregulačné orgány musia oznámiť prípady, keď organizácie zapojené do štítu na ochranu osobných údajov nerespektujú ich rozhodnutia príslušnému štátnemu orgánu alebo prípadne súdom, a musia informovať ministerstvo.

f) Činnosť Federálnej obchodnej komisie

Federálna obchodná komisia sa zaviazala, že bude prioritne preskúmať podania týkajúce sa údajného nedodržiavania zásad prijaté od: i) samoregulačných orgánov z oblasti ochrany súkromia a iných nezávislých subjektov riešenia sporov; ii) členských štátov EÚ a iii) ministerstva s cieľom určiť, či bol porušený oddiel 5 zákona o Federálnej obchodnej komisii zakazujúci nekalé alebo klamlivé konanie alebo praktiky v rámci obchodovania. Ak Federálna obchodná komisia dospeje k záveru, že má dôvod domnievať sa, že bol porušený oddiel 5, môžu danú vec vyriešiť tak, že bude žiadať príkaz na zdržanie sa konania zakazujúci namietané praktiky alebo tak, že podá sťažnosť na federálny obvodný súd, výsledkom čoho by v prípade úspechu mohol byť príkaz federálneho súdu s tým istým účinkom. To zahŕňa nepravdivé tvrdenia o dodržiavaní zásad štítu na ochranu osobných údajov alebo o účasti v štíte na ochranu osobných údajov zo strany organizácií, ktoré buď už nie sú na zozname organizácií zapojených do štítu na ochranu osobných údajov, alebo ministerstvu nikdy neosvedčili svoje dodržiavanie zásad. Za porušenie administratívneho príkazu na zdržanie sa konania môže FTC uložiť občianskoprávne sankcie a v za porušenie príkazu federálneho súdu môže začať občianskoprávne alebo trestné konanie za pohrdanie súdom. Federálna obchodná komisia oznámi každé prijaté opatrenie ministerstvu. Ministerstvo nabáda iné štátne orgány, aby ho informovali o konečnom vybavení takýchto podaní alebo o iných rozhodnutiach nariaďujúcich dodržiavanie zásad štítu na ochranu osobných údajov.

g) Trvalé nedodržiavanie zásad

- i) Ak určitá organizácia trvale nedodržiava zásady, nemá už ďalej nárok využívať výhody vyplývajúce zo štítu na ochranu osobných údajov. Organizácie, ktoré trvale nedodržiavajú zásady, budú ministerstvom vyradené zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov a musia vrátiť alebo vymazať osobné informácie, ktoré prijali na základe štítu na ochranu osobných údajov.
- ii) Trvalé nedodržiavanie zásad nastane vtedy, keď organizácia, ktorá osvedčila svoje dodržiavanie zásad ministerstvu, odmietne splniť konečné rozhodnutie ktoréhokoľvek samoregulačného orgánu z oblasti ochrany súkromia, nezávislého orgánu na riešenie sporov alebo štátneho orgánu, alebo v prípadoch, keď takýto orgán rozhodne, že určitá organizácia často nedodržiava zásady až do tej miery, že jej tvrdenie o dodržiavaní zásad nie je viac vierohodné. V týchto prípadoch musí daná organizácia okamžite informovať ministerstvo o takýchto skutočnostiach. Ak to neurobí, môže byť žalovateľná podľa zákona o nepravdivých vyhláseniach (18 U.S.C. § 1001). Skutočnosť, že sa organizácia už nezapája do samoregulačného programu súkromného sektora v oblasti ochrany súkromia alebo nevyužíva nezávislý mechanizmus riešenia sporov, ju nezbavuje povinnosti dodržiavať zásady a považovala by sa za trvalé nedodržiavanie zásad.
- iii) Ministerstvo vyradí organizáciu zo zoznamu organizácií zapojených do štítu na ochranu osobných údajov v reakcii na akékoľvek upozornenie o trvalom nedodržiavaní zásad, ktoré dostane od samotnej organizácie, samoregulačného orgánu z oblasti ochrany súkromia alebo iného nezávislého orgánu na riešenie sporov, alebo od štátneho orgánu, ale len po tom, čo ministerstvo najprv 30 dní vopred upozorní danú organizáciu

⁽¹⁾ Orgány na riešenie sporov majú právomoc rozhodovať o tom, za akých okolností uplatnia tieto sankcie. Citlivosť predmetných údajov je jedným z faktorov, ktorý treba zohľadniť pri rozhodovaní o tom, či sa má požadovať vymazanie údajov, ako v prípadoch, keď organizácia zhromaždila, použila alebo zverejnila informácie v očividnom rozpore so zásadami štítu na ochranu osobných údajov.

a dá jej možnosť reagovať. V zozname organizácií zapojených do štítu na ochranu osobných údajov vedenom ministerstvom bude tiež jasne uvedené, ktoré organizácie majú zabezpečené a ktoré organizácie už nemajú zabezpečené výhody vyplývajúce zo štítu na ochranu osobných údajov.

- iv) Organizácia, ktorá podáva žiadosť o účasť na samoregulačnom orgáne s cieľom opätovného splnenia kritérií štítu na ochranu osobných údajov musí poskytnúť tomuto orgánu úplné informácie o svojom predchádzajúcom zapojení do štítu na ochranu osobných údajov.

12. Možnosť voľby – Časové súvislosti vyjadrenia nesúhlasu s využívaním osobných informácií („Opt out“)

- a) Vo všeobecnosti je cieľom zásady možnosti voľby zabezpečiť, aby sa osobné informácie využívali a poskytovali spôsobmi, ktoré sú zlučiteľné s očakávaniami a rozhodnutiami danej fyzickej osoby. To znamená, že jednotlivec by mal mať možnosť vyjadriť nesúhlas (alebo súhlas) s tým, či sa majú jeho osobné informácie využiť na priamy marketing, a to kedykoľvek, s ohľadom na primeranú lehotu stanovenú danou organizáciou, ktorú potrebuje napríklad na to, aby vyjadrenie nesúhlasu fyzickej osoby s využívaním jej osobných informácií nadobudlo účinnosť. Organizácia môže tiež požadovať dostatočné informácie na potvrdenie totožnosti jednotlivca požadujúceho ukončenie využívania jeho osobných informácií. V Spojených štátoch môžu fyzické osoby uplatniť túto možnosť voľby prostredníctvom využitia relevantného centrálného programu, ako je služba poštových preferencií (Mail Preference Service) Združenia priameho marketingu (Direct Marketing Association). Organizácie, ktoré sa zúčastňujú na službe poštových preferencií Združenia priameho marketingu by mali podporovať jej dostupnosť pre spotrebiteľov, ktorí si neželajú dostávať komerčné informácie. V každom prípade by jednotlivec mal mať k dispozícii ľahko dostupný a z hľadiska výdavkov prístupný mechanizmus na využitie tejto možnosti.
- b) Podobne môže organizácia využívať informácie na určité priame marketingové účely, keď nie je prakticky možné poskytnúť fyzickej osobe príležitosť vyjadriť nesúhlas pred použitím daných informácií, ak daná organizácia zároveň (a kedykoľvek na požiadanie) poskytne fyzickej osobe takúto možnosť zamietnuť (bez toho, že by fyzickej osobe vznikli nejaké náklady), aby mu boli doručované akékoľvek ďalšie priame marketingové oznamy a ak organizácia vyhovie želaniu danej fyzickej osoby.

13. Cestovné informácie

- a) Informácie týkajúce sa rezervácií v rámci osobnej leteckej dopravy a iné informácie týkajúce sa cestovania, ako napríklad informácie o osobách často využívajúcich letecké služby alebo informácie o hotelových rezerváciách a zvláštnych požiadavkách na zaobchádzanie, ako napríklad o jedle zodpovedajúcom náboženským požiadavkám alebo o potrebe fyzickej pomoci možno organizáciám so sídlom mimo EÚ prenášať vo viacerých odlišných prípadoch. Podľa článku 26 smernice je možné prenášať osobné údaje „do tretej krajiny, ktorá nezabezpečuje primeranú úroveň ochrany v zmysle článku 25 ods. 2“ za podmienky, že i) je potrebné poskytnúť služby požadované zákazníkom alebo splniť podmienky dohody, ako napríklad dohody uzavretej s „osobou často využívajúcou letecké služby“; alebo ii) že na to dal zákazník výslovný súhlas. Organizácie v USA zapojené do štítu na ochranu osobných údajov poskytujú primeranú ochranu osobných údajov, a preto im môžu byť prenášané údaje z EÚ bez toho, aby splňali tieto podmienky alebo iné podmienky stanovené v článku 26 smernice. Keďže štít na ochranu osobných údajov zahŕňa osobitné pravidlá týkajúce sa citlivých informácií, takéto informácie (ktoré je potrebné zhromažďovať napríklad v súvislosti s tým, že zákazníci potrebujú fyzickú pomoc) je možné zahrnúť do prenosov informácií účastníkom štítu na ochranu osobných údajov. Vo všetkých prípadoch však musí organizácia prenášajúca dané informácie rešpektovať právo členského štátu EÚ, v ktorom vyvíja činnosť, ktoré môže okrem iného ukladať osobitné podmienky pre narábanie s citlivými údajmi.

14. Farmaceutické výrobky a liečivá

- a) Uplatňovanie právnych predpisov členského štátu EÚ alebo zásad štítu na ochranu osobných údajov

Právne predpisy členských štátov EÚ sa vzťahujú na zhromažďovanie osobných údajov a na akékoľvek spracúvanie, ktoré sa vykonáva pred prenosom do Spojených štátov. Zásady štítu na ochranu osobných údajov sa na tieto údaje vzťahujú po tom, ako sa prenesú do Spojených štátov. Ak je to vhodné, údaje využívané na farmaceutický výskum a iné účely by mali byť anonymizované.

b) Budúci vedecký výskum

- i) Osobné údaje získané v rámci osobitných lekárskech alebo farmaceutických výskumných štúdií hrajú často významnú úlohu v ďalšom vedeckom výskume. Ak sa osobné údaje zhromaždené v rámci jednej výskumnej štúdie prenesú organizácii v USA, ktorá je účastníkom štítu na ochranu osobných údajov, táto organizácia môže využívať dané údaje v rámci nového vedeckého výskumu, ak sa pri prvej štúdii poskytne oznámenie a možnosť voľby. Takéto oznámenie by malo poskytnúť informácie o akomkoľvek budúcom osobitnom využití daných údajov, ako napríklad následnom využívaní v pravidelných intervaloch, v súvisiacich štúdiách alebo v marketingu.
- ii) Je zrejmé, že nie je možné presne vymedziť všetky budúce možnosti využitia daných údajov, pretože nový výskum môže byť podnietený novými pohľadmi na pôvodné údaje, na základe nových objavov a pokroku v medicíne a na základe vývoja v oblasti zdravotníctva a regulačného systému. Tam, kde je to vhodné, by preto oznámenie malo obsahovať vysvetlenie, že osobné údaje môžu byť použité v rámci aktivít budúceho lekárskeho a farmaceutického výskumu, ktoré nemožno vopred predvídať. Ak využívanie údajov nie je zlučiteľné s hlavným účelom (účelmi) výskumu, na ktorý boli dané údaje pôvodne zhromaždené alebo na ktorý dal jednotlivec následne súhlas, je potrebné získať nový súhlas.

c) Rozhodnutie nezúčastniť sa na klinickej štúdii

Účastníci sa môžu kedykoľvek rozhodnúť nezúčastňovať sa ďalej na klinickej štúdii alebo môžu byť o to kedykoľvek požiadaní. Všetky osobné údaje zhromaždené pred skončením účasti na štúdii môžu byť naďalej spracúvané spolu s inými údajmi zhromaždenými v rámci klinickej štúdie, avšak len vtedy, ak to bolo objasnené príslušnému účastníkovi v oznámení v čase, keď súhlasil s účasťou.

d) Prenosy na účely regulácie a dohľadu

Farmaceutické spoločnosti alebo spoločnosti vyrábajúce zdravotnícke pomôcky majú povolené poskytovať osobné údaje z klinických štúdií uskutočnených v EÚ regulačným orgánom v Spojených štátoch s cieľom regulácie alebo dohľadu. Podobné prenosy sa môžu uskutočňovať aj iným stranám než regulačným orgánom, ako napríklad na iné miesta, kde má určitá spoločnosť prevádzky, a iné vedecké pracoviská, v súlade so zásadami oznámenia a možnosti voľby.

e) Slepé štúdie

- i) V záujme zabezpečenia objektivity pri mnohých klinických skúškach nemôže byť účastníkom a často ani výskumníkom poskytnutý prístup k informáciám o tom, akým liečebným metódam sú podrobení jednotliví účastníci. Ak by bol takýto prístup umožnený, ohrozila by sa platnosť príslušnej výskumnej štúdie a jej výsledkov. Účastníkom v takýchto klinických skúškach (ďalej len „skrytý výskum“) sa nemusí poskytnúť prístup k údajom o ich liečbe počas štúdie, ak im takéto obmedzenie bolo vysvetlené vtedy, keď sa účastník rozhodoval o účasti na skúške a keby odhalenie takýchto informácií ohrozilo integritu príslušného výskumu.
- ii) Súhlas s účasťou na určitej štúdii za týchto podmienok je vlastne zrieknutím sa práva na prístup k spomínaným informáciám. Po ukončení skúšky a analýze výsledkov by účastníci mali mať prístup k svojim údajom, ak oň požiadajú. Mali by ich v prvom rade žiadať od lekára alebo iného poskytovateľa zdravotnej starostlivosti, ktorý im poskytol ošetrovanie v rámci klinickej skúšky alebo následne od sponzorujúcej organizácie.

f) Bezpečnosť výrobkov a monitorovanie účinnosti

Farmaceutická spoločnosť alebo spoločnosť vyrábajúca zdravotnícke pomôcky nemusí uplatňovať zásady štítu na ochranu osobných údajov, pokiaľ ide o zásady oznámenia, možnosti voľby, zodpovednosti za ďalší prenos a prístup v rámci svojich aktivít monitorovania bezpečnosti výrobkov a účinnosti, vrátane podávania správ o nepriaznivých prípadoch a sledovania stavu pacientov/subjektov užívajúcich určité lieky alebo používajúcich zdravotnícke pomôcky, pokiaľ je dodržiavanie zásad v rozpore s dodržiavaním regulačných požiadaviek. Platí to tak vo vzťahu k správam poskytovaným napríklad poskytovateľmi zdravotnej starostlivosti farmaceutickým

spoločnostiam alebo spoločnostiam vyrábajúcim zdravotnícke pomôcky, ako aj vo vzťahu k správam poskytovaným farmaceutickými spoločnosťami a spoločnosťami vyrábajúcimi zdravotnícke pomôcky vládny organizáciám ako napríklad Americký úrad pre potraviny a lieky.

g) Kľúčom kódované údaje

Výskumné údaje hlavný vedúci pracovník výskumu vždy zakóduje v ich pôvodnom stave osobitným kľúčom, aby sa neodhalila totožnosť jednotlivých dotknutých osôb. Farmaceutickým spoločnostiam sponzorujúcim takýto výskum sa tento kľúč neposkytne. Tento osobitný kľúčový kód má k dispozícii len spomínaný výskumný pracovník, aby mohol/mohla za určitých okolností identifikovať osobu, ktorá je predmetom výskumu (napríklad v prípade, že je potrebná následná lekárska starostlivosť). Prenos takto zakódovaných údajov z EÚ do Spojených štátov nepredstavuje prenos osobných údajov podliehajúcich zásadám štítu na ochranu osobných údajov.

15. Verejné záznamy a verejne dostupné informácie

- a) Organizácia musí v prípade údajov z verejne dostupných zdrojov uplatňovať zásady štítu na ochranu osobných údajov, ktoré sa týkajú bezpečnosti, integrity údajov a obmedzenia účelu, ako aj nápravy, presadzovania a zodpovednosti. Tieto zásady sa vzťahujú aj na osobné údaje zhromaždené z verejných záznamov, t. j. tých záznamov, ktoré uchovávajú štátne orgány alebo právnické osoby na akejkoľvek úrovni, do ktorých môže verejnosť vo všeobecnosti nahliadať.
- b) Zásady oznámenia, možnosti voľby alebo zodpovednosti za ďalší prenos nie je potrebné uplatňovať na informácie obsiahnuté vo verejných záznamoch, pokiaľ nie sú kombinované s informáciami obsiahnutými v neverejných záznamoch a pokiaľ sa rešpektujú všetky podmienky týkajúce sa potreby nahliadania stanovené príslušnou jurisdikciou. Vo všeobecnosti tiež nie je potrebné uplatňovať zásady oznámenia, možnosti voľby alebo zodpovednosti za ďalší prenos na verejne dostupné informácie, pokiaľ subjekt z EÚ prenášajúci dané údaje neuvedie, že takéto informácie podliehajú obmedzeniam, ktoré vyžadujú, aby daná organizácia na zamýšľané účely využívania týchto informácií uplatňovala vyššie uvedené zásady. Organizácie nebudú zodpovedné za to, ako takéto informácie využívajú tí, ktorí ich získali z uverejnených materiálov.
- c) Keď sa zistí, že určitá organizácia zámerne zverejnila osobné informácie v rozpore so zásadami, aby mohla, resp. aby iní mohli využívať výhody vyplývajúce z týchto výnimiek, prestane spĺňať kritériá na využívanie výhod vyplývajúcich zo štítu na ochranu osobných údajov.
- d) Na informácie z verejných záznamov nie je potrebné uplatňovať zásadu prístupu, pokiaľ nie sú kombinované s inými osobnými informáciami (s výnimkou malých množstiev informácií používaných na zaradenie alebo organizovanie informácií vo verejných záznamoch); je však potrebné rešpektovať všetky podmienky nahliadania stanovené príslušnou jurisdikciou. Naopak v prípadoch, keď sú informácie z verejných záznamov kombinované s inými informáciami z neverejných záznamov (iných ako tie, ktoré boli osobitne uvedené vyššie), organizácia musí poskytnúť prístup ku všetkým takýmto informáciám za predpokladu, že nepodliehajú iným povoleným výnimkám.
- e) Podobne ako pri informáciách z verejných záznamov nie je potrebné poskytovať prístup k informáciám, ktoré už sú verejne dostupné širokej verejnosti, pokiaľ nie sú kombinované s informáciami, ktoré nie sú verejne dostupné. To znamená, že organizácie, ktorých predmetom podnikania je predaj verejne dostupných informácií, môžu pri odpovedaní na žiadosti o prístup k osobným informáciám účtovať obvyklý poplatok danej organizácie. Fyzické osoby sa môžu prípadne pokúsiť získať prístup k informáciám o sebe u organizácií, ktoré pôvodne zhromaždili dané údaje.

16. Žiadosti o prístup zo strany orgánov verejnej moci

- a) S cieľom zabezpečiť transparentnosť vo vzťahu k oprávneným žiadostiam o prístup k osobným informáciám zo strany orgánov verejnej moci môžu organizácie zapojené do štítu na ochranu osobných údajov dobrovoľne vydávať pravidelné správy o transparentnosti týkajúce sa počtu žiadostí o osobné informácie, ktoré prijali od orgánov verejnej moci z dôvodov presadzovania práva alebo vnútroštátnej bezpečnosti, pokiaľ je takéto zverejnenie povolené na základe platných právnych predpisov.

- b) Informácie, ktoré organizácie zapojené do štítu na ochranu osobných údajov poskytujú v týchto správach, spolu s informáciami poskytnutými spravodajskými službami a ďalšími informáciami možno použiť na informovanie v rámci každoročného spoločného preskúmania fungovania štítu na ochranu osobných údajov v súlade s jeho zásadami.
 - c) Absencia oznámenia v súlade s písm. a) bodom xii) zásady o oznámení nebráni organizácii odpovedať na akúkoľvek zákonnú požiadavku ani neovplyvní jej schopnosť odpovede v tomto smere.
-

*Príloha I***Arbitrážny model**

V tejto prílohe I sú uvedené podmienky, podľa ktorých sú organizácie zapojené do štítu na ochranu osobných údajov povinné rozhodovať o nárokoch podľa zásady nápravy, presadzovania práva a zodpovednosti. Možnosť záväzného rozhodcovského konania opísaná nižšie sa vzťahuje na určité „zostatkové“ pohľadávky týkajúce sa údajov v rámci štítu na ochranu osobných údajov medzi EÚ a USA. Zmyslom tejto možnosti je zabezpečiť rýchly, nezávislý a spravodlivý mechanizmus, podľa rozhodnutia jednotlivca, na riešenie údajných porušení zásad, ktoré neboli vyriešené prostredníctvom žiadnych iných mechanizmov štítu na ochranu osobných údajov.

A. Rozsah

Táto možnosť rozhodcovského konania je k dispozícii pre jednotlivcov na určenie, či organizácia zapojená do štítu na ochranu osobných údajov v prípade zostatkových pohľadávok porušila svoje záväzky voči jednotlivcovi v súvislosti so zásadami a či takéto porušenie ostalo úplne alebo čiastočne nenapravené. Táto možnosť je dostupná len na tieto účely. Táto možnosť nie je k dispozícii napríklad v prípade výnimiek zo zásad ⁽¹⁾ alebo v prípade tvrdení o neprimeranosti štítu na ochranu osobných údajov.

B. Dostupné prostriedky nápravy

Podľa tejto možnosti rozhodcovského konania má výbor pre štít na ochranu osobných údajov (zložený z jedného alebo troch rozhodcov, podľa dohody strán) právomoc nariadiť konkrétnu, nepeňažnú spravodlivú náhradu (ako napríklad prístup, opravu, vymazanie alebo vrátenie predmetných údajov jednotlivca) potrebnú pre nápravu porušenia zásad, ktorá sa týka výhradne jednotlivca. Toto sú jediné právomoci arbitrážneho výboru týkajúce sa nápravných prostriedkov. Pri zvažovaní prostriedkov nápravy musí arbitrážny výbor zohľadniť iné prostriedky nápravy, ktoré už boli uložené inými mechanizmami v rámci štítu na ochranu osobných údajov. Nie sú k dispozícii žiadne náhrady škody, nákladov, poplatkov alebo iné prostriedky nápravy. Každá strana znáša svoje vlastné náklady na právneho zástupcu.

C. Predarbitrážne požiadavky

Jednotlivec, ktorý sa rozhodne uplatniť možnosť rozhodcovského konania, musí pred začiatkom arbitrážneho nároku vykonať tieto kroky: 1. predložiť údajné porušenie zásad priamo organizácii a poskytnúť jej možnosť vyriešiť problém v lehote stanovenej v oddiele III.11 písm. d) bode i) zásad; 2. využiť nezávislý mechanizmus nápravy podľa zásad, ktorý je jednotlivcovi bezplatne k dispozícii a 3. predložiť tento problém svojmu orgánu na ochranu údajov, ktorý ho postúpi ministerstvu obchodu, a poskytnúť ministerstvu obchodu príležitosť vynaložiť maximálne úsilie na vyriešenie problému v časovom rámci stanovenom v liste správy zahraničného obchodu z ministerstva obchodu, a to bez akýchkoľvek nákladov pre jednotlivca.

Táto možnosť rozhodcovského konania sa nesmie uplatniť, ak to isté údajné porušenie zásad 1. bolo už predtým predmetom záväzného rozhodcovského konania; 2. bolo predmetom právoplatného rozsudku vyneseného v súdnom konaní, v ktorom bol jednotlivec jednou zo strán, alebo 3. bolo predtým vysporiadané oboma stranami. Táto možnosť sa okrem toho nemôže uplatniť, ak orgán EÚ na ochranu údajov 1. má právomoc podľa oddielov III.5 alebo III.9 zásad alebo 2. má právomoc vyriešiť údajné porušenie priamo s organizáciou. Právomoc DPA na riešenie rovnakého nároku voči prevádzkovateľovi v EÚ nebráni uplatneniu tejto možnosti rozhodcovského konania voči odlišnej právnickej osobe, ktorá nie je viazaná právomocou DPA.

D. Záväzný charakter rozhodnutí

Rozhodnutie jednotlivca uplatniť túto možnosť záväzného rozhodcovského konania je úplne dobrovoľné. Arbitrážne rozhodnutia budú záväzné pre všetky strany rozhodcovského konania. Keď sa raz uplatní, jednotlivec sa vzdáva možnosti požadovať náhradu za to isté údajné porušenie v inom fóre, s výnimkou prípadu, že ak nepeňažná spravodlivá náhrada nie je úplne uspokojivým nápravným prostriedkom pre takéto porušenie, uplatnenie rozhodcovského konania zo strany jednotlivca nebude brániť nároku na náhradu škody, ktorý je inak dostupný na súdoch.

⁽¹⁾ Oddiel I.5 zásad.

E. Preskúmanie a výkon

Jednotlivci a organizácie zapojené do štítu na ochranu osobných údajov budú môcť požiadať o súdne preskúmanie a výkon arbitrážnych rozsudkov podľa práva USA v rámci zákona o federálnej arbitráži ⁽¹⁾. Akékoľvek takéto prípady sa musia predložiť na federálny okresný súd, ktorého územné pokrytie zahŕňa hlavné miesto podnikania organizácie zapojenej do štítu na ochranu osobných údajov.

Účelom tejto možnosti rozhodcovského konania je riešiť individuálne spory a arbitrážne rozhodnutia nemajú plniť funkciu presvedčivého alebo záväzného precedensu vo veciach týkajúcich sa ostatných strán vrátane budúcich rozhodcovských konaní na súdoch EÚ alebo USA alebo konaní Federálnej obchodnej komisie.

F. Arbitrážny výbor

Strany si zvolia rozhodcov z príslušného zoznamu opísaného nižšie.

Ministerstvo obchodu USA a Európska komisia v súlade s platnými právnymi predpismi vypracujú zoznam aspoň 20 rozhodcov na základe nezávislosti, integrity a odborných znalostí. V súvislosti s týmto postupom sa uplatňujú tieto pravidlá:

Rozhodcovia:

1. zostanú uvedení na zozname počas obdobia 3 rokov, ak nenastanú výnimočné okolnosti alebo príčiny, s možnosťou predĺženia o ďalšie 3 roky;
2. nebudú sa riadiť žiadnymi pokynmi ani nebudú spojení so žiadnou stranou alebo organizáciou zapojenou do štítu na ochranu osobných údajov, ani USA, EÚ alebo ktorýmkoľvek členským štátom EÚ, ani so žiadnym iným vládny orgánom, orgánom verejnej moci alebo orgánom na presadzovanie práva a
3. musia byť oprávnení vykonávať advokátsku prax v USA a byť odborníkmi v oblasti práva USA na ochranu súkromia s odbornými znalosťami zákonov EÚ z oblasti ochrany údajov.

G. Rozhodcovské konania

Ministerstvo obchodu a Európska komisia sa v súlade s platnými právnymi predpismi do 6 mesiacov od prijatia rozhodnutia o primeranosti dohodnú o prijatí existujúceho zaužívaného súboru rozhodcovských konaní USA (ako napríklad AAA alebo JAMS) s cieľom riadiť konania pred výborom pre štít na ochranu osobných údajov, na základe týchto podmienok:

1. Jednotlivec môže začať záväzné rozhodcovské konanie za predpokladu, že sú splnené predarbitrážne podmienky uvedené vyššie, dorúčením „oznámenia“ organizácii. Toto oznámenie musí obsahovať zhrnutie krokov, ktoré boli prijaté podľa časti C s cieľom vyriešiť nárok, opis údajného porušenia a na základe rozhodnutia jednotlivca aj akékoľvek podkladové dokumenty a materiály a/alebo diskusiu o právnych predpisoch týkajúcich sa údajného nároku.

⁽¹⁾ V kapitole 2 zákona o federálnej arbitráži (ďalej len „FAA“) sa stanovuje, že „rozhodcovská dohoda alebo rozhodcovské rozhodnutie, ktoré vyplývajú z právneho vzťahu, či už zmluvného alebo nie, ktorý sa považuje za obchodnú zmluvu, vrátane transakcie, alebo dohodu opísanú v [oddiele 2 zákona FAA], patrí do rozsahu pôsobnosti dohovoru [o uznaní a výkone cudzích rozhodcovských rozhodnutí z 10. júna 1958, 21 U.S.T. 2519, T.I.A.S. č. 6997 (ďalej len „Newyorský dohovor“)]“ (9 U.S.C. § 202). V zákone FAA sa ďalej stanovuje, že „dohoda alebo rozhodnutie, ktoré vyplýva z takéhoto vzťahu, ktorý je výlučne medzi občanmi Spojených štátov, sa považuje za nepatriacu do rozsahu pôsobnosti [Newyorského] dohovoru, pokiaľ takýto vzťah nezahŕňa majetok nachádzajúci sa v zahraničí, neplánuje sa výkon alebo presadzovanie práva v zahraničí alebo nemá žiadny iný primeraný vzťah s jedným alebo viacerými cudzími štátmi“ (tamtiež). Podľa kapitoly 2, „ktorákoľvek strana rozhodcovského konania môže podať návrh na ktorýkoľvek súd, ktorý má podľa tejto kapitoly jurisdikciu, na príkaz potvrdzujúci rozhodnutie voči ktorejkoľvek inej strane rozhodcovského konania. Súd potvrdí rozhodnutie, pokiaľ nezistí jediný dôvod odmietnutia alebo odkladu uznania či výkonu rozhodnutia uvedeného v spomínanom [Newyorskom] dohovore“ (tamtiež, § 207). V kapitole 2 sa ďalej stanovuje, že „okresné súdy Spojených štátov... majú pôvodnú jurisdikciu rozhodovať o... žalobe alebo konaní [podľa Newyorského dohovoru], a to bez ohľadu na spornú časť“ (tamtiež, § 203).

V kapitole 2 sa tiež stanovuje, že „kapitola 1 sa vzťahuje na žaloby a konania zahrnuté v tejto kapitole, pokiaľ daná kapitola nie je v rozpore s touto kapitolou alebo [Newyorským] dohovorm ratifikovaným Spojenými štátmi“ (tamtiež, § 208). V kapitole 1 sa stanovuje, že „písomné ustanovenie v... zmluve, ktoré potvrdzuje obchodnú transakciu na urovanie sporu vyplývajúceho z takejto zmluvy alebo transakcie prostredníctvom rozhodcovského konania, alebo odmietnutie vykonať celú alebo ktorúkoľvek časť z neho, alebo písomnej dohody na predloženie existujúceho sporu vyplývajúceho z takejto zmluvy, transakcie alebo odmietnutia rozhodcovského konania, je platné, neodvolateľné a vymáhateľné s výnimkou prípadov existujúcich podľa zákona a vlastného kapitálu pre zrušenie akejkoľvek zmluvy“ (tamtiež, § 2). V kapitole 1 sa ďalej stanovuje, že „ktorákoľvek strana rozhodcovského konania sa môže obrátiť na určený súd v súvislosti s príkazom na potvrdenie rozhodnutia, následkom čoho súd udeliť takýto príkaz, pokiaľ sa rozhodnutie nezruší, nezmení alebo neopraví, ako sa to stanovuje v oddieloch 10 a 11 [zákona FAA]“ (tamtiež, § 9).

2. Vypracujú sa postupy, aby sa zaistilo, že to isté údajné porušenie jednotlivca nebude spojené s duplicitnými prostriedkami nápravy alebo konaniami.
3. Súbežne s rozhodcovským konaním môže prebiehať činnosť Federálnej obchodnej komisie.
4. Na týchto rozhodcovských konaniach sa nesmie zúčastniť žiadny zástupca USA, EÚ alebo ktoréhokoľvek členského štátu EÚ alebo iného vládneho orgánu, orgánu verejnej moci alebo orgánu na presadzovanie práva, pričom DPA v EÚ môžu na žiadosť jednotlivca z EÚ poskytovať pomoc jedine v rámci vypracovania oznámenia, ale DPA v EÚ nesmú mať prístup k zisteniu alebo akýmkoľvek iným materiálom týkajúcim sa týchto rozhodcovských konaní.
5. Rozhodcovské konanie prebieha v Spojených štátoch a jednotlivec si môže vybrať spôsob účasti prostredníctvom videokonferencie alebo telefónu, ktoré sa jednotlivcovi poskytnú bezplatne. Nebude sa vyžadovať osobná účasť.
6. Jazykom rozhodcovského konania bude angličtina, pokiaľ sa strany nedohodnú inak. Na základe odôvodnenej žiadosti a pri zohľadnení skutočnosti, či jednotlivec zastupuje advokát, sa jednotlivcovi na arbitrážnom vypočutí bezplatne poskytnú tlmočnické služby, ako aj preklad arbitrážnych materiálov, pokiaľ výbor nezistí, že za okolností špecifického rozhodcovského konania by to viedlo k neprimeraným alebo neúmerným nákladom.
7. S materiálmi, ktoré sa predložili rozhodcom, sa bude zaobchádzať dôverne a budú sa používať jedine v súvislosti s rozhodcovským konaním.
8. V prípade potreby sa môže povoliť individuálne sprístupnenie zistení, s ktorými budú strany zaobchádzať dôverne a ktoré sa budú používať jedine v súvislosti s rozhodcovským konaním.
9. Rozhodcovské konanie sa ukončí do 90 dní od doručenia oznámenia samotnej organizácii, pokiaľ sa strany nedohodnú inak.

H. Náklady

Rozhodcovia by mali vykonať primerané kroky s cieľom minimalizovať náklady alebo poplatky za rozhodcovské konania.

Ministerstvo obchodu na základe platných právnych predpisov uľahčí po konzultácii s Európskou komisiou zriadenie fondu, do ktorého budú musieť organizácie zapojené do štítu na ochranu osobných údajov odvádzať ročné príspevky, ktoré budú sčasti založené na veľkosti organizácie a ktoré pokryjú náklady rozhodcovského konania, vrátane poplatkov za rozhodcu, až do maximálnych súm („stropov“). Fond bude spravovať tretia strana, ktorá bude pravidelne podávať správy o operáciách fondu. Ministerstvo obchodu a Európska komisia budú v rámci ročného preskúmania hodnotiť činnosť fondu, ako aj potrebu prispôsobiť sumu príspevkov alebo stropov, a okrem iného zväžia počet, náklady a načasovanie rozhodcovských konaní, pričom vzájomne chápu, že organizácie zapojené do štítu na ochranu osobných údajov sa nebudú neprimerane finančne zaťažovať. Náklady na právneho zástupcu nie sú pokryté v tomto ustanovení ani v rámci žiadneho fondu podľa tohto ustanovenia.

PRÍLOHA III

List ministra zahraničných vecí USA Johna Kerryho

7. júla 2016

Vážená pani komisárka Jourová,

som potešený skutočnosťou, že sme dosiahli dohodu v otázke štítu na ochranu osobných údajov medzi Európskou úniou a Spojenými štátmi, ktorý bude zahŕňať mechanizmus ombudsmana, prostredníctvom ktorého budú môcť orgány z EÚ predkladať v mene fyzických osôb žiadosti týkajúce sa postupov signálového spravodajstva USA.

Prezident Barack Obama 17. januára 2014 ohlásil dôležité reformy v spravodajskej oblasti, ktoré sú obsiahnuté v prezidentskej politickej smernici 28 (PPD-28). Na základe smernice PPD-28 som vymenoval tajomníčku ministerstva zahraničných vecí Catherine A. Novelliovú, ktorá je aj hlavnou koordinátorkou medzinárodnej diplomacie v oblasti informačných technológií, za našu kontaktnú osobu pre zahraničné vlády, ktoré chcú vyjadriť znepokojenie týkajúce sa činností signálového spravodajstva USA. Vychádzajúc z tejto úlohy som v súlade s podmienkami stanovenými v prílohe A, ktoré boli aktualizované od môjho listu z 22. februára 2016, vytvoril mechanizmus ombudsmana pre štít na ochranu osobných údajov. Vykonávaním tejto funkcie som poveril tajomníčku ministerstva Novelliovú. Tajomníčka Novelliová je nezávislá od spravodajských služieb USA a podlieha priamo mne.

Svojim zamestnancom som nariadil, aby vyčlenili potrebné zdroje na zavedenie tohto nového mechanizmu ombudsmana a som presvedčený o tom, že to bude účinný nástroj na riešenie obáv osôb z EÚ.

S úctou
John F. Kerry

Príloha A

Mechanizmus ombudsmana pre štít na ochranu osobných údajov medzi EÚ a USA týkajúci sa signálového spravodajstva

Uznávajúc význam rámca štítu na ochranu osobných údajov medzi EÚ a USA sa týmto memorandom stanovuje postup zavedenia nového mechanizmu týkajúceho sa signálového spravodajstva, ktorý je v súlade s prezidentskou politickou smernicou 28 (PPD-28) ⁽¹⁾.

Prezident Obama predniesol 17. januára 2014 prejav, v ktorom ohlásil dôležité reformy v spravodajskej oblasti. V tomto prejave zdôraznil, že „naše úsilie pomáha chrániť nielen našu krajinu, ale aj našich priateľov a spojencov. Toto úsilie bude účinné, iba ak bežní občania iných krajín budú veriť, že Spojené štáty rešpektujú aj ich súkromie.“ Prezident Obama oznámil vydanie novej prezidentskej smernice PPD-28, ktorá „jasne stanoví, čo robíme a čo nerobíme, pokiaľ ide o naše zahraničné sledovanie.“

V oddiele 4 písm. d) smernice PPD-28 sa nariaďuje ministrovi zahraničných vecí, aby vymenoval „hlavného koordinátora medzinárodnej diplomacie v oblasti informačných technológií“ (ďalej len „hlavný koordinátor“), ktorý by mal „slúžiť ako kontaktná osoba pre zahraničné vlády, ktoré chcú vyjadriť znepokojenie týkajúce sa činností signálového spravodajstva Spojených štátov.“ Od januára 2015 vykonáva funkciu hlavného koordinátora tajomníčka ministerstva Catherine Novelliová.

V tomto memorande je opísaný nový mechanizmus, ktorý bude hlavný koordinátor dodržiavať v záujme uľahčenia spracovávaní žiadostí týkajúcich sa prístupu, na účely národnej bezpečnosti, k údajom prenášaným z EÚ do Spojených štátov na základe štítu na ochranu osobných údajov, štandardných zmluvných doložiek, záväzných firemných pravidiel, „výnimiek“ ⁽²⁾ alebo „možných budúcich výnimiek“ ⁽³⁾ stanovenými postupmi v súlade s platnými právnymi predpismi a politikou Spojených štátov, a odpovedania na tieto žiadosti.

- 1. Ombudsman pre štít na ochranu osobných údajov.** Hlavná koordinátorka bude slúžiť ako ombudsman pre štít na ochranu osobných údajov a podľa potreby určí ďalších úradníkov ministerstva zahraničných vecí, ktorí jej budú pomáhať pri vykonávaní úloh uvedených v tomto memorande. (Koordinátorka a všetci ostatní úradníci vykonávajúci takéto povinnosti sa budú ďalej uvádzať ako „ombudsman pre štít na ochranu osobných údajov“.) Ombudsman pre štít na ochranu osobných údajov bude úzko spolupracovať s poverenými úradníkmi z iných ministerstiev a agentúr, ktorí sú zodpovední za spracovávanie žiadostí v súlade s platnými právnymi predpismi a politikami Spojených štátov. Ombudsman nie je závislý od spravodajských služieb. Ombudsman podlieha priamo ministrovi zahraničných vecí, ktorý zabezpečí, aby ombudsman vykonával svoju funkciu objektívne a bez pôsobenia neprimeraných vplyvov, ktoré by mohli viesť k ovplyvňovaniu poskytovanej odpovede.
- 2. Účinná koordinácia.** Ombudsman pre štít na ochranu osobných údajov bude môcť účinne využívať orgány dohľadu, ako je uvedené v ďalšej časti, a koordinovať ich činnosť s cieľom zabezpečiť, aby odpovede ombudsmana na žiadosti predkladajúceho orgánu EÚ, zaoberajúceho sa sťažnosťami jednotlivcov, boli založené na potrebných informáciách.

⁽¹⁾ Ak sa rozhodnutie Komisie o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA uplatní aj na Island, Lichtenštajnsko a Nórsko, súbor dokumentov týkajúcich sa štítu na ochranu osobných údajov sa bude vzťahovať na Európsku úniu, aj na uvedené tri krajiny. Všetky odkazy na EÚ a jej členské štáty sa teda budú chápať tak, že zahŕňajú aj Island, Lichtenštajnsko a Nórsko.

⁽²⁾ „Výnimky“ v tomto kontexte sú komerčný prenos, resp. prenosi, ktoré sa uskutočňujú pod podmienkou, že: a) dotknutá osoba nepochybne vyjadrila súhlas s navrhovaným prenosom, alebo že b) prenos je nevyhnutný na plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom alebo na vykonanie predzmluvných opatrení prijatých na žiadosť dotknutej osoby, alebo že c) prenos je nevyhnutný na uzatvorenie alebo plnenie zmluvy uzatvorenej v záujme dotknutej osoby medzi prevádzkovateľom a treťou stranou, alebo že d) prenos je nevyhnutný alebo požadovaný právnymi predpismi z dôvodov dôležitého verejného záujmu alebo na určenie, výkon alebo obranu právneho nároku, alebo že e) prenos je nevyhnutný na ochranu životne dôležitých záujmov dotknutej osoby, alebo že f) prenos sa uskutočňuje z registra, ktorý je podľa právnych predpisov určený na poskytovanie informácií verejnosti a ktorý je prístupný na nahliadanie verejnosti alebo akejkoľvek osobe, ktorá vie preukázať oprávnený záujem, pokiaľ sú v danom prípade splnené podmienky nahliadania, stanovené v právnych predpisoch.

⁽³⁾ „Možné budúce výnimky“ v tomto kontexte sú komerčný prenos, resp. prenosi, ktoré sa uskutočňujú za jednej z nasledujúcich podmienok, pokiaľ uvedená podmienka predstavuje oprávnený dôvod na prenos osobných údajov z EÚ do USA: a) dotknutá osoba vyjadrila výslovný súhlas s navrhovaným prenosom po tom, ako bola informovaná o rizikách, ktoré takéto prenosi môžu pre ňu predstavovať z dôvodu absencie rozhodnutia o primeranosti a primeraných záruk, alebo b) prenos je nevyhnutný na ochranu životne dôležitých záujmov dotknutej osoby alebo iných osôb, ak je dotknutá osoba fyzicky alebo právne nespôsobilá vyjadriť súhlas, alebo c) v prípade prenosu do tretej krajiny alebo medzinárodnej organizácii a v prípade, že nie je použiteľná žiadna iná odchýlka ani možná budúca odchýlka, a len ak prenos nie je opakujúcej sa povahy, sa týka len obmedzeného počtu dotknutých osôb, je nevyhnutný na účely závažných oprávnených záujmov prevádzkovateľa, nad ktorými neprevládajú záujmy alebo práva a slobody dotknutej osoby, a prevádzkovateľ posúdil všetky okolnosti sprevádzajúce prenos údajov a na základe tohto posúdenia poskytol vhodné záruky, pokiaľ ide o ochranu osobných údajov.

Ak sa žiadosť týka súladu príslušného sledovania s právom USA, ombudsman pre štít na ochranu osobných údajov bude môcť spolupracovať s jedným z nezávislých orgánov dohľadu s vyšetrovacími právomocami.

- a) Ombudsman pre štít na ochranu osobných údajov bude úzko spolupracovať s ďalšími úradníkmi vlády Spojených štátov vrátane príslušných nezávislých orgánov dohľadu s cieľom zabezpečiť, aby sa úplné žiadosti spracovávali a riešili v súlade s platnými právnymi predpismi a politikami. Ombudsman pre štít na ochranu osobných údajov bude môcť svoju činnosť úzko koordinovať predovšetkým s Úradom riaditeľa národnej spravodajskej služby, ministerstvom spravodlivosti a ďalšími ministerstvami a agentúrami, ktoré sa podieľajú na ochrane národnej bezpečnosti Spojených štátov, s generálnymi inšpektormi, úradníkmi pre uplatňovanie zákona o slobodnom prístupe k informáciám (Freedom of Information Act) a úradníkmi pre ochranu občianskych slobôd a súkromia.
- b) Vláda Spojených štátov sa bude spoliehať na mechanizmy koordinácie a dohľadu v oblasti národnej bezpečnosti v rámci ministerstiev a agentúr s cieľom zabezpečiť, aby ombudsman pre štít na ochranu osobných údajov mohol v zmysle oddielu 4 písm. e) odpovedať na úplné žiadosti podľa oddielu 3 písm. b).
- c) Ombudsman pre štít na ochranu osobných údajov môže o stanovisko k otázkam týkajúcim sa žiadostí požiadať Radu pre dohľad nad ochranou súkromia a občianskych slobôd.

3. Podávanie žiadostí

- a) Žiadosť sa na začiatku predloží orgánom členských štátov pre dohľad nad národnými bezpečnostnými službami a/alebo spracovanie osobných údajov orgánmi verejnej moci. Žiadosť predloží ombudsmanovi centralizovaný orgán EÚ (ďalej len „orgán EÚ zaoberajúci sa sťažnosťami fyzických osôb“).
- b) Orgán EÚ zaoberajúci sa sťažnosťami fyzických osôb bude zabezpečovať úplnosť žiadosti týmito opatreniami:
 - i) Overí totožnosť fyzickej osoby a skutočnosť, že táto fyzická osoba koná vo svojom mene a nie ako zástupca vládnej alebo medzivládnej organizácie.
 - ii) Zaistí, aby žiadosť bola vypracovaná písomne a aby obsahovala tieto základné informácie:
 - všetky informácie, ktoré tvoria základ žiadosti,
 - charakter požadovaných informácií alebo požadovanej nápravy,
 - orgány vlády Spojených štátov, ktorých by sa sťažnosť mala týkať, ak také sú, a
 - ďalšie opatrenia vykonávané na získanie požadovaných informácií alebo nápravy a odpovede získané týmito ďalšími opatreniami.
 - iii) Overí, či sa žiadosť vzťahuje na údaje, o ktorých sa odôvodnene predpokladá, že boli prenášané z EÚ do Spojených štátov na základe štítu na ochranu osobných údajov, štandardných zmluvných doložiek, záväzných firemných pravidiel, výnimiek alebo možných budúcich výnimiek.
 - iv) Vykoná úvodné zisťovanie, či žiadosť nie je neopodstatnená, svojvoľná alebo podaná v zlej viere.
- c) Aby bola žiadosť úplná na účely ďalšieho vybavovania zo strany ombudsmana pre štít na ochranu osobných údajov podľa tohto memoranda, nemusí v nej byť preukázané, že vláda Spojených štátov mala skutočne prístup k údajom žiadateľa prostredníctvom činností signálového spravodajstva.

4. Povinnosť komunikovať s predkladajúcim orgánom EÚ zaoberajúcim sa sťažnosťami fyzických osôb

- a) Ombudsman pre štít na ochranu osobných údajov potvrdí prijatie žiadosti predkladajúcemu orgánu EÚ zaoberajúcemu sa sťažnosťami fyzických osôb.
- b) Ombudsman pre štít na ochranu osobných údajov vykoná úvodné preskúmanie, ktorým overí, či je žiadosť úplná v súlade s oddielom 3 písm. b). Ak ombudsman pre štít na ochranu osobných údajov zaznamená akékoľvek nedostatky alebo bude mať nejaké otázky týkajúce sa úplnosti žiadosti, obráti sa na predkladajúci orgán EÚ zaoberajúci sa sťažnosťami fyzických osôb s cieľom uvedené obavy vyriešiť.

- c) Ak ombudsman pre štít na ochranu osobných údajov potrebuje na uľahčenie riadneho spracovania žiadosti viac informácií o tejto žiadosti, alebo ak je potrebné, aby fyzická osoba, ktorá pôvodne podala žiadosť, vykonala konkrétny úkon, ombudsman pre štít na ochranu osobných údajov o tom informuje predkladajúci orgán EÚ zaoberajúci sa sťažnosťami fyzických osôb.
 - d) Ombudsman pre štít na ochranu osobných údajov bude sledovať stav vybavovania žiadostí a podľa potreby bude predkladajúcemu orgánu EÚ zaoberajúcemu sa sťažnosťami fyzických osôb poskytovať aktualizované informácie.
 - e) Ak je žiadosť úplná podľa oddielu 3 tohto oznámenia, ombudsman pre štít na ochranu osobných údajov včas pošle predkladajúcemu orgánu EÚ zaoberajúcemu sa sťažnosťami fyzických osôb primeranú odpoveď, vzhľadom na trvalú povinnosť ochrany informácií v súlade s platnými právnymi predpismi a politikami. Ombudsman pre štít na ochranu osobných údajov pošle predkladajúcemu orgánu EÚ zaoberajúcemu sa sťažnosťami fyzických osôb odpoveď, v ktorej potvrdí, že i) sťažnosť bola riadne vyšetrená a ii) právo, právne predpisy, vládne nariadenia, prezidentské smernice a politiky agentúr USA, v ktorých sú stanovené obmedzenia a záruky uvedené v liste Úradu riaditeľa národnej spravodajskej služby, boli dodržané, alebo v prípade ich nedodržania, že sa prijali nápravné opatrenia. Ombudsman pre štít na ochranu osobných údajov nepotvrdí ani nepoprie, že jednotlivec bol cieľom sledovania, a ani nepotvrdí, že sa uplatnilo konkrétne nápravné opatrenie. Ako je ďalej vysvetlené v oddiele 5, žiadosti podané na základe zákona o slobodnom prístupe k informáciám sa budú spracovávať v súlade s týmto zákonom a príslušnými nariadeniami.
 - f) Ombudsman pre štít na ochranu osobných údajov bude komunikovať priamo s orgánom EÚ zaoberajúcim sa sťažnosťami fyzických osôb, ktorý bude následne zodpovedný za komunikáciu s jednotlivcom podávajúcim žiadosť. Ak je priama komunikácia súčasťou jedného zo základných postupov uvedených v ďalšej časti, táto komunikácia bude prebiehať v súlade s existujúcimi postupmi.
 - g) Záväzky uvedené v tomto memorande sa nebudú vzťahovať na všeobecné tvrdenia, že štít na ochranu osobných údajov medzi EÚ a USA nie je zlučiteľný s požiadavkami Európskej únie na ochranu údajov. Záväzky uvedené v tomto memorande vychádzajú zo spoločného porozumenia Európskej komisie a vlády USA, že vzhľadom na rozsah záväzkov v rámci tohto mechanizmu môže dôjsť k obmedzeniu zdrojov, okrem iného aj vo vzťahu k žiadostiam podľa zákona o slobodnom prístupe k informáciám. Ak by vykonávanie funkcie ombudsmana pre štít na ochranu osobných údajov viedlo k prekročeniu primeraných obmedzení prostriedkov a bránilo by v plnení týchto záväzkov, vláda USA prediskutuje s Európskou komisiou úpravy, ktoré by mohli byť vhodné na riešenie situácie.
5. **Žiadosti o informácie.** Žiadosti o prístup k záznamom vlády Spojených štátov je možné podávať a spracovávať na základe zákona o slobodnom prístupe k informáciám (ďalej len „zákon“).
- a) Zákon umožňuje každej osobe, bez ohľadu na jej štátnu príslušnosť, domáhať sa prístupu k existujúcim záznamom federálnych agentúr. Tento zákon je kodifikovaný v Zbierke zákonov Spojených štátov, 5 U.S.C. § 552. Zákon je spolu s doplňujúcimi informáciami týkajúcimi sa zákona o slobodnom prístupe k informáciám dostupný na www.FOIA.gov a <http://www.justice.gov/oip/foia-resources>. Každá agentúra má hlavného úradníka pre uplatňovanie zákona o slobodnom prístupe k informáciám a na svojom verejnom webovom sídle poskytuje informácie o tom, ako je možné podať agentúre žiadosť na základe tohto zákona. Agentúry majú svoje postupy pre vzájomné konzultácie o žiadostiach na základe zákona o slobodnom prístupe k informáciám, ktoré sa týkajú záznamov inej agentúry.
 - b) Napríklad:
 - i) Úrad riaditeľa národnej spravodajskej služby zriadil portál úradu (portál ODNI FOIA) týkajúci sa zákona o slobodnom prístupe k informáciám: <http://www.dni.gov/index.php/about-this-site/foia>. Na tomto portáli sa poskytujú informácie o podávaní žiadostí, overovaní stavu vybavovania existujúcich žiadostí a o prístupe k informáciám, ktoré Úrad riaditeľa národnej spravodajskej služby uvoľnil a zverejnil na základe zákona o slobodnom prístupe k informáciám. Portál ODNI FOIA obsahuje aj odkazy na iné webové stránky zložiek spravodajských služieb týkajúce sa zákona o slobodnom prístupe k informáciám. <http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites>.
 - ii) Komplexné informácie týkajúce sa zákona o slobodnom prístupe k informáciám poskytuje úrad informačnej politiky ministerstva spravodlivosti: <http://www.justice.gov/oip>. Na tejto webovej stránke sa uvádzajú nielen informácie o podávaní žiadostí ministerstvu spravodlivosti na základe zákona o slobodnom prístupe k informáciám, ale poskytujú sa aj usmernenia vláde Spojených štátov, pokiaľ ide o výklad a uplatňovanie požiadaviek uvedeného zákona.

- c) Podľa zákona o slobodnom prístupe k informáciám sa na prístup k vládnym záznamom vzťahujú určité vymenované výnimky. Patria k nim obmedzenia prístupu k utajovaným informáciám týkajúcim sa národnej bezpečnosti, osobným údajom tretích strán a informáciám týkajúcim sa vyšetrovaní v rámci presadzovania práva. Tieto obmedzenia sú porovnateľné s obmedzeniami, ktoré každý členský štát EÚ uložil vo svojom zákone o prístupe k informáciám. Tieto obmedzenia sa uplatňujú rovnako voči americkým občanom, aj voči občanom iných štátov.
- d) Spory ohľadom zverejňovania záznamov, ktoré sa požaduje na základe zákona o slobodnom prístupe k informáciám, sa môžu riešiť správnu cestou a potom na federálnom súde. Súd musí nanovo určiť, či odopretie prístupu k záznamom bolo správne [podľa ustanovenia 5 U.S.C. § 552 písm. a) ods. 4 bod B)], a môže vláde nariadiť, aby poskytla prístup k záznamom. V niektorých prípadoch súdy vyvrátili tvrdenia vlády, že informácie by sa nemali poskytovať, pretože sú utajené. Hoci nie je možné získať peňažnú náhradu škody, súdy môžu priznať náhradu nákladov na právneho zástupcu.
6. **Žiadosti o ďalšie opatrenia.** Žiadosť obsahujúca obvinenie z porušenia zákona alebo iného pochybenia bude postúpená príslušnému orgánu vlády Spojených štátov, vrátane nezávislých orgánov dohľadu, s právomocou vyšetrovať príslušnú žiadosť a riešiť porušenie právnych predpisov, ako je to opísané v ďalšej časti.
- a) Generálni inšpektori sú zo zákona nezávislí, majú širokú právomoc vykonávať vyšetrovanie, audity a preskúmania programov vrátane podvodov, zneužitia alebo porušenia zákona a môžu odporúčať nápravné opatrenia.
- i) V zákone o generálnych inšpektoroch (Inspector General Act) z roku 1978, v znení zmien, sú vo väčšine agentúr ustanovení federálni generálni inšpektori ako nezávislé a objektívne orgány, ktorých úlohou je boj proti mrhaniu, podvodom a zneužívaniu v programoch a operáciách príslušných agentúr. Na tento účel je každý generálny inšpektor zodpovedný za vykonávanie auditov a vyšetrovaní týkajúcich sa programov a operácií jeho agentúry. Generálni inšpektori okrem toho zabezpečujú vedenie a koordináciu a odporúčajú postupy pre činnosti zamerané na podporu hospodárnosti, účinnosti a efektívnosti a na prevenciu a odhaľovanie podvodov a zneužívania v programoch a operáciách agentúry.
- ii) Každá zložka spravodajských služieb má svoj úrad generálneho inšpektora, ktorý okrem iného zodpovedá za dohľad nad zahraničnou spravodajskou činnosťou. Mnohé správy generálnych inšpektorov o spravodajských programoch boli zverejnené.
- iii) Napríklad:
- Úrad generálneho inšpektora spravodajských služieb bol zriadený na základe oddielu 405 zákona o schválení spravodajskej činnosti za rozpočtový rok 2010 (Intelligence Authorization Act of Fiscal Year 2010 – <http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf>). Generálny inšpektor spravodajských služieb je zodpovedný za vykonávanie auditov, vyšetrovaní, inšpekcí a preskúmaní všetkých spravodajských služieb na účely zistenia a riešenia systémových rizík, zraniteľných miest a nedostatkov spoločných pre misie agentúr spravodajskej služby, s cieľom pozitívne vplyvať na hospodárnosť a efektívnosť všetkých spravodajských služieb. Generálny inšpektor spravodajských služieb je oprávnený vyšetrovať sťažnosti alebo informácie týkajúce sa obvinení z porušovania zákonov, predpisov, nariadení, z mrhania, podvodov, zneužívania právomoci alebo závažného či konkrétneho ohrozenia verejného zdravia a bezpečnosti v súvislosti s programami a činnosťami Úradu riaditeľa národnej spravodajskej služby a/alebo spravodajskej služby. Generálny inšpektor spravodajských služieb poskytuje informácie o tom, ako ho priamo kontaktovať na účely predloženia správy: <http://www.dni.gov/index.php/about-this-site/contact-the-ig>.
- Úrad generálneho inšpektora na Ministerstve spravodlivosti USA (DOJ – <https://www.justice.gov>) je zákonom zriadený nezávislý subjekt, ktorého poslaním je odhaľovanie a prevencia mrhania, podvodov, zneužívania a pochybení v programoch ministerstva spravodlivosti a v činnosti jeho zamestnancov, ako aj podpora hospodárnosti a efektívnosti v týchto programoch. Úrad generálneho inšpektora vyšetroje údajné porušenia trestného a občianskeho práva zamestnancami ministerstva spravodlivosti a vykonáva aj audity a inšpekcie programov ministerstva. Úrad generálneho inšpektora má právomoc vo všetkých prípadoch sťažností na pochybenia, vznesených voči zamestnancom ministerstva spravodlivosti vrátane Federálneho úradu pre vyšetrovanie (FBI), Národného úradu pre kontrolu obchodu s drogami (DEA), Federálneho úradu pre väznice (Federal Bureau of Prisons), Federálnej policajnej služby USA (U.S. Marshals Service), Úradu pre alkohol, tabak, zbrane a výbušniny (ATF), Úradu štátneho zástupcu Spojených štátov a zamestnancov, ktorí pracujú na iných úsekoch alebo v iných úradoch ministerstva spravodlivosti. (Jedinou výnimkou je, že

údajné pochybenia zamestnancov prokuratúry a orgánov presadzovania práva ministerstva, ktoré sa týkajú vykonávania právomoci prokurátorov vyšetrovať, viesť súdne spory alebo poskytovať právne poradenstvo, rieši úrad ministerstva pre profesionálnu zodpovednosť). Okrem toho sa v oddieli 1001 vlasteneckého zákona USA (*Patriot Act*), ktorý bol prijatý 26. októbra 2001, generálnemu inšpektorovi nariaďuje, aby preskúmaval informácie a prijímal sťažnosti s obvineniami z porušovania občianskych práv a občianskych slobôd zamestnancami ministerstva spravodlivosti. Úrad generálneho inšpektora má verejné webové sídlo <https://www.oig.justice.gov>, ktorého súčasťou je „horúca linka“ na podávanie sťažností: <https://www.oig.justice.gov/hotline/index.htm>.

b) Príslušné povinnosti majú aj úrady a subjekty vlády USA na ochranu súkromia a občianskych slobôd. Napríklad:

- i) V oddiele 803 vykonávacích odporúčaní zákona o vyšetrovacej komisii pre 11. september (9/11 Commission Act) z roku 2007, kodifikovanom v Zbierke zákonov Spojených štátov, 42 U.S.C. § 2000-ee1, sa v rámci určitých ministerstiev a agentúr (vrátane ministerstva zahraničných vecí, ministerstva spravodlivosti a Úradu riaditeľa národnej spravodajskej služby) zriaďujú funkcie úradníkov pre ochranu súkromia a občianskych slobôd. V oddiele 803 sa uvádza, že títo úradníci pre ochranu súkromia a občianskych slobôd budú slúžiť ako hlavní poradcovia zabezpečujúci okrem iného, aby takéto ministerstvo, agentúra alebo iný subjekt mali zavedené primerané postupy na riešenie sťažností fyzických osôb, ktorých súkromie alebo občianske slobody údajne toto ministerstvo, agentúra alebo iný subjekt porušili.
- ii) Úrad pre ochranu občianskych slobôd a súkromia v rámci Úradu riaditeľa národnej spravodajskej služby (ďalej len „ODNI CLPO“) vedie úradník pre ochranu občianskych slobôd Úradu riaditeľa národnej spravodajskej služby, pričom táto funkcia bola zriadená na základe zákona o národnej bezpečnosti (National Security Act) z roku 1948, v znení zmien. Medzi úlohy ODNI CLPO patrí zabezpečiť, aby politiky a postupy zložiek spravodajských služieb zahŕňali primeranú ochranu súkromia a občianskych slobôd, a preskúmavať a vyšetrovať sťažnosti s obvineniami z porušovania občianskych slobôd a súkromia v rámci programov a činností Úradu riaditeľa národnej spravodajskej služby. ODNI CLPO poskytuje verejnosti informácie vrátane pokynov k tomu, ako podávať sťažnosti, na svojej webovej lokalite: www.dni.gov/clpo. Ak ODNI CLPO dostane sťažnosť týkajúcu sa súkromia alebo občianskych slobôd v súvislosti s programami a činnosťami spravodajských služieb, bude sa ďalšími zložkami spravodajských služieb koordinovať postup, akým by sa mala táto sťažnosť ďalej spracovať. Upozorňujeme, že aj Národná bezpečnostná agentúra (NSA) má úrad pre ochranu občianskych slobôd a súkromia, ktorý poskytuje informácie o svojich povinnostiach na webovej lokalite: https://www.nsa.gov/civil_liberties/. Ak z informácií vyplýva, že agentúra neplní požiadavky na ochranu súkromia (napr. požiadavku uvedenú v oddiele 4 smernice PPD-28), agentúry majú mechanizmy na zabezpečenie súladu, prostredníctvom ktorých sa prípad preskúma a prijímú sa nápravné opatrenia. Agentúry sú povinné prípady neplnenia požiadaviek smernice PPD-28 hlásiť Úradu riaditeľa národnej spravodajskej služby.
- iii) Úrad pre ochranu súkromia a občianskych slobôd na ministerstve spravodlivosti podporuje vykonávanie úloh a povinností hlavného úradníka ministerstva pre ochranu súkromia a občianskych slobôd. Hlavným poslaním Úradu pre ochranu súkromia a občianskych slobôd je chrániť súkromie a občianske slobody Američanov prostredníctvom preskúmania a koordinácie postupov ministerstva v oblasti ochrany osobných údajov a dohľadu nad nimi. Úrad pre ochranu súkromia a občianskych slobôd poskytuje právne poradenstvo a usmernenia zložkám ministerstva, zabezpečuje, aby ministerstvo plnilo požiadavky na ochranu súkromia vrátane dodržiavania zákona o ochrane súkromia (Privacy Act) z roku 1974, ustanovení týkajúcich sa ochrany súkromia v zákone o elektronickej verejnej správe (E-Government Act) z roku 2002 a vo federálnom zákone o riadení informačnej bezpečnosti (Federal Information Security Management Act), ako aj smerníc o správnych postupoch vydávaných na podporu týchto zákonov, pripravuje a poskytuje v rámci ministerstva odbornú prípravu týkajúcu sa ochrany súkromia, pomáha hlavnému úradníkovi pre ochranu súkromia a občianskych slobôd pri príprave politiky ministerstva v oblasti ochrany súkromia, vypracováva správy týkajúce sa ochrany súkromia pre prezidenta a Kongres, a preskúmava postupy ministerstva pri narábaní s informáciami, aby sa zabezpečilo, že tieto postupy sú v súlade s ochranou súkromia a občianskych slobôd. Úrad pre ochranu osobných údajov poskytuje verejnosti informácie o svojich povinnostiach na adrese: <http://www.justice.gov/opcl>.
- iv) Podľa ustanovení 42 U.S.C. § 2000ee a nasledujúcich musí Rada pre dohľad nad ochranou súkromia a občianskych slobôd (Privacy and Civil Liberties Oversight Board) sústavne preskúmavať i) politiky a postupy ministerstiev, agentúr a zložiek exekutívy týkajúce sa úsilia o ochranu krajiny pred terorizmom, ako aj ich vykonávanie, aby sa zabezpečila ochrana súkromia a občianskych slobôd a ii) ďalšie aktivity exekutívy týkajúce sa takého úsilia, aby sa zistilo, či sa v rámci týchto aktivít primerane chráni súkromie a občianske slobody a či sú v súlade s platnými zákonmi, nariadeniami a politikami týkajúcimi sa ochrany súkromia a občianskych slobôd. Rada prijíma a preskúmava správy a ďalšie informácie od úradníkov pre ochranu osobných údajov a úradníkov pre ochranu občianskych slobôd a v prípade potreby im dáva odporúčania týkajúce sa ich činnosti. V oddiele 803 vykonávacích odporúčaní zákona o vyšetrovacej komisii pre 11. september z roku 2007, kodifikovanom v Zbierke zákonov Spojených štátov, 42 U.S.C. § 2000-ee1, sa pre úradníkov pre ochranu súkromia a občianskych slobôd ôsmich federálnych agentúr [vrátane ministra obrany, ministra vnútornej bezpečnosti, riaditeľa národnej spravodajskej služby a riaditeľa Ústrednej spravodajskej služby (CIA)] a všetkých ďalších agentúr určených radou stanovuje povinnosť predkladať PCLOB pravidelné správy obsahujúce údaje o počte, charaktere a rozdelení sťažností na údajné porušenia predpisov, ktoré prijala

príslušná agentúra. V splnomocňovacom zákone sa Rade pre dohľad nad ochranou súkromia a občianskych slobôd nariaďuje prijímať tieto správy a v prípade potreby dávať úradníkom pre ochranu súkromia a občianskych slobôd odporúčania týkajúce sa ich činnosti.

PRÍLOHA IV

List predsedníčky Federálnej obchodnej komisie Edith Ramirezovej

7. júla 2016

ELEKTRONICKOU POŠTOU

Věra Jourová
Komisárka pre spravodlivosť, spotrebiteľov a rodovú rovnosť
Európska komisia
Rue de la Loi/Wetstraat 200
1049 Brusel
Belgicko

Vážená pani komisárka Jourová,

Federálna obchodná komisia Spojených štátov (ďalej len „FTC“) oceňuje možnosť opísať spôsob, akým presadzuje nový rámec štítu na ochranu osobných údajov medzi EÚ a USA (ďalej len „rámec štítu na ochranu osobných údajov“ alebo „rámec“). Domnievame sa, že rámec bude zohrávať rozhodujúcu úlohu pri posilňovaní ochrany osobných údajov v obchodných transakciách v stále viac prepojenom svete. Rámec umožní podnikom vykonávať dôležité operácie v globálnom hospodárstve a zároveň zabezpečí spotrebiteľom v EÚ zachovanie dôležitej ochrany osobných údajov. FTC sa dlhodobo angažuje v oblasti cezhraničnej ochrany osobných údajov a presadzovanie nového rámca bude jej vysokou prioritou. V ďalšej časti vysvetľujeme históriu intenzívneho presadzovania ochrany súkromia zo strany FTC všeobecne, vrátane nášho presadzovania pôvodného programu „bezpečného prístavu“, ako aj prístup FTC k presadzovaniu nového rámca.

FTC prvýkrát verejne vyjadrila svoj záväzok presadzovať program bezpečného prístavu v roku 2000. V tom čase poslal vtedajší predseda FTC Robert Pitofsky list Európskej komisii, v ktorom vyjadril záväzok FTC dôrazne presadzovať zásady bezpečného prístavu. FTC pokračovala v plnení tohto záväzku prostredníctvom takmer 40 opatrení na presadzovanie programu, početných doplňujúcich vyšetrovaní a spolupráce s jednotlivými európskymi orgánmi pre ochranu osobných údajov vo veciach spoločného záujmu.

Keď Európska komisia v novembri 2013 vyjadrila znepokojenie týkajúce sa vykonávania a presadzovania programu bezpečného prístavu, spoločne s Ministerstvom obchodu USA sme začali konzultácie s úradníkmi Európskej komisie, aby sme preskúmali možnosti, ako tento program posilniť. V priebehu týchto konzultácií vydal 6. októbra 2015 Súdny dvor Európskej únie rozhodnutie vo veci Schrems, v ktorom okrem iného zrušil rozhodnutie Európskej komisie týkajúce sa primeranosti programu bezpečného prístavu. Po tomto rozhodnutí sme pokračovali v úzkej spolupráci s ministerstvom obchodu a Európskou komisiou v úsilí o posilnenie ochrany súkromia poskytovanej fyzickým osobám z EÚ. Výsledkom týchto pokračujúcich konzultácií je rámec štítu na ochranu osobných údajov. Podobne ako v prípade programu bezpečného prístavu sa FTC týmto zaväzuje dôrazne presadzovať nový rámec. Tento list je potvrdením uvedeného záväzku.

Potvrdzujeme svoj záväzok najmä v týchto štyroch kľúčových oblastiach: 1. prioritné vybavovanie postúpených žiadostí a vyšetrovanie; 2. riešenie falošných alebo podvodných vyhlásení o zapojení do štítu na ochranu osobných údajov; 3. nepretržité monitorovanie výkonu nariadení a 4. väčšie zapájanie orgánov EÚ pre ochranu osobných údajov pri presadzovaní rámca a spolupráca s nimi. V ďalšej časti uvádzame podrobné informácie o každom z týchto záväzkov a príslušné súvislosti týkajúce sa úlohy FTC pri ochrane súkromia spotrebiteľov a presadzovaní programu bezpečného prístavu, ako aj širší pohľad na stav ochrany súkromia v Spojených štátoch ⁽¹⁾.

I. SÚVISLOSTI**A. Presadzovanie ochrany súkromia Federálnou komisiou pre obchod a jej práca v oblasti politík**

FTC má široké právomoci v oblasti presadzovania občianskeho práva v záujme ochrany spotrebiteľa a hospodárskej súťaže v obchodnej sfére. Ako súčasť svojho mandátu v oblasti ochrany spotrebiteľa FTC presadzuje širokú škálu

⁽¹⁾ Doplňujúce informácie o federálnych a štátnych zákonoch týkajúcich sa ochrany súkromia v USA uvádzame v prílohe A a súhrn našich najnovších opatrení na presadzovanie ochrany súkromia a bezpečnosti je dostupný na webovej lokalite FTC <https://www.ftc.gov/reports/privacy-data-security-update-2015>.

zákonov na ochranu súkromia a bezpečnosti údajov o spotrebiteľoch. V základnom zákone, ktorý FTC presadzuje, zákone o FTC (FTC Act), sa zakazuje „nekalé“ a „klamlivé“ konanie alebo praktiky v obchode alebo ovplyvňujúce obchod⁽¹⁾. Vyhlásenia, opomenutia alebo praktiky sú klamlivé, ak sú závažné a môžu zavádzať spotrebiteľov konajúcich za daných okolností primerane⁽²⁾. Konanie alebo praktiky sú nekalé, ak spôsobujú alebo môžu spôsobiť závažnú ujmu, ktorej sa spotrebiteľia nemôžu primerane vyhnúť alebo ktorá nie je vyvážená vyrovnávacími výhodami pre spotrebiteľov alebo hospodársku súťaž⁽³⁾. FTC presadzuje aj cieľené predpisy na ochranu informácií týkajúcich sa zdravia, úverov a ďalších finančných záležitostí, ako aj online informácií o deťoch, a vydala nariadenia, ktorými sa každý z týchto predpisov vykonáva.

Právomoc FTC sa podľa zákona o FTC uplatňuje vo veciach „v obchode alebo ovplyvňujúcich obchod“. FTC nemá právomoc v oblasti presadzovania trestného práva, ani vo veciach národnej bezpečnosti. Rovnako nemá FTC dosah na väčšinu ďalších vládnych opatrení. Okrem tohto existujú výnimky v právomoci FTC, pokiaľ ide o obchodné činnosti vrátane činnosti bánk, leteckých spoločností, poisťovní a bežných prenosových činností poskytovateľov telekomunikačných služieb. FTC nemá právomoc ani vo vzťahu k väčšine neziskových organizácií, má však právomoc vo vzťahu k fiktívnym charitatívnym organizáciám alebo iným neziskovým organizáciám, ktorých činnosť je v skutočnosti zameraná na vytváranie zisku. FTC má právomoc aj vo vzťahu k neziskovým organizáciám, ktoré svojou činnosťou vytvárajú zisk pre svojich na zisk zameraných členov vrátane poskytovania významných hospodárskych výhod týmto členom⁽⁴⁾. V niektorých prípadoch sa právomoc FTC prekrýva s právomocou iných orgánov presadzovania práva.

Vybudovali sme si pevné pracovné vzťahy s federálnymi a štátnymi orgánmi a v prípade potreby s nimi úzko spolupracujeme pri koordinácii vyšetrovaní alebo vybavovaní postúpených žiadostí.

Presadzovanie je základným prvkom prístupu FTC k ochrane súkromia. Doposiaľ FTC riešila viac ako 500 prípadov ochrany súkromia a bezpečnosti spotrebiteľských informácií. Tento súbor prípadov zahŕňa prípady týkajúce sa offline aj online informácií a zahŕňa opatrenia na presadzovanie práva voči veľkým aj malým spoločnostiam, ktoré boli obvinené z nesprávneho zaobchádzania s citlivými údajmi o spotrebiteľoch, nezabezpečili osobné informácie spotrebiteľov, klamlivo sledovali spotrebiteľov online, posielali spotrebiteľom nevyžiadané správy (spam), inštalovali do počítačov spotrebiteľov sledovacie programy (spyware) alebo iné škodlivé programy, porušovali zásadu „nevolať“ a ďalšie pravidlá telemarketingu a nenáležite zhromažďovali a vymieňali si informácie o mobilných zariadeniach spotrebiteľov. Opatrenia FTC na presadzovanie práva, vo fyzickej aj digitálnej podobe, vysielajú spoločnostiam dôležitý signál o potrebe chrániť súkromie spotrebiteľov.

FTC uskutočnila aj viaceré iniciatívy v oblasti politík zamerané na posilnenie ochrany súkromia spotrebiteľov, o ktoré sa opiera pri svojej práci pri presadzovaní práva. FTC zorganizovala viaceré semináre a vydala správy, v ktorých odporúča najlepšie postupy zamerané, okrem iného, na zlepšenie ochrany súkromia v mobilnom ekosystéme, zvýšenie transparentnosti v oblasti obchodovania s údajmi, maximalizovanie výhod plynúcich z veľkých dát (big data) pri súčasnom zmierňovaní ich rizík, predovšetkým pre spotrebiteľov s nízkymi príjmami a nedostatočnou dostupnosťou služieb a zdôrazňovanie dôsledkov rozpoznávania tvárí a internetu vecí pre ochranu súkromia a bezpečnosť.

FTC sa podieľa aj na vzdelávaní spotrebiteľov a podnikov s cieľom posilniť vplyv svojich iniciatív v oblasti presadzovania práva a prípravy politík. FTC používa rozličné nástroje, napríklad publikácie, online zdroje, semináre a sociálne médiá, na poskytovanie vzdelávacích materiálov týkajúcich sa širokej škály tém vrátane mobilných aplikácií, ochrany súkromia detí a bezpečnosti údajov. Najnovšie začala realizovať iniciatívu „Začni bezpečnosťou“ („Start with security“), ktorá zahŕňa nové usmernenia pre podniky vychádzajúce zo skúseností získaných z jej prípadov týkajúcich sa bezpečnosti údajov, ako aj sériu seminárov v celej krajine. FTC má okrem toho dlhodobu vedúcu postavenie vo vzdelávaní spotrebiteľov v oblasti základnej počítačovej bezpečnosti. Vlani si našu webovú stránku OnGuard Online a jej verziu v španielčine, Alerta en Línea, pozrelo viac ako 5 miliónov návštevníkov.

B. Právna ochrana USA v prospech spotrebiteľov z EÚ

Rámec bude fungovať v kontexte širšej oblasti ochrany súkromia v USA, v rámci ktorej sú spotrebiteľia z EÚ chránení viacerými spôsobmi.

⁽¹⁾ 15 U.S.C. § 45a).

⁽²⁾ Pozri politické vyhlásenie FTC o klamlivej činnosti v prílohe k Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), dostupné na <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

⁽³⁾ Pozri 15 U.S.C. § 45n); Pozri politické vyhlásenie FTC o nekalej činnosti v prílohe k Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), dostupné na <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

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

Zákaz nekalého alebo klamlivého konania alebo praktík v zákone o FTC sa neobmedzuje na ochranu spotrebiteľov v USA pred spoločnosťami z USA, keďže zahŕňa postupy, ktoré 1. spôsobujú alebo môžu spôsobiť primerane predvídateľnú ujmu v Spojených štátoch alebo 2. predstavujú závažné konanie v Spojených štátoch. FTC môže ďalej pri ochrane zahraničných spotrebiteľov využívať všetky nápravné opatrenia, ktoré sú k dispozícii na ochranu domácich spotrebiteľov, vrátane odškodnenia.

Práca FTC pri presadzovaní práva skutočne prináša výrazný prospech spotrebiteľom v USA aj zahraničným spotrebiteľom. Napríklad, naše prípady presadzovania ustanovení oddielu 5 zákona o FTC znamenali rovnakú ochranu súkromia spotrebiteľov v USA aj zahraničných spotrebiteľov. Vo veci obchodníka s informáciami, spoločnosti Accusearch, FTC konštatovala, že predaj dôverných telefónnych záznamov tretím stranám bez vedomia alebo súhlasu spotrebiteľov bol zo strany spoločnosti nekalou praktikou a porušením oddielu 5 zákona o FTC. Spoločnosť Accusearch predávala informácie týkajúce sa spotrebiteľov v USA aj zahraničných spotrebiteľov⁽¹⁾. Súd vydal voči spoločnosti Accusearch súdny príkaz, ktorým okrem iného zakázal obchodovanie s osobnými informáciami spotrebiteľov alebo ich nákup bez ich písomného súhlasu, pokiaľ neboli tieto informácie získané zákonným spôsobom z verejne dostupných zdrojov, a nariadil vyplatenie sumy takmer 200 000 USD⁽²⁾.

Ďalším príkladom je dohoda FTC so spoločnosťou TRUSTe. Dohoda zabezpečuje, že spotrebiteľia, vrátane spotrebiteľov z Európskej únie, sa môžu spoľahnúť na ubezpečenia, ktoré globálny samoregulačný orgán poskytuje o svojom preskúmaní a certifikácii domácich a zahraničných online služieb⁽³⁾. Dôležité je, že naše opatrenia voči spoločnosti TRUSTe posilňujú v širšom rozsahu aj samoregulačný systém v oblasti ochrany súkromia, keďže zaisťujú zodpovednosť subjektov, ktoré zohrávajú dôležitú úlohu v samoregulačných systémoch vrátane cezhraničných rámcov ochrany súkromia.

FTC tiež presadzuje ďalšie ciele zákony, ktorými sa ochrana rozširuje na spotrebiteľov mimo USA, ako je napríklad zákon o ochrane súkromia detí v rámci online sietí (Children's Online Privacy Protection Act). V zákone sa okrem iného požaduje, aby prevádzkovatelia webových stránok a online služieb zameraných na deti alebo stránok určených pre širokú verejnosť, na ktorých sa úmyselne zhromažďujú osobné informácie od detí mladších ako 13 rokov, poskytovateli upozornenie pre rodičov a získavali overiteľný súhlas rodičov. Webové stránky a služby prevádzkované poskytovateľmi so sídlom v USA, na ktoré sa vzťahuje tento zákon a na ktorých sa zhromažďujú osobné informácie od detí zo zahraničia, musia spĺňať požiadavky stanovené v uvedenom zákone. Webové stránky a online služby prevádzkované poskytovateľmi so sídlom v zahraničí musia tiež spĺňať požiadavky stanovené v uvedenom zákone, ak sa zameriavajú na deti v Spojených štátoch alebo sa na nich úmyselne zhromažďujú osobné informácie od detí v Spojených štátoch. Okrem federálnych zákonov USA, ktoré presadzuje FTC, môžu ďalšie výhody pre spotrebiteľov z EÚ prinášať aj niektoré iné federálne a štátne zákony týkajúce sa ochrany spotrebiteľov a súkromia.

C. Presadzovanie programu bezpečného prístavu

V rámci svojho programu presadzovania ochrany súkromia a bezpečnosti sa FTC usiluje chrániť spotrebiteľov z EÚ aj realizáciou opatrení, ktoré súvisia s porušovaním programu bezpečného prístavu. FTC vykonala 39 opatrení na presadzovanie programu bezpečného prístavu: 36 obvinení z falošných vyhlásení o osvedčení a tri veci, proti spoločnostiam Google, Facebook a Myspace, týkajúce sa údajných porušení zásad bezpečného prístavu⁽⁴⁾. Tieto prípady ukazujú, že osvedčenia je možné presadzovať a že za porušovanie zásad hrozia následky. V správnych opatreniach (consent orders) na dvadsať rokov sa od spoločností Google, Facebook a Myspace požaduje, aby zaviedli komplexné programy na ochranu súkromia, ktoré musia byť primerane navrhnuté tak, aby riešili riziká ochrany súkromia súvisiace s vývojom a spravovaním nových a existujúcich produktov a služieb a aby chránili súkromie a dôvernosť osobných informácií. V rámci komplexných programov na ochranu súkromia, ktoré boli nariadené týmito uzneseniami, sa musia identifikovať predvídateľné závažné riziká a musia byť k dispozícii mechanizmy na ich riešenie. Spoločnosti sa tiež musia podrobiť priebežnému nezávislému posudzovaniu svojich programov na ochranu súkromia, ktorého výsledky sa musia poskytnúť FTC. V uzneseniach sa týmto spoločnostiam tiež zakazuje, aby neposkytovali nepravdivé informácie o svojich postupoch v oblasti ochrany súkromia a svojej účasti na akomkoľvek programe na ochranu súkromia alebo bezpečnosti. Tento zákaz by sa vzťahoval aj na konanie a praktiky spoločností na základe štítu na ochranu osobných

⁽¹⁾ Pozri Úrad kanadského komisára pre ochranu súkromia, sťažnosť podľa zákona PIPEDA proti spoločnosti Accusearch, Inc., ktorá podniká ako Abika.com, [https://www.priv.gc.ca/cf-dc/2009_009_0731_e.asp](https://www.priv.gc.ca/cf-dc/2009/009_0731_e.asp). Úrad kanadského komisára pre ochranu súkromia predložil informácie amicus curiae (priateľa súdu) v odvolacom konaní FTC a vykonal vlastné vyšetrovanie, pričom dospel k záveru, že postupy spoločnosti Accusearch porušovali aj kanadské právne predpisy.

⁽²⁾ Pozri vec FTC/Accusearch, Inc., č. 06CV015D (D. Wyo. 20. decembra 2007), potvrdené 50 F.3d 1187 (10. Cir. 2009).

⁽³⁾ Pozri vec True Ultimate Standards Everywhere, Inc., č. C-4512 (F.T.C. 12. marca 2015) (decision and order), dostupné na <https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf>.

⁽⁴⁾ Pozri vec Google, Inc., č. C-4336 (F.T.C. 13. októbra 2011) (decision and order), dostupné na <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>; vec Facebook, Inc., č. C-4365 (F.T.C. 27. júla 2012) (decision and order), dostupné na <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>; vec Myspace LLC, č. C-4369 (F.T.C. 30. augusta 2012) (decision and order), dostupné na <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace>.

údajov. FTC môže presadzovať plnenie týchto uznesení prostredníctvom občianskoprávných sankcií. Spoločnosť Google už skutočne v roku 2012 zaplatila ako občianskoprávnú sankciu rekordnú sumu 22,5 milióna USD za porušovanie uznesenia FTC. Takže tieto uznesenia FTC pomáhajú chrániť viac ako miliardu spotrebiteľov na celom svete, z ktorých stovky miliónov žijú v Európe.

Veci FTC sa zameriavali aj na falošné, klamlivé alebo zavádzajúce vyhlásenia o účasti na programe bezpečného prístavu. FTC berie tieto vyhlásenia vážne. Napríklad vo veci *FTC/Karnani* FTC v roku 2011 zasiahla proti internetovému obchodníkovi v Spojených štátoch, ktorý bol obvinený, že spolu so svojou spoločnosťou uviedol britských spotrebiteľov do omylu, že spoločnosť sídli v Spojenom kráľovstve, keď okrem iného používali webové označenie.uk a uvádzali odkazy na britskú menu a poštový systém Spojeného kráľovstva⁽¹⁾. Keď však spotrebiteľia dostali výrobky, zistili neočakávané dovozné clo, záruky, ktoré neplatia v Spojenom kráľovstve, a poplatky spojené s vrátením dane. FTC obviňovala obžalovaných aj z toho, že klamali spotrebiteľov vo veci svojej účasti na programe bezpečného prístavu. Pozoruhodné je, že všetci postihnutí spotrebiteľia žili v Spojenom kráľovstve.

Mnohé z našich prípadov presadzovania programu bezpečného prístavu sa týkali organizácií, ktoré sa zapojili do programu, ale neobnovili si svoje ročné osvedčenie a napriek tomu vystupovali ako aktuálni členovia. Ako sa rozoberá v ďalšej časti, FTC sa tiež zaväzuje odhaľovať falošné vyhlásenia o účasti na rámci štítu na ochranu osobných údajov. Táto strategická činnosť v rámci presadzovania bude dopĺňať zvýšenú aktivitu ministerstva obchodu pri overovaní plnenia požiadaviek programu týkajúcich sa osvedčovania a opätovného osvedčovania, pri monitorovaní skutočného plnenia požiadaviek, a to aj s použitím dotazníkov pre účastníkov rámca, a pri zvýšenom úsilí o odhaľovanie falošných vyhlásení o členstve v rámci a zneužívania akejkoľvek certifikačnej značky rámca⁽²⁾.

II. PRIORITNÉ VYBAVOVANIE POSTÚPENÝCH ŽIADOSTÍ A VYŠETROVANIE

Rovnako ako v prípade programu bezpečného prístavu sa FTC zaväzuje prioritne vybavovať žiadosti týkajúce sa štítu na ochranu osobných údajov postúpené členskými štátmi EÚ. Uprednostňovať budeme aj veci týkajúce sa nedodržiavania samoregulačných usmernení v súvislosti s rámcom štítu na ochranu osobných údajov postúpené samoregulačnými orgánmi z oblasti ochrany súkromia a inými nezávislými orgánmi pre riešenie sporov.

S cieľom uľahčiť postupovanie žiadostí členskými štátmi EÚ na základe rámca FTC vypracováva štandardizovaný postup postupovania žiadostí a poskytuje členským štátom EÚ usmernenia o druhu informácií, ktoré by najlepšie pomohli FTC pri vyšetrovaní postúpených žiadostí. V rámci tohto úsilia určí FTC svoje kontaktné miesto pre žiadosti postúpené členskými štátmi EÚ. Najužitočnejšie je, ak orgán, ktorý žiadosť postupuje, vykoná predbežné vyšetrovanie údajného porušenia pravidiel a môže pri vyšetrovaní spolupracovať s FTC.

Po prijatí žiadosti postúpenej členským štátom EÚ alebo samoregulačným orgánom môže FTC vykonať celú škálu opatrení na riešenie nastolených problémov. Môžeme napríklad preskúmať podmienky spoločnosti v oblasti ochrany súkromia, získať ďalšie informácie priamo od spoločnosti alebo od tretích strán, ďalej konzultovať so subjektom, ktorý žiadosť postúpil, posúdiť, či ide o systematické porušovanie pravidiel alebo či je postihnutý značný počet spotrebiteľov, určiť, či postúpená žiadosť poukazuje na problémy, ktoré sú v právomoci ministerstva obchodu, posúdiť, či by pomohlo vzdelávanie spotrebiteľov a podnikov a v prípade potreby začať konanie na presadzovanie pravidiel.

FTC sa tiež zaväzuje k výmene informácií o postúpených žiadostiach s orgánmi presadzovania práva, ktoré žiadosti postúpili, vrátane informácií o stave vybavovania postúpených žiadostí, v súlade s právnymi predpismi a obmedzeniami týkajúcimi sa dôvernosti. Pokiaľ to bude možné vzhľadom na počet postúpených žiadostí a ich druh, poskytované informácie budú zahŕňať hodnotenie postúpených vecí vrátane opisu závažných nastolených problémov a každé opatrenie prijaté na riešenie porušenia zákona v jurisdikcii FTC. FTC tiež poskytne orgánu, ktorý žiadosť postúpil, spätnú väzbu o druhoch postúpených žiadostí, aby sa zvýšila efektívnosť úsilia o riešenie protiprávneho konania. Ak orgán presadzovania práva, ktorý žiadosť postúpil, požaduje informácie o stave vybavovania konkrétnej postúpenej žiadosti na

⁽¹⁾ Pozri vec *FTC/Karnani*, č. 2:09-cv-05276 (C.D. Cal. 20. mája 2011) (stipulated final order), dostupné na <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf>; pozri aj Lesley Fair, FTC Business Center Blog, Around the World in Shady Ways, <https://www.ftc.gov/blog/2011/06/around-world-shady-ways> (9. júna 2011).

⁽²⁾ List od Kena Hyatta, úradujúceho tajomníka ministerstva obchodu pre medzinárodný obchod, Úrad pre medzinárodný obchod, Vere Jourovej, komisárke pre spravodlivosť, spotrebiteľov a rodovú rovnosť.

účely vedenia vlastného konania na účely presadzovania predpisov, FTC odpovie s ohľadom na počet posudzovaných postúpených žiadostí a v súlade so zásadami dôvernosti a ďalšími právnymi požiadavkami.

FTC bude tiež úzko spolupracovať s orgánmi EÚ pre ochranu osobných údajov s cieľom poskytovať im pomoc pri presadzovaní predpisov. V určitých prípadoch by táto spolupráca mohla zahŕňať výmenu informácií a pomoc pri vyšetrovaní na základe zákona USA o bezpečnom internete (Safe Web Act), ktorý oprávňuje FTC na pomoc zahraničným orgánom presadzovania práva, ak zahraničný orgán presadzuje právne predpisy zakazujúce postupy značne podobné postupom zakázaným na základe právnych predpisov, ktoré presadzuje FTC ⁽¹⁾. Ako súčasť tejto pomoci môže FTC zdieľať informácie, ktoré získala v súvislosti so svojím vyšetrovaním, začať donucovací postup v mene orgánu EÚ pre ochranu osobných údajov, ktorý vykonáva svoje vlastné vyšetrovanie, a pokúšať sa o získanie ústneho svedectva svedkov alebo obžalovaných v súvislosti s konaním orgánu pre ochranu osobných údajov na účely presadenia predpisov, v súlade s požiadavkami zákona USA o bezpečnom internete. FTC pravidelne využíva túto právomoc na pomoc iným orgánom na celom svete vo veciach ochrany súkromia a spotrebiteľov ⁽²⁾.

Okrem prednostného vybavovania žiadostí týkajúcich sa štítu na ochranu osobných údajov, postúpených členskými štátmi EÚ a samoregulačnými orgánmi z oblasti ochrany súkromia ⁽³⁾, sa FTC zaväzuje v prípade potreby vyšetrovať možné porušenia rámca z vlastnej iniciatívy a s použitím celej škály nástrojov.

Počas vyše desiatich rokov FTC uskutočňuje rozsiahly program vyšetrovania problémov v oblasti ochrany súkromia a bezpečnosti týkajúcich sa obchodných organizácií. V rámci tohto vyšetrovania FTC bežne kontrolovala, či dotknutý subjekt uskutočňoval vyhlásenia týkajúce sa programu bezpečného prístavu. Ak subjekt takéto vyhlásenia uskutočňoval a vyšetrovaním sa zistilo zjavné porušenie zásad bezpečného prístavu, FTC zahrnula obvinenia z porušovania týchto zásad do svojich opatrení na presadzovanie programu. V tomto aktívnom prístupe budeme pokračovať aj pri realizácii nového rámca. Dôležité je, že FTC vykonáva oveľa viac vyšetrovaní, než sú tie, ktoré sa napokon skončia prijatím verejných opatrení na presadzovanie pravidiel. Mnohé vyšetrovania FTC sú uzavreté, pretože zamestnanci nezistia zjavné porušenie zákona. Keďže vyšetrovania FTC sú neverejné a dôverné, uzavretie vyšetrovania sa často nezverejňuje.

Takmer 40 opatrení na presadzovanie pravidiel, ktoré FTC začala uplatňovať vo vzťahu k programu bezpečného prístavu, sú dôkazom jej záväzku aktívne presadzovať cezhraničné programy ochrany súkromia. FTC bude vyhľadávať potenciálne porušenia rámca pri vyšetrovaní v oblasti ochrany súkromia a bezpečnosti, ktoré vykonávame pravidelne.

III. RIEŠENIE FALOŠNÝCH ALEBO PODVODNÝCH VYHLÁSENÍ O ZAPOJENÍ DO ŠTÍTU NA OCHRANU OSOBNÝCH ÚDAJOV

Ako už bolo uvedené vyššie, FTC bude prijímať opatrenia voči subjektom, ktoré uvádzajú nepravdivé vyhlásenia o svojej účasti na rámci štítu na ochranu osobných údajov. FTC bude prednostne posudzovať žiadosti postúpené ministerstvom obchodu, týkajúce sa organizácií, v prípade ktorých ministerstvo zistí, že neoprávnene tvrdia, že sú aktuálne zapojené do rámca, alebo že bez povolenia používajú certifikačnú značku rámca.

Okrem toho poznamenávame, že ak sa v podmienkach organizácie týkajúcich sa ochrany súkromia uvádza, že dodržiava zásady štítu na ochranu osobných údajov, a uvedená organizácia sa nezaregistruje na ministerstve obchodu ani svoju registráciu nepredĺži, táto skutočnosť ju sama osebe pravdepodobne neuchráni pred presadzovaním uvedených záväzkov rámca komisiou FTC.

⁽¹⁾ Pri rozhodovaní, či využiť svoju právomoc podľa zákona USA o bezpečnom internete, FTC okrem iného zvažuje: a) či žiadajúci orgán súhlasí, že poskytne alebo bude poskytovať FTC recipročnú pomoc; b) či by splnenie požiadavky nepoškodilo verejný záujem Spojených štátov a c) či sa vyšetrovanie alebo konanie na presadzovanie pravidiel žiadajúceho orgánu týka konania alebo praktík, ktoré spôsobujú alebo môžu spôsobiť ujmu značnému počtu osôb. 15 U.S.C. § 46 písm. j) ods. 3 Táto právomoc sa nevzťahuje na presadzovanie právnych predpisov týkajúcich sa hospodárskej súťaže.

⁽²⁾ Napríklad v rozpočtových rokoch 2012 – 2015 FTC využila svoju právomoc na výmenu informácií podľa zákona USA o bezpečnom internete pri odpovedaní na takmer 60 žiadostí zahraničných agentúr a vydala takmer 60 občianskoprávných výziev na podanie vysvetlenia (ktoré sú rovnocenné administratívnej výzve) v rámci pomoci pri 25 zahraničných vyšetrovaniach.

⁽³⁾ Hoci FTC nerieši sťažnosti jednotlivých spotrebiteľov ani pri nich nevystupuje ako mediátor, potvrdzuje, že sa bude prioritne zaoberať žiadosťami týkajúcimi sa štítu na ochranu osobných údajov postúpenými orgánmi EÚ pre ochranu osobných údajov. FTC okrem toho používa sťažnosti vo svojej databáze na ochranu spotrebiteľov, ktorá je prístupná mnohým ďalším orgánom presadzovania práva, s cieľom zisťovať trendy, určovať priority presadzovania pravidiel a identifikovať potenciálne ciele vyšetrovania. Občania EÚ môžu používať na podávanie sťažností FTC rovnaký systém ako občania USA, ktorý je dostupný na webovej lokalite www.ftc.gov/complaint. V prípade sťažností fyzických osôb, ktoré sa týkajú štítu na ochranu osobných údajov, však môže byť pre občanov EÚ najužitočnejšie, aby predkladali sťažnosti orgánu pre ochranu osobných údajov svojho členského štátu alebo orgánu alternatívneho riešenia sporov.

IV. MONITOROVANIE UZNESENÍ

FTC tiež potvrdzuje svoj záväzok monitorovať výkon uznesení týkajúcich sa presadzovania pravidiel s cieľom zabezpečiť dodržiavanie rámca štítu na ochranu osobných údajov.

V budúcich uzneseniach FTC týkajúcich sa rámca budeme dodržiavanie rámca vyžadovať prostredníctvom rôznych vhodných predbežných opatrení. Zahŕňa to zákaz uskutočňovania nepravdivých vyhlásení týkajúcich sa rámca a ďalších programov na ochranu súkromia, ak je toto konanie dôvodom základného opatrenia FTC.

Prípady, v ktorých FTC presadzovala pôvodný program bezpečného prístavu, sú poučné. V 36 prípadoch nepravdivých alebo klamlivých vyhlásení o osvedčení v rámci programu bezpečného prístavu sa každým uznesením obžalovanému zakazuje, aby uvádzal nepravdivé informácie o svojom zapojení do programu bezpečného prístavu alebo akéhokoľvek iného programu na ochranu súkromia alebo bezpečnosti, a od spoločnosti sa vyžaduje, aby sprístupnila FTC správy o súlade s predpismi. V prípadoch porušenia zásad bezpečného prístavu sa od daných spoločností požadovalo, aby zaviedli komplexné programy na ochranu súkromia a počas obdobia dvadsiatich rokov získavali nezávislé každoročné posúdenie týchto programov treťou stranou, ktorého výsledky musia poskytnúť FTC.

Porušenie správnych uznesení FTC môže viesť k občianskoprávnym trestom vo výške až 16 000 USD za každé nespĺnenie príkazu alebo 16 000 USD denne za pokračujúce neplnenie ⁽¹⁾, čo v prípade praktík, ktoré sa týkajú mnohých spotrebiteľov, môže viesť k sumám vo výške miliónov dolárov. V každom „consent order“ sú zahrnuté aj ustanovenia o podávaní správ a o dodržiavaní predpisov. Subjekty, na ktoré sa uznesenie vzťahuje, musia stanovený počet rokov uchovávať dokumenty preukazujúce, že dodržiavajú predpisy. S príkazmi sa musia oboznámiť aj zamestnanci zodpovední za zaistenie plnenia príkazu.

FTC systematicky monitoruje dodržiavanie príkazov týkajúcich sa programu bezpečného prístavu, ako to robí so všetkými svojimi príkazmi FTC berie presadzovanie svojich príkazov týkajúcich sa ochrany osobných údajov a bezpečnosti vážne a v prípade potreby podáva žaloby na ich presadenie. Napríklad, ako už bolo uvedené, spoločnosť Google zaplatila v dôsledku obvinení z porušovania príkazu FTC občianskoprávnú sankciu vo výške 22,5 milióna USD. Dôležité je, že príkazy FTC budú naďalej chrániť všetkých spotrebiteľov na celom svete, ktorí prichádzajú do styku s daným podnikom, nielen tých, ktorí podali sťažnosť.

A napokon, FTC bude naďalej viesť online zoznam spoločností, na ktoré sa vzťahujú príkazy v súvislosti s presadzovaním programu bezpečného prístavu a nového rámca štítu na ochranu osobných údajov ⁽²⁾. Zásady štítu na ochranu osobných údajov teraz navyše vyžadujú od spoločností, na ktoré sa vzťahuje uznesenie FTC alebo príkaz súdu z dôvodu nedodržiavania zásad, aby zverejnili všetky príslušné časti správ o dodržiavaní predpisov alebo hodnotiacich správ predložených FTC, ktoré sa týkajú rámca, a to v rozsahu zodpovedajúcom právnym a správny predpisom o zachovaní dôvernosti.

V. SÚČINNOSŤ S ORGÁNMI EÚ PRE OCHRANU OSOBNÝCH ÚDAJOV A SPOLUPRÁCA PRI PRESADZOVANÍ PRAVIDIEL

FTC uznáva významnú úlohu, ktorú zohrávajú orgány EÚ pre ochranu osobných údajov, pokiaľ ide o dodržiavanie pravidiel rámca, a vyzýva na intenzívnejšie konzultácie a spoluprácu pri presadzovaní pravidiel. Okrem konzultácií s orgánmi pre ochranu osobných údajov v konkrétnych veciach sa FTC zaväzuje, že sa bude zúčastňovať pravidelných stretnutí s určenými zástupcami pracovnej skupiny zriadenej podľa článku 29 s cieľom všeobecne prerokovať, ako zlepšiť spoluprácu pri presadzovaní pravidiel, pokiaľ ide o rámec. FTC sa bude tiež podieľať spolu so zástupcami ministerstva obchodu, Európskej komisie a pracovnej skupiny zriadenej podľa článku 29 na každoročnom preskúmaní rámca s cieľom diskutovať o jeho vykonávaní.

FTC tiež podnecuje tvorbu nástrojov, ktoré posilnia spoluprácu pri presadzovaní pravidiel s orgánmi EÚ pre ochranu osobných údajov, ako aj s ďalšími orgánmi na presadzovanie ochrany súkromia na celom svete. FTC predovšetkým spoločne s partnermi v oblasti presadzovania pravidiel v Európskej únii a na celom svete vlni spustila systém varovania v rámci globálnej siete pre presadzovanie ochrany súkromia (Global Privacy Enforcement Network) s cieľom vymieňať si informácie o vyšetrovaniach a podporovať koordináciu presadzovania pravidiel. Nástroj varovania v rámci siete by mohol byť obzvlášť užitočný v súvislosti s rámcom štítu na ochranu osobných údajov. FTC a orgány EÚ pre ochranu osobných údajov by ho mohli využívať na koordináciu v súvislosti s rámcom a ďalšími vyšetrovaniami týkajúcimi sa ochrany súkromia, a tiež ako východisko pre výmenu informácií s cieľom poskytnúť spotrebiteľom koordinovanú

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

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

a účinnejšiu ochranu súkromia. Tešíme sa na pokračovanie spolupráce so zapojenými orgánmi EÚ pri širšom zavádzaní systému varovania v rámci globálnej siete pre presadzovanie ochrany súkromia a pri vývoji iných nástrojov na zlepšenie spolupráce pri presadzovaní pravidiel v prípadoch týkajúcich sa ochrany súkromia vrátane tých, ktoré sa týkajú rámca.

FTC s potešením potvrdzuje svoj záväzok presadzovať nový rámec štítu na ochranu osobných údajov. Tešíme sa aj na pokračujúcu spoluprácu s kolegami z EÚ pri ochrane súkromia spotrebiteľov na oboch stranách Atlantiku.

S úctou

Edith Ramirez

predsedníčka

Dodatok A

Rámec štítu na ochranu osobných údajov medzi EÚ a USA v kontexte: Prehľad situácie v oblasti ochrany súkromia a bezpečnosti v USA

Ochrana, ktorú poskytuje rámec štítu na ochranu osobných údajov medzi EÚ a USA (ďalej len „rámec“), existuje v kontexte širšej ochrany súkromia, ktorú umožňuje právny systém USA ako celok. Po prvé, Federálna obchodná komisia Spojených štátov (Federal Trade Commission – ďalej len „FTC“) má rozsiahly program ochrany súkromia a bezpečnosti údajov pre obchodné činnosti, ktorý chráni spotrebiteľov na celom svete. Po druhé, situácia v oblasti ochrany súkromia a bezpečnosti spotrebiteľov v USA sa od roku 2000, keď bol prijatý pôvodný program bezpečného prístavu USA a EÚ, výrazne zmenila. Od toho obdobia bolo prijatých mnoho federálnych a štátnych zákonov týkajúcich sa ochrany súkromia a bezpečnosti a výrazne vzrástol počet súdnych žalôb v súvislosti s presadzovaním práva na súkromie. Široký rozsah právnej ochrany súkromia a bezpečnosti spotrebiteľov v USA, ktorý sa uplatňuje na postupy zaobchádzania s obchodnými údajmi, dopĺňa ochranu, ktorú fyzickým osobám z EÚ poskytuje nový rámec.

I. VŠEOBECNÝ PROGRAM FTC NA PRESADZOVANIE OCHRANY SÚKROMIA A BEZPEČNOSTI

FTC je najvýznamnejším orgánom USA na ochranu spotrebiteľov zameraným na ochranu súkromia v obchodnej oblasti. FTC má právomoc stíhať nekalé a klamlivé konanie alebo postupy, ktoré porušujú súkromie spotrebiteľov, a tiež presadzovať zákony cielenejšie zamerané na ochranu súkromia, ktoré chránia určité finančné informácie, informácie týkajúce sa zdravia, informácie o deťoch a informácie, ktoré sa využívajú na prijímanie niektorých rozhodnutí súvisiacich s nárokmi spotrebiteľov.

FTC má jedinečné skúsenosti s presadzovaním ochrany súkromia spotrebiteľov. Opatrenia FTC na presadzovanie práva sú zamerané na riešenie prípadov nezákonných postupov v offline aj online prostredí. FTC napríklad prijala opatrenia na presadzovanie práva voči známym spoločnostiam, akými sú Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC a Snapchat, ako aj voči menej známym spoločnostiam. FTC podala žalobu na podniky, ktoré údajne posielali spotrebiteľom nevyžiadané správy (spam), inštalovali im do počítačov sledovacie programy (spyware), nezabezpečili osobné informácie o spotrebiteľoch, klamlivo sledovali spotrebiteľov online, porušovali súkromie detí, nezákonne zhromažďovali informácie o mobilných zariadeniach spotrebiteľov a nezabezpečili zariadenia pripojené na internet a využívané na uchovávanie osobných informácií. Vo výsledných uzneseniach sa spravidla stanovilo trvalé monitorovanie zo strany FTC na obdobie dvadsiatich rokov, zakázalo sa ďalšie porušovanie zákona a uložili sa podnikom vysoké finančné pokuty za porušovanie týchto príkazov⁽¹⁾. Dôležité je, že uznesenia FTC nechránia len fyzické osoby, ktoré sa sťažovali na daný problém, ale chránia všetkých spotrebiteľov, ktorí s dotknutým podnikom prídu do styku. Pokiaľ ide o cezhraničnú ochranu, FTC má právomoc chrániť spotrebiteľov na celom svete pred postupmi uplatňovanými v USA⁽²⁾.

FTC doposiaľ riešila viac ako 130 prípadov týkajúcich sa nevyžiadaných správ (spam) a sledovacích programov (spyware), viac ako 120 prípadov týkajúcich sa porušovania zásady „nevolať“ v rámci telemarketingu, viac ako 100 prípadov opatrení podľa zákona o korektnom nakladaní so spotrebiteľskými informáciami (Fair Credit Reporting Act), takmer 60 prípadov týkajúcich sa ochrany bezpečnosti údajov, viac ako 50 prípadov všeobecných opatrení na ochranu súkromia, takmer 30 prípadov týkajúcich sa porušovania zákona Gramm-Leach-Bliley a viac ako 20 prípadov opatrení na presadzovanie zákona o ochrane súkromia detí v rámci online režimov (Children's Online Privacy Protection Act)⁽³⁾. Okrem riešenia týchto prípadov FTC tiež vydáva a publikuje varovné listy⁽⁴⁾.

⁽¹⁾ Každému subjektu, ktorý nesplní príkaz FTC, sa udelí civilná sankcia až do výšky 16 000 USD za každé nesplnenie, alebo 16 000 USD za každý deň pretrvávajúceho neplnenia. Pozri 15 U.S.C. § 45 ods. 1; 16 C.F.R. § 1.98 písm. c).

⁽²⁾ Kongres výslovne potvrdil právomoc FTC hľadať právne prostriedky nápravy vrátane odškodnenia v prípade akéhokoľvek konania alebo postupov v zahraničnom obchode, ktoré 1. spôsobujú alebo môžu spôsobiť primerane predvídateľnú ujmu v Spojených štátoch, alebo 2. predstavujú závažné konanie v Spojených štátoch. Pozri 15 U.S.C. § 45 písm. a) bod 4.

⁽³⁾ Komisia FTC v niektorých prípadoch týkajúcich sa ochrany súkromia a bezpečnosti údajov obvinila danú spoločnosť, že sa zapojila do nekalých aj klamlivých postupov. V týchto prípadoch tiež niekedy ide o údajné porušovanie viacerých zákonov, ako napríklad zákona o náležitom podávaní informácií o úverovej schopnosti zákazníkov, zákona Gramm-Leach-Bliley a zákona o ochrane súkromia detí v rámci online režimov.

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

V rámci dôsledného presadzovania ochrany súkromia FTC tiež pravidelne vyhľadáva prípady možného porušovania zásad programu bezpečného prístavu. Odkedy bol program bezpečného prístavu prijatý, FTC vykonala z vlastnej iniciatívy mnoho vyšetrovaní dodržiavania zásad bezpečného prístavu a v 39 prípadoch viedla konanie proti spoločnostiam z USA pre porušovanie zásad bezpečného prístavu. FTC bude pokračovať v tomto aktívnom prístupe tým, že presadzovanie nového rámca sa stane jej prioritou.

II. FEDERÁLNE A ŠTÁTNE ZÁKONY TÝKAJÚCE SA OCHRANY SÚKROMIA SPOTREBITEĽOV

V prehľade presadzovania zásad bezpečného prístavu, ktorý tvorí prílohu k rozhodnutiu Európskej komisie o primeranosti programu bezpečného prístavu, je uvedený súhrn mnohých federálnych a štátnych zákonov týkajúcich sa ochrany súkromia, ktoré boli v platnosti v čase prijatia programu bezpečného prístavu v roku 2000 ⁽¹⁾. Komerčné zhromažďovanie a využívanie osobných informácií v tom čase popri oddiele 5 zákona o Federálnej obchodnej komisii (FTC Act) upravovali mnohé federálne zákony vrátane: zákona o politike v oblasti káblvej komunikácie (Cable Communications Policy Act), zákona o ochrane súkromia vodičov motorových vozidiel (Driver's Privacy Protection Act), zákona o ochrane súkromia v rámci elektronickej komunikácie (Electronic Communications Privacy Act), zákona o elektronickom prevode finančných prostriedkov (Electronic Funds Transfer Act), zákona o náležitom podávaní informácií o úverovej schopnosti zákazníkov (Fair Credit Reporting Act), zákona Gramm-Leach-Bliley (Gramm-Leach-Bliley Act), zákona o práve na ochranu osobných finančných údajov (Right to Financial Privacy Act), zákona o ochrane spotrebiteľov využívajúcich telefónnu sieť (Telephone Consumer Protection Act) a zákona o ochrane súkromných videozáznamov (Video Privacy Protection Act). Analogické zákony týkajúce sa týchto oblastí majú aj mnohé štáty USA.

Od roku 2000 sa vykonali početné zmeny na federálnej úrovni aj na úrovni jednotlivých štátov, ktoré ďalej zvýšili ochranu súkromia spotrebiteľov ⁽²⁾. Na federálnej úrovni napríklad FTC v roku 2013 zmenila zákon o ochrane súkromia detí v rámci online režimov (Children's Online Privacy Protection Act) s cieľom zaviesť viaceré ďalšie opatrenia na ochranu osobných informácií o deťoch. FTC tiež vydala dva predpisy na vykonávanie zákona Gramm-Leach-Bliley, predpis o ochrane súkromia a predpis o zárukách, v rámci ktorých sa od finančných inštitúcií ⁽³⁾ vyžaduje, aby zverejnili svoje postupy výmeny informácií a zaviedli komplexný program informačnej bezpečnosti na ochranu spotrebiteľských informácií ⁽⁴⁾. Podobne aj zákon o spravodlivých a presných úverových transakciách (Fair and Accurate Credit Transactions Act), prijatý v roku 2003, dopĺňa dlhodobo platné zákony USA o úveroch tým, že stanovuje požiadavky na maskovanie a zdieľanie určitých citlivých finančných údajov a na zaobchádzanie s nimi. FTC na základe tohto zákona schválila viaceré pravidlá týkajúce sa okrem iného práva spotrebiteľov na bezplatnú výročnú správu o úveroch, požiadaviek na bezpečné zaobchádzanie s informáciami zo správ o spotrebiteľoch, práva spotrebiteľov na odmietnutie prijímania určitých ponúk úverov alebo poistenia, práva spotrebiteľov na odmietnutie použitia informácií poskytovaných pridruženou spoločnosťou pri predaji jej výrobkov a služieb a požiadaviek na finančné inštitúcie a veriteľov, aby zaviedli programy na odhaľovanie krádeží identity a na ich prevenciu ⁽⁵⁾. Okrem toho sa v roku 2013 revidovali pravidlá vyhlásené na základe zákona o prenosnosti a zúčtovateľnosti zdravotného poistenia (Health Insurance Portability and Accountability Act), keď sa pridali doplňujúce záruky na ochranu súkromia a bezpečnosti osobných informácií týkajúcich sa zdravia ⁽⁶⁾. Do platnosti vstúpili aj pravidlá chrániace spotrebiteľov pred neželanými telefonickými volaniami v rámci telemarketingu, automatickými telefonickými volaniami a nevyžiadanými správami (spam). Kongres tiež prijal zákony, v ktorých je stanovená požiadavka, aby spoločnosti zhromažďujúce informácie týkajúce sa zdravia upozornili spotrebiteľov v prípade porušenia pravidiel ⁽⁷⁾.

Aj jednotlivé štáty sú veľmi aktívne pri prijímaní zákonov týkajúcich sa ochrany súkromia a bezpečnosti. Od roku 2000 prijalo 47 štátov USA, District of Columbia, Guam, Portoriko a Panenské ostrovy zákony, v ktorých je stanovená

⁽¹⁾ Pozri Ministerstvo obchodu USA, Prehľad presadzovania zásad bezpečného prístavu (Safe Harbor Enforcement Overview), https://build.export.gov/main/safeharbor/eu/eg_main_018476.

⁽²⁾ Komplexnejší súhrn opatrení právnej ochrany v Spojených štátoch nájdete v dokumente Daniel J. Solove a Paul Schwartz, Information Privacy Law (5. vydanie 2015).

⁽³⁾ Finančné inštitúcie sú v zákone Gramm-Leach-Bliley vymedzené veľmi široko, aby zahŕňali všetky podniky, ktoré sa „významne podieľajú“ na poskytovaní finančných produktov alebo služieb. Patria tam napríklad podniky, ktoré sa zaoberajú preplácaním šekov, požičiavateľa peňazí na výplaty, sprostredkovatelia hypoték, odhadcovia osobného majetku alebo nehnuteľností a profesionálni daňoví poradcovia.

⁽⁴⁾ Podľa zákona o finančnej ochrane spotrebiteľa (Consumer Financial Protection Act) z roku 2010, Titul X Pub. L. 111 – 203, 124 Stat. 1955 (21. júl 2010) [známy tiež ako zákon Dodd-Franka o reforme Wall Street a ochrane spotrebiteľa (Dodd-Frank Wall Street Reform and Consumer Protection Act)], väčšina právomocí FTC v oblasti vytvárania pravidiel podľa zákona Gramm-Leach-Bliley bola presunutá na úrad pre finančnú ochranu spotrebiteľa. FTC si ponechala právomoc v oblasti presadzovania práva podľa zákona Gramm-Leach-Bliley, ako aj právomoc v oblasti vytvárania pravidiel podľa predpisu o zárukách a obmedzenú právomoc v oblasti vytvárania pravidiel podľa predpisu o ochrane súkromia, pokiaľ ide o predajcov motorových vozidiel.

⁽⁵⁾ Podľa zákona o finančnej ochrane spotrebiteľa (Consumer Financial Protection Act) sa komisia FTC o svoju úlohu pri presadzovaní zákona o náležitom podávaní informácií o úverovej schopnosti zákazníkov (Fair Credit Reporting Act) delí s úradom pre finančnú ochranu spotrebiteľa, ale právomoc v oblasti vytvárania pravidiel bola z veľkej časti presunutá na tento úrad (s výnimkou pravidiel týkajúcich sa výstrahy a zaobchádzania s údajmi).

⁽⁶⁾ Pozri 45 C.F.R. body 160, 162, 164.

⁽⁷⁾ Pozri napr. zákon o americkej obnove a reinvestíciách (American Recovery & Reinvestment Act) z roku 2009, Pub. L. č. 111 – 5, 123 Stat. 115 (2009) a príslušné nariadenia, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. bod 318.

požiadavka, aby podniky oznamovali jednotlivcom prípady porušenia bezpečnosti osobných informácií⁽¹⁾. V najmenej 32 štátoch a Portoriku platia zákony týkajúce sa zaobchádzania s údajmi, v ktorých sú stanovené požiadavky na zničenie osobných informácií alebo zaobchádzanie s nimi⁽²⁾. Viaceré štáty prijali aj všeobecné zákony týkajúce sa bezpečnosti údajov. Okrem toho štát Kalifornia prijal viaceré zákony týkajúce sa ochrany súkromia vrátane zákona, v ktorom je stanovená požiadavka, aby spoločnosti mali zavedené stratégie v oblasti ochrany súkromia a aby zverejnili svoje postupy pre uplatňovanie zásady „nesledovať“⁽³⁾, „objasňovacieho“ zákona („Shine the light“ law), v ktorom je stanovená požiadavka väčšej transparentnosti pre obchodníkov s údajmi⁽⁴⁾, a zákona, ktorým sa zavádza „tlačidlo vymazania“ umožňujúce maloletým osobám požiadať o vymazanie určitých informácií v sociálnych médiách⁽⁵⁾. Federálna vláda a vlády jednotlivých štátov USA na základe týchto zákonov a s pomocou ďalších orgánov ukládajú vysoké peňažné tresty spoločnostiam, ktoré nedodržiavajú zásady ochrany súkromia a bezpečnosti, pokiaľ ide o osobné informácie o spotrebiteľoch⁽⁶⁾.

Aj súkromnoprávne konania viedli k úspešným rozsudkom a dohodám, ktoré zabezpečujú zvýšenú ochranu súkromia a bezpečnosti údajov. Napríklad v roku 2015 spoločnosť Target súhlasila s vyplatením sumy 10 miliónov USD ako súčasťou dohody so zákazníkmi, ktorí namietali, že ich osobné finančné informácie boli prezradené v dôsledku rozsiahleho úniku údajov. V roku 2013 spoločnosť AOL súhlasila s vyplatením sumy 5 miliónov USD v rámci dohody o riešení skupinovej žaloby, ktorá sa týkala údajného neprimeraného odhalenia identity súvisiaceho so zverejnením vyhľadávaných výrazov stoviek tisícov členov AOL. Federálny súd okrem toho schválil vyplatenie sumy 9 miliónov USD spoločnosťou Netflix za údajné uchovávanie záznamov histórie prenájomov, čím došlo k porušeniu zákona o ochrane súkromných videozáznamov (Video Privacy Protection Act) z roku 1988. Federálne súdy v Kalifornii schválili dve samostatné dohody so spoločnosťou Facebook, jednu vo výške 20 miliónov USD a druhú vo výške 9,5 milióna USD, týkajúce sa zhromažďovania, využívania a zdieľania osobných informácií používateľov služieb spoločnosti. A v roku 2008 súd štátu Kalifornia schválil dohodu so spoločnosťou LensCrafters vo výške 20 miliónov USD za nezákonné zverejnenie informácií týkajúcich sa liečebnej starostlivosti o spotrebiteľa.

Skrátka, ako tento súhrn ukazuje, Spojené štáty zaisťujú výraznú právnu ochranu súkromia a bezpečnosti spotrebiteľov. Nový rámec štítu na ochranu osobných údajov, ktorý zabezpečuje významné záruky pre fyzické osoby z EÚ, bude fungovať v súčinnosti s týmto rozsiahlejším systémom, v ktorom je ochrana súkromia a bezpečnosti spotrebiteľov významnou prioritou.

⁽¹⁾ Pozri napr. National Conference of State Legislatures („NCSL“), State Security Breach Notification Laws (4. januára 2016), dostupné na <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

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

⁽³⁾ Obchodný a profesijný kódex štátu Kalifornia, §§ 22575 – 22579.

⁽⁴⁾ Občiansky kódex štátu Kalifornia, §§ 1798.80 – 1798.84.

⁽⁵⁾ Obchodný a profesijný kódex štátu Kalifornia, §§ 22580 – 22582.

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

PRÍLOHA V

List amerického ministra dopravy Anthonyho Foxxa

19. februára 2016

Komisárka Věra Jourová
Európska komisia
Rue de la Loi/Wetstraat 200
1049 Brusel
Belgicko

Vec: Rámec štítu na ochranu osobných údajov medzi EÚ a USA

Vážená pani komisárka Jourová,

Ministerstvo dopravy Spojených štátov amerických (ďalej len „ministerstvo“ alebo „MD“) oceňuje poskytnutú možnosť opísať svoju úlohu pri presadzovaní rámca štítu na ochranu osobných údajov medzi EÚ a USA. Tento rámec zohráva kľúčovú úlohu pri ochrane osobných údajov poskytovaných počas obchodných transakcií v stále viac prepojenom svete. Umožňuje podnikom uskutočňovať dôležité operácie v globálnom hospodárstve a zároveň zabezpečuje dôležitú ochranu súkromia spotrebiteľov z EÚ.

MD po prvýkrát verejne vyjadrilo svoj záväzok presadzovať uplatňovanie rámca bezpečného prístavu v liste zaslanom Európskej komisii pred vyše 15 rokmi. V tomto liste sa MD zaviazalo k dôslednému presadzovaniu zásad bezpečného prístavu. MD tento záväzok stále uplatňuje a týmto listom tento záväzok potvrdzuje.

MD obnovuje svoj záväzok zvlášť v nasledujúcich kľúčových oblastiach: 1. prioritné vyšetrovanie údajných porušení štítu na ochranu osobných údajov; 2. prijímanie náležitých opatrení na presadzovanie uplatňovania pravidiel voči subjektom uvádzajúcim nepravdivé alebo klamlivé tvrdenia o osvedčení v súvislosti so štítom na ochranu osobných údajov a 3. monitorovanie a zverejňovanie výkonu uznesení o porušení štítu na ochranu osobných údajov. Poskytujeme informácie o každom z týchto záväzkov a, na poskytnutie nevyhnutného kontextu, relevantné informácie o úlohe MD pri ochrane súkromia spotrebiteľov a presadzovaní rámca štítu na ochranu osobných údajov.

I. SÚVISLOSTI

A. Právomoc MD v oblasti ochrany súkromia

Ministerstvo je pevne odhodlané zabezpečovať ochranu informácií poskytovaných spotrebiteľmi leteckým spoločnostiam alebo predajcom leteniek. Právomoc MD konať v tejto oblasti je zakotvená v 49 U.S.C. 41712, ktorým sa prepravcovi alebo predajcovi leteniek zakazuje, aby sa pri predaji leteniek dopúšťal „nekalých alebo klamlivých praktík alebo používal nekalé metódy hospodárskej súťaže“, ktoré by spôsobili alebo by bolo pravdepodobné, že spôsobia spotrebiteľovi ujmu. Vzorom pre oddiel 41712 je oddiel 5 zákona o Federálnej obchodnej komisii (Federal Trade Commission – FTC) (15 U.S.C. 45). Podľa nášho výkladu predpis o nekalých alebo klamlivých praktikách leteckým spoločnostiam alebo predajcom leteniek zakazuje: 1. porušovať podmienky svojich podmienok ochrany súkromia alebo 2. zhromažďovať alebo zverejňovať súkromné informácie spôsobom, ktorý narušuje verejný poriadok, ktorý je nemorálny a spôsobuje spotrebiteľovi značnú ujmu, ktorá nie je vyvážená žiadnymi vyrovnávacími výhodami. Oddiel 41712 tiež vykladáme tak, že prepravcom alebo predajcom leteniek zakazuje: 1. porušiť akékoľvek pravidlo vydané ministerstvom, ktoré označuje konkrétne postupy v oblasti ochrany súkromia ako nekalé alebo klamlivé; alebo 2. porušovať zákon o ochrane súkromia detí v rámci online sietí (Children's Online Privacy Protection Act – COPPA) alebo pravidiel FTC na vykonávanie COPPA. Podľa federálnych právnych predpisov má MD výlučnú právomoc regulovať postupy leteckých spoločností v oblasti ochrany súkromia, pričom sa o právomoc, pokiaľ ide o postupy v oblasti ochrany osobných údajov pri predaji leteniek, delí s FTC.

To znamená, že ak sa prepravca alebo predajca leteniek verejne zaviazá k dodržiavaniu zásad ochrany súkromia podľa rámca štítu na ochranu osobných údajov, môže ministerstvo využiť zákonnú právomoc podľa oddielu 41712 na zabezpečenie dodržiavania týchto zásad. To znamená, že ak cestujúci poskytne informácie prepravcovi alebo predajcovi leteniek, ktorý sa zaviazal dodržiavať zásady ochrany súkromia podľa rámca štítu na ochranu osobných údajov, každé nedodržanie týchto zásad zo strany prepravcu alebo predajcu leteniek bude predstavovať porušenie oddielu 41712.

B. Postupy presadzovania predpisov

Úrad ministerstva pre presadzovanie predpisov a konania v oblasti letectva (ďalej len „Úrad pre presadzovanie predpisov v oblasti letectva“) vyšetruje a koná v prípadoch podľa 49 U.S.C. 41712. Presadzuje uplatňovanie zákonného zákazu nekalých a klamlivých praktík podľa oddielu 41712 najmä prostredníctvom rokovaní, prípravy príkazov na zdržanie sa konania a vypracovávaním uznesení o vymenovaní občianskoprávných sankcií. Úrad získava informácie o možných porušeníach prevažne prostredníctvom sťažností od fyzických osôb, cestovných kancelárií, leteckých spoločností a amerických a zahraničných vládnych agentúr. Spotrebiteľia môžu sťažnosti na letecké spoločnosti a predajcov leteniek týkajúce sa ochrany súkromia podávať prostredníctvom webovej lokality MD ⁽¹⁾.

Ak sa v rámci daného prípadu nedosiahne primerané a vhodné urovnanie, má Úrad pre presadzovanie predpisov v oblasti letectva právomoc začať konanie na presadzovanie právnych predpisov zahŕňajúce vypočutie dôkazov pred správnym sudcom MD. Správny sudca má právomoc vydávať príkazy na zdržanie sa ďalšieho porušovania a ukladať občianskoprávne sankcie. Porušenie oddielu 41712 môže mať za následok vydanie príkazu na zdržanie sa konania a uloženie občianskoprávných sankcií do výšky 27 500 USD za každé porušenie oddielu 41712.

Ministerstvo nemá právomoc priznať náhradu škody alebo poskytnúť peňažné odškodnenie jednotlivým sťažovateľom. Ministerstvo má však právomoc schvaľovať urovnania, ktoré vstúpia z vyšetrení začatých jeho Úradom pre presadzovanie predpisov v oblasti letectva a z ktorých majú spotrebiteľia priamy prospech (napr. hotovosť, kupóny), ako náhradu za peňažné pokuty, ktoré by sa inak museli zaplatiť americkej vláde. Dialo sa to v minulosti a môže sa to diať aj v súvislosti so zásadami rámca štítu na ochranu osobných údajov, ak si to vyžadujú okolnosti. Opakované porušovanie oddielu 41712 zo strany niektorej leteckej spoločnosti by tiež vzbudilo pochybnosti o pripravenosti danej leteckej spoločnosti dodržiavať zásady, čo by v mimoriadne závažných prípadoch mohlo viesť tomu, že sa daná letecká spoločnosť nebude viac považovať za prevádzkyschopnú a bude jej odňaté oprávnenie na prevádzkovanie hospodárskej činnosti.

MD dostalo do dnešného dňa pomerne málo sťažností týkajúcich sa údajných porušení ochrany súkromia predajcami leteniek alebo leteckými spoločnosťami. Keď k nim dôjde, vyšetrujú sa v súlade s vyššie uvedenými zásadami.

C. Právna ochrana poskytovaná MD v prospech spotrebiteľov z EÚ

Podľa oddielu 41712 sa zákaz nekalých alebo klamlivých praktík v leteckej doprave alebo pri predaji leteniek vzťahuje na amerických a zahraničných leteckých prepravcov, ako aj na predajcov leteniek. MD často prijíma opatrenia proti americkým a zahraničným leteckým spoločnostiam z dôvodu praktík, ktoré sa dotýkajú zahraničných aj amerických spotrebiteľov, na základe toho, že k praktikám leteckej spoločnosti došlo počas poskytovania prepravy do alebo zo Spojených štátov. MD využíva a bude naďalej využívať všetky opravné prostriedky, ktoré má k dispozícii, na ochranu zahraničných aj amerických spotrebiteľov pred nekalými alebo klamlivými praktikami v leteckej doprave zo strany regulovaných subjektov.

Vo vzťahu k leteckým spoločnostiam MD presadzuje aj uplatňovanie ďalších cielených právnych predpisov poskytujúcich ochranu aj spotrebiteľom mimo USA, ako je COPPA. COPPA okrem iného vyžaduje, aby prevádzkovatelia webových stránok a online služieb zameraných na deti alebo stránok určených pre širokú verejnosť, ktoré úmyselne zhromažďujú osobné informácie od detí mladších ako 13 rokov, poskytovali upozornenie pre rodičov a získavali overiteľný súhlas rodičov. Webové stránky a služby prevádzkované poskytovateľmi so sídlom v USA, na ktoré sa vzťahuje tento zákon a na ktorých sa zhromažďujú osobné informácie od detí zo zahraničia, musia spĺňať požiadavky stanovené v uvedenom zákone. Webové stránky a online služby prevádzkované poskytovateľmi so sídlom v zahraničí musia tiež spĺňať požiadavky stanovené v uvedenom zákone, ak sa zameriavajú na deti v Spojených štátoch alebo sa na nich úmyselne zhromažďujú osobné informácie od detí v Spojených štátoch. V rozsahu, v akom americké alebo zahraničné letecké spoločnosti pôsobiace v Spojených štátoch porušujú COPPA, má MD právomoc na prijímanie opatrení na presadzovanie predpisov.

II. PRESADZOVANIE UPLATŇOVANIA ŠTÍTU NA OCHRANU OSOBNÝCH ÚDAJOV

Ak sa letecká spoločnosť alebo predajca leteniek rozhodne zapojiť do rámca štítu na ochranu osobných údajov a ministerstvu príde sťažnosť, že takáto letecká spoločnosť alebo takýto predajca leteniek rámec údajne porušil, prijme ministerstvo nasledujúce kroky na dôrazné presadenie uplatňovania rámca.

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

A. Prioritné vyšetrowanie údajných porušení

Úrad ministerstva pre presadzovanie predpisov v oblasti letectva vyšetrí každú sťažnosť na údajné porušovanie štítu na ochranu osobných údajov (vrátane sťažností prijatých od orgánov pre ochranu osobných údajov EÚ) a tam, kde existuje dôkaz o porušovaní, prijme opatrenia na presadzovanie uplatňovania. Úrad pre presadzovanie predpisov v oblasti letectva bude okrem toho spolupracovať s FTC a ministerstvom obchodu a prioritne sa bude zaoberať tvrdeniami, že regulované subjekty nedodržiavajú záväzky v oblasti ochrany súkromia prijaté v rámci štítu na ochranu osobných údajov.

Po prijatí oznámenia o údajnom porušení rámca štítu na ochranu osobných údajov môže Úrad ministerstva pre presadzovanie predpisov v oblasti letectva v rámci vyšetrovania prijať rôzne kroky. Môže napríklad preskúmať podmienky ochrany súkromia predajcu leteniek alebo leteckej spoločnosti, získať ďalšie informácie od predajcu leteniek alebo leteckej spoločnosti alebo tretích strán, obrátiť sa znovu na sťažovateľa a posúdiť, či ide o systematické porušovanie pravidiel alebo či je postihnutý značný počet spotrebiteľov. Ďalej určí, či sa daný prípad týka záležitostí patriacich do rozsahu pôsobnosti ministerstva obchodu alebo FTC, posúdi, či by pomohlo vzdelávanie spotrebiteľov a podnikov, a v prípade potreby začne konanie na presadzovanie predpisov.

Ak ministerstvo získa informáciu o možnom porušovaní štítu na ochranu osobných údajov zo strany predajcov leteniek, bude konanie vo veci koordinovať s FTC. Taktiež budeme FTC a ministerstvo obchodu informovať o výsledku všetkých opatrení na presadzovanie uplatňovania štítu na ochranu osobných údajov.

B. Riešenie nepravdivých alebo klamlivých tvrdení o zapojení do štítu

Ministerstvo je odhodlané vyšetrovať porušenia štítu na ochranu osobných údajov vrátane nepravdivých alebo klamlivých tvrdení o zapojení do programu štítu na ochranu osobných údajov. Prioritne sa budeme zaoberať žiadosťami postúpenými ministerstvom obchodu týkajúcimi sa organizácií, o ktorých zistí, že neoprávnene tvrdia, že sú v súčasnosti zapojené do štítu na ochranu osobných údajov, alebo že bez oprávnenia používajú certifikačnú značku rámca štítu na ochranu osobných údajov.

Ďalej upozorňujeme, že ak sa v podmienkach ochrany osobných údajov organizácie uvádza, že dodržiava základné zásady štítu na ochranu osobných údajov, skutočnosť, že nevykoná alebo si nepredĺži registráciu na ministerstve obchodu, pravdepodobne sama osebe nechráni organizáciu od presadenia uplatnenia takýchto záväzkov zo strany MD.

C. Monitorovanie a zverejňovanie výkonu uznesení o porušení štítu na ochranu osobných údajov

Úrad ministerstva pre presadzovanie predpisov v oblasti letectva zostáva tiež naďalej odhodlaný podľa potreby monitorovať príkazy týkajúce sa presadzovania pravidiel s cieľom zaistiť dodržiavanie programu štítu na ochranu osobných údajov. Konkrétne, ak úrad vydá uznesenie nariaďujúce leteckej spoločnosti alebo predajcovi leteniek, aby sa zdržali budúcich porušení štítu na ochranu osobných údajov a oddielu 41712, bude monitorovať, či daný subjekt dodržiava ustanovenie o zdržaní sa konania uvedené v príkaze. Úrad ďalej zabezpečí, aby boli príkazy vo veciach štítu na ochranu osobných údajov dostupné na jeho webovej lokalite.

Tešíme sa na ďalšiu spoluprácu s našimi federálnymi partnermi a zainteresovanými stranami z EÚ v záležitostiach štítu na ochranu osobných údajov.

Dúfam, že tieto informácie budú pre Vás užitočné. Ak máte ešte nejaké otázky alebo potrebujete ďalšie informácie, môžete sa so mnou kedykoľvek skontaktovať.

S úctou

Anthony R. Foxx

minister dopravy

PRÍLOHA VI

**List generálneho právneho zástupcu Roberta Litta
Úrad riaditeľa národnej spravodajskej služby**

22. februára 2016

Pán Justin S. Antonipillai
právny zástupca
Ministerstvo obchodu USA
1401 Constitution Ave., NW
Washington, DC 20230

Pán Ted Dean
zástupca námestníka
Správa zahraničného obchodu (ITA)
1401 Constitution Ave., NW
Washington, DC 20230

Vážený pán Antonipillai, vážený pán Dean,

v priebehu uplynulého dva a pol roka poskytli Spojené štáty v rámci rokovaní o šтите na ochranu osobných údajov medzi EÚ a USA podstatné informácie o fungovaní zhromažďovania informácií spravodajskými službami Spojených štátov prostredníctvom signálového spravodajstva. Išlo okrem iného o informácie o právnom rámci upravujúcom túto oblasť, viacvrstvovom dohľade nad týmito činnosťami, rozsiahlej transparentnosti týchto činností a celkovej ochrane súkromia a občianskych slobôd, ktoré mali Európskej komisii pomôcť pri rozhodovaní o primeranosti týchto ochranných opatrení, ktoré sa týkajú výnimky z uplatňovania zásad šтите na ochranu osobných údajov z dôvodov národnej bezpečnosti. V tomto dokumente sa uvádza zhrnutie poskytnutých informácií.

I. PPD-28 A VYKONÁVANIE ČINNOSTÍ AMERICKÉHO SIGNÁLOVÉHO SPRAVODAJSTVA

Spravodajské služby USA zhromažďujú zahraničné spravodajské informácie dôkladne kontrolovaným spôsobom, v prísnom súlade s americkými právnymi predpismi a pod viacúrovňovým dohľadom, pričom dôraz sa kladie na dôležité zahraničné spravodajské informácie a priority národnej bezpečnosti. Zhromažďovanie informácií prostredníctvom signálového spravodajstva v USA upravuje celá škála zákonov a politík vrátane Americkej ústavy, zákona o sledovaní v rámci zahraničného spravodajstva (50 U.S.C. § 1801 a nasl.) (Foreign Intelligence Surveillance Act – FISA), vykonávacieho nariadenia č. 12333 a jeho vykonávacích postupov, prezidentských usmernení a početných postupov a usmernení schválených súdom FISA a generálnym prokurátorom, ktorými sa zavádzajú dodatočné pravidlá obmedzujúce zhromažďovanie, uchovávanie, používanie a šírenie zahraničných spravodajských informácií ⁽¹⁾.

a) **Prehľad PPD 28**

V januári 2014 predniesol prezident Obama prejav, v ktorom predstavil rôzne reformy činností amerického signálového spravodajstva, a vydal prezidentskú politickú smernicu 28 (Presidential Policy Directive 28 – PPD-28) týkajúcu sa týchto činností ⁽²⁾. Prezident zdôraznil, že činnosti amerického signálového spravodajstva pomáhajú zabezpečiť nielen našu krajinu a naše slobody, ale aj bezpečnosť a slobody iných krajín vrátane členských štátov EÚ, ktoré informácie získané americkými spravodajskými agentúrami využívajú pri ochrane svojich vlastných občanov.

PPD-28 stanovuje súbor zásad a požiadaviek, ktoré sa vzťahujú na všetky činnosti amerického signálového spravodajstva a na všetkých ľudí bez ohľadu na štátnu príslušnosť alebo bydlisko. Zvlášť stanovuje určité požiadavky na postupy s cieľom riešiť otázky zhromažďovania, uchovávanie a šírenia osobných informácií o osobách, ktoré nie sú občanmi ani rezidentmi USA, získaných v rámci amerického signálového spravodajstva. Tieto požiadavky sú vysvetlené podrobnejšie ďalej, ale súhrnným spôsobom:

- V PPD sa opakovane zdôrazňuje, že Spojené štáty zhromažďujú informácie prostredníctvom signálového spravodajstva len v súlade s oprávneniami stanovenými v zákonoch, vykonávacích nariadeniach a iných prezidentských smerniciach.

⁽¹⁾ Ďalšie informácie týkajúce sa činností amerického zahraničného spravodajstva sú zverejnené online a verejne prístupné prostredníctvom stránky IC on the Record (www.icontherecord.tumblr.com), verejnej webovej lokality Úradu riaditeľa národnej spravodajskej služby (Office of the Director of National Intelligence – ODNI) venovanej posilňovaniu transparentnosti spravodajských činností vlády.

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

- V PPD sa stanovujú postupy na zaistenie toho, že sa činnosti signálového spravodajstva budú vykonávať len v záujme dosahovania legitímnych a oprávnených cieľov v oblasti národnej bezpečnosti.
- PPD tiež vyžaduje, aby sa pri plánovaní činností zhromažďovania informácií prostredníctvom signálového spravodajstva zohľadňovala ochrana súkromia a občianskych slobôd. Spojené štáty predovšetkým nezhromažďujú spravodajské informácie s cieľom potláčať alebo obťažovať osoby, ktoré ich kritizujú alebo s nimi nesúhlasia; s cieľom znevýhodňovať ľudí na základe ich etnickej a rasovej príslušnosti, pohlavia, sexuálnej orientácie alebo vierovyznania; alebo s cieľom poskytnúť obchodnú konkurenčnú výhodu americkým spoločnostiam a americkým hospodárskym odvetviám.
- PPD nariaďuje, aby dané zhromažďovanie informácií prostredníctvom signálového spravodajstva bolo čo najviac prispôbené konkrétnym situáciám a aby sa informácie hromadne získavané prostredníctvom signálového spravodajstva mohli používať len na konkrétne stanovené účely.
- PPD nariaďuje, aby spravodajské služby prijali postupy „náležite koncipované tak, aby minimalizovali šírenie a uchovávanie osobných informácií zhromaždených v rámci činností signálového spravodajstva“ a zvlášť aby sa určité ochranné opatrenia vo vzťahu k osobným informáciám amerických občanov alebo rezidentov rozšírili aj na informácie osôb, ktoré nie sú občanmi ani rezidentmi USA.
- Boli prijaté a zverejnené postupy agentúr na vykonanie PPD-28.

Uplatniteľnosť postupov a ochrany uvedených v tomto liste na štít na ochranu osobných údajov je jasná. Po postúpení údajov spoločnostiam v Spojených štátoch v súlade so štítom na ochranu osobných údajov, alebo v skutočnosti akýmkoľvek spôsobom, môžu americké spravodajské agentúry vyžadovať tieto údaje od takýchto spoločností len na základe žiadosti, ktorá je v súlade s FISA alebo je podaná v súlade s jedným zo zákonných ustanovení o príkaze na vydanie informácií z dôvodu národnej bezpečnosti (National Security Letter), o ktorých sa hovorí ďalej (¹). Okrem toho, bez potvrdenia alebo popretia mediálnych správ, v ktorých sa objavujú tvrdenia, že spravodajské služby USA zhromažďujú údaje z transatlantických káblov počas prenosu do Spojených štátov, ak by americké spravodajské služby zhromažďovali údaje z transatlantických káblov, robili by to v súlade s obmedzeniami a ochrannými opatreniami uvedenými v tomto liste vrátane požiadaviek PPD-28.

b) Obmedzenia zhromažďovania informácií

V PPD-28 sa stanovuje niekoľko dôležitých všeobecných zásad, ktorými sa riadi zhromažďovanie informácií prostredníctvom signálového spravodajstva:

- Zhromažďovanie informácií prostredníctvom signálového spravodajstva musí byť povolené na základe zákona alebo prezidentského povolenia a musí sa uskutočňovať v súlade s ústavou a zákonom.
- Pri plánovaní činností signálového spravodajstva sa musí zohľadňovať ochrana súkromia a občianskych slobôd.
- Informácie sa budú prostredníctvom signálového spravodajstva zhromažďovať len v prípade existencie platného účelu z hľadiska zahraničného spravodajstva alebo kontrarozviedky.
- Spojené štáty nebudú zhromažďovať informácie prostredníctvom signálového spravodajstva na účely potlačania alebo obťažovania osôb, ktoré ich kritizujú alebo s nimi nesúhlasia.
- Spojené štáty nebudú zhromažďovať informácie prostredníctvom signálového spravodajstva s cieľom znevýhodňovať ľudí na základe ich etnickej a rasovej príslušnosti, pohlavia, sexuálnej orientácie alebo vierovyznania.
- Spojené štáty nebudú zhromažďovať informácie prostredníctvom signálového spravodajstva s cieľom poskytnúť obchodnú konkurenčnú výhodu americkým spoločnostiam a hospodárskym odvetviám.
- Činnosť amerického signálového spravodajstva musí byť vždy čo najviac prispôbená konkrétnym situáciám, pričom sa musí brať do úvahy dostupnosť iných zdrojov informácií. To okrem iného znamená, že kedykoľvek je to možné, vykonávajú sa činnosti zhromažďovania informácií prostredníctvom signálového spravodajstva cieľovým spôsobom, nie hromadne.

Požiadavka, aby bola činnosť signálového spravodajstva „čo najviac prispôbená konkrétnym situáciám“, sa vzťahuje na spôsob zhromažďovania informácií prostredníctvom signálového spravodajstva, ako aj na to, aké informácie sa v skutočnosti zhromažďujú. Napríklad pri rozhodovaní o tom, či sa majú zhromažďovať informácie prostredníctvom

(¹) Orgány presadzovania práva alebo regulačné orgány môžu požadovať informácie od spoločností na účely vyšetrovania v Spojených štátoch na základe iných trestnoprávných, občianskoprávných a regulačných právomocí, ktoré nie sú predmetom tohto dokumentu, ktorý sa obmedzuje na právomoci v oblasti národnej bezpečnosti.

signálového spravodajstva, musia spravodajské služby zväziť dostupnosť iných informácií vrátane diplomatických alebo verejných zdrojov a prioritne zhromažďovať informácie týmito cestami, kde je to vhodné a uskutočniteľné. Okrem toho by sa na základe pravidiel činnosti zložiek spravodajských služieb malo vyžadovať, aby bolo zhromažďovanie informácií, pokiaľ je to možné, zamerané na konkrétne ciele alebo témy zahraničného spravodajstva prostredníctvom použitia diskriminantov (napr. konkrétnych zariadení, selektorov a identifikátorov).

Je dôležité pozerať sa na informácie poskytované Komisii ako na celok. Rozhodnutia o tom, čo je „uskutočniteľné“ alebo „realizovateľné“ sa neponechávajú na vlastné uváženie fyzickým osobám, ale podliehajú pravidlám, ktoré agentúry prijali na základe PPD-28 – a ktoré boli verejne prístupné –, a iným procesom opísaným v tomto dokumente ⁽¹⁾. Ako sa hovorí v PPD-28, hromadné zhromažďovanie informácií prostredníctvom signálového spravodajstva je zhromažďovanie, ktoré „sa z technických alebo operačných dôvodov uskutočňuje bez použitia diskriminantov (napr. konkrétnych identifikátorov, selektorov a pod.)“. V tomto zmysle sa v PPD-28 uznáva, že zložky spravodajských služieb musia za určitých okolností zhromažďovať informácie prostredníctvom signálového spravodajstva hromadným spôsobom, aby identifikovali nové alebo vznikajúce hrozby a iné informácie kľúčové z hľadiska národnej bezpečnosti, ktoré sú často ukryté v rámci rozsiahleho a komplexného systému moderných globálnych komunikácií. Tiež sa v nej uznávajú obavy týkajúce sa ochrany súkromia a občianskych slobôd, ktoré vznikajú pri hromadnom zhromažďovaní informácií prostredníctvom signálového spravodajstva. PPD-28 sa preto spravodajským službám nariaďuje, aby sa prioritne zameriavali na alternatívy, ktoré umožňujú uskutočňovanie skôr cieleného ako hromadného zhromažďovania informácií prostredníctvom signálového spravodajstva. V súlade s tým by mali zložky spravodajských služieb, pokiaľ je to možné, vykonávať skôr cielené ako hromadné zhromažďovanie informácií prostredníctvom signálového spravodajstva ⁽²⁾. Týmto zásadami sa zaisťuje, aby sa z výnimky na vykonávanie hromadného zhromažďovania nestalo všeobecné pravidlo.

Pokiaľ ide o pojem „primeranosť“, ide o základnú zásadu amerického práva. Znamená, že od zložiek spravodajských služieb sa nebude vyžadovať, aby prijali všetky teoreticky možné opatrenia, ale skôr budú musieť vyvážiť svoje úsilie ochrániť legitímne záujmy v oblasti ochrany súkromia a občianskych slobôd a praktické potreby činností signálového spravodajstva. Aj v tomto prípade boli pravidlá agentúr sprístupnené a môžu poskytnúť ubezpečenie, že pojmom „náležite koncipované tak, aby minimalizovali šírenie a uchovávanie osobných informácií“ sa neoslabuje všeobecné pravidlo.

V PPD-28 sa tiež stanovuje, že informácie zhromažďované prostredníctvom signálového spravodajstva hromadným spôsobom sa môžu používať len na šesť konkrétnych účelov: odhaľovanie určitých činností zahraničných mocností a prijímanie opatrení proti nim; boj proti terorizmu; boj proti šíreniu zbraní hromadného ničenia; kybernetická bezpečnosť; odhaľovanie hrozieb pre americké alebo spojenecké ozbrojené sily a prijímanie opatrení proti nim a boj proti nadnárodným hrozbám trestnej činnosti vrátane obchádzania sankcií. Prezidentov poradca pre otázky národnej bezpečnosti, po porade s riaditeľom národnej spravodajskej služby (Director for National Intelligence – DNI), každoročne preskúma tieto prípustné použitia informácií hromadne zhromaždených v rámci signálového spravodajstva, aby posúdil, či nie je potrebné ich zmeniť. DNI tento zoznam v čo najväčšom možnom rozsahu verejne prístupný, v súlade so záujmami národnej bezpečnosti. Týmto sa poskytuje dôležité a transparentné obmedzenie používania informácií hromadne zhromaždených prostredníctvom signálového spravodajstva.

Okrem toho spravodajské agentúry vykonávajúce PPD-28 zdokonalili existujúce analytické postupy a normy pre vyhľadávanie nevyhodnotených informácií v rámci signálového spravodajstva ⁽³⁾. Analytici musia svoje hľadané výrazy a techniky štruktúrovať tak, aby sa zabezpečilo, že sú vhodné na identifikovanie spravodajských informácií relevantných z hľadiska platnej úlohy zahraničného spravodajstva alebo presadzovania práva. Na tento účel sa musia spravodajské agentúry pri vyhľadávaní informácií o osobách zameriavať na kategórie informácií získavaných v rámci signálového spravodajstva zodpovedajúce požiadavke zahraničného spravodajstva alebo presadzovania práva, aby sa zabránilo používaniu osobných informácií nesúvisiacich s požiadavkami zahraničného spravodajstva alebo presadzovania práva.

Je dôležité zdôrazniť, že akékoľvek činnosti hromadného zhromažďovania týkajúce sa internetovej komunikácie, ktoré vykonávajú spravodajské služby USA prostredníctvom signálového spravodajstva, prebiehajú na malej časti internetu. Používaním cielených hľadaných výrazov, ako sa opisuje vyššie, sa okrem toho zaisťuje, aby sa k analytikom na preskúmanie dostali len tie informácie, o ktorých sa predpokladá, že môžu mať spravodajskú hodnotu. Účelom týchto obmedzení je chrániť súkromie a občianske slobody všetkých osôb bez ohľadu na ich štátnu príslušnosť a bydlisko.

⁽¹⁾ Dostupné na adrese www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Týmto postupmi sa realizujú koncepcie zacieleného prístupu a prispôsobenia konkrétnym situáciám, o ktorých sa hovorí v tomto liste, spôsobom špecifickým pre každú zložku spravodajských služieb.

⁽²⁾ Ako príklad možno uviesť postupy NSA, ktorými sa vykonáva PPD-28, v ktorých sa uvádza, že „pokiaľ je to možné, zhromažďovanie sa bude uskutočňovať pomocou jedného alebo viacerých selektorov s cieľom zamerať zhromažďovanie na konkrétne ciele zahraničného spravodajstva (napr. na konkrétneho známeho medzinárodného teroristu alebo teroristickú skupinu) alebo na konkrétne témy zahraničného spravodajstva (napr. šírenie zbraní hromadného ničenia zahraničnou mocnosťou alebo jej agentmi)“.

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

Spojené štáty uplatňujú prepracované postupy na zaistenie toho, aby sa činnosti signálového spravodajstva vykonávali len v záujme dosahovania príslušných cieľov v oblasti národnej bezpečnosti. Prezident každý rok stanoví najvyššie národné priority, pokiaľ ide o zhromažďovanie zahraničných spravodajských informácií, čomu predchádza rozsiahly, formálny medziagentúrny proces. DNI je zodpovedný za premietnutie týchto spravodajských priorít do rámca národných spravodajských priorít (National Intelligence Priorities Framework – NIPF). Smernicou PPD-28 sa posilnil a vylepšil medziagentúrny proces s cieľom zaistiť, aby všetky spravodajské priority spravodajských služieb preskúmali a schválili vysokopostavení politickí činitelia. Smernica o spravodajských službách (Intelligence Community Directive – ICD) 204 poskytuje ďalšie usmernenia k NIPF a v januári 2015 bola aktualizovaná s cieľom zapracovať požiadavky PPD-28 ⁽¹⁾. Hoci je NIPF utajený, o informáciách týkajúcich sa konkrétnych priorít amerického zahraničného spravodajstva sa každoročne informuje v odtajnenom *posúdení celosvetových hrozieb*, (Worldwide Threat Assessment) DNI, ktoré je tiež dostupné na webovej stránke ODNI.

Priority v rámci NIPF sú stanovené pomerne všeobecne. Zahŕňajú témy ako sledovanie kapacít konkrétnych zahraničných protivníkov v oblasti jadrových a balistických rakiet, účinky korupcie súvisiacej s drogovými kartelmi a porušovanie ľudských práv v konkrétnych krajinách. A nevzťahujú sa len na signálové spravodajstvo, ale na všetky spravodajské činnosti. Organizácia, ktorá je zodpovedná za premietnutie priorít stanovených v rámci NIPF do samotného zhromažďovania informácií prostredníctvom signálového spravodajstva, sa nazýva Národný výbor pre signálové spravodajstvo (National Signals Intelligence Committee – SIGCOM). Pracuje pod záštitou riaditeľa Národnej bezpečnostnej agentúry (National Security Agency – NSA), ktorý je vykonávacím nariadením č. 12333 definovaný ako „funkčný manažér pre signálové spravodajstvo“ zodpovedný za dohľad nad signálovým spravodajstvom vo všetkých zložkách spravodajských služieb pod dohľadom ministra obrany aj DNI, ako aj za jeho koordináciu. V SIGCOM sú združení zástupcovia zo všetkých spravodajských agentúr a po tom, ako Spojené štáty plne vykonajú PPD-28, budú v ňom mať plné zastúpenie aj iné ministerstvá a agentúry so záujmom na politike v oblasti signálového spravodajstva.

Všetky americké ministerstvá a agentúry, ktoré využívajú zahraničné spravodajstvo, predkladajú svoje žiadosti o zhromažďovanie informácií SIGCOM. SIGCOM tieto žiadosti posudzuje, zisťuje, aby boli v súlade s NIPF a prisudzuje im prioritu na základe kritérií ako:

- Môže signálové spravodajstvo v tomto prípade poskytnúť užitočné informácie alebo sa môže danej požiadavke vyhovieť použitím lepších alebo nákladovo efektívnejších zdrojov informácií, ako sú snímky alebo verejne dostupné informácie?
- Aká kritická je potreba týchto informácií? Ak má vysokú prioritu v rámci NIPF, väčšinou bude mať vysokú prioritu v rámci signálového spravodajstva.
- Aký druh signálového spravodajstva by sa mohol použiť?
- Je zhromažďovanie čo najviac prispôbené danej situácii? Mali by sa uplatniť časové, zemepisné alebo iné obmedzenia?

V rámci procesu požiadaviek na signálové spravodajstvo sa tiež vyžaduje dôkladné zváženie iných faktorov, konkrétne:

- Je cieľ zhromažďovania alebo metodika zhromažďovania zvlášť citlivá? Ak áno, bude si vyžadovať posúdenie vysoko-postavenými politickými činiteľmi.
- Bude zhromažďovanie informácií predstavovať neodôvodnené riziko pre súkromie a občianske slobody bez ohľadu na štátnu príslušnosť?
- Sú na ochranu súkromia alebo záujmov národnej bezpečnosti potrebné dodatočné ochranné opatrenia, pokiaľ ide o šírenie a uchovávanie?

A napokon, na konci procesu, sa priority odobrené SIGCOM postúpia vyškoleným pracovníkom NSA, ktorí vykonávajú prieskum a identifikujú konkrétne selektory, ako sú telefónne čísla alebo e-mailové adresy, na základe ktorých by sa mali zhromažďovať zahraničné spravodajské informácie zodpovedajúce týmto prioritám. Každý selektor sa musí pred zadáním do systémov zhromažďovania informácií NSA preskúmať a schváliť. Ale aj potom bude to, či a kedy sa dané

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

zhromažďovanie informácií uskutoční, čiastočne závisieť od iných faktorov, ako je napríklad dostupnosť príslušných zdrojov pre zhromažďovanie informácií. Týmto procesom sa zaisťuje, že ciele zhromažďovania informácií v rámci signálového spravodajstva odrážajú platné a dôležité potreby v rámci zahraničného spravodajstva. A, samozrejme, keď sa uskutočňuje zhromažďovanie informácií v súlade s FISA, musia NSA a ďalšie agentúry uplatňovať dodatočné obmedzenia schválené Súdom pre sledovanie v rámci zahraničného spravodajstva. Stručne povedané, ani NSA ani žiadna iná americká spravodajská agentúra nerozhoduje sama o tom, aké informácie sa majú zhromažďovať.

Celkove sa týmto procesom zaručuje, aby všetky americké spravodajské priority určovali politickí činitelia, ktorí najlepšie dokážu identifikovať požiadavky na americké zahraničné spravodajstvo, a aby títo politickí činitelia brali do úvahy nielen potenciálnu hodnotu zhromažďovania informácií, ale aj riziká spojené s týmto získavaním vrátane rizík pre súkromie, národné hospodárske záujmy a zahraničné vzťahy.

Pokiaľ ide o údaje prenášané do Spojených štátov v súlade so štítom na ochranu osobných údajov, hoci Spojené štáty nemôžu potvrdiť ani poprieť konkrétne spravodajské metódy alebo operácie, požiadavky PPD-28 sa vzťahujú na všetky operácie v rámci signálového spravodajstva uskutočňované Spojenými štátmi bez ohľadu na druh alebo zdroj údajov, ktoré sa zhromažďujú. Tiež treba povedať, že obmedzenia a ochranné opatrenia vzťahujúce sa na zhromažďovanie informácií prostredníctvom signálového spravodajstva sa vzťahujú na informácie zhromažďované prostredníctvom signálového spravodajstva na akýkoľvek schválený účel, či už ide o potreby zahraničnej politiky alebo národnej bezpečnosti.

Postupy, o ktorých sa hovorí vyššie, jasne poukazujú na odhodlanie zabráňovať svojvoľnému a nerozlišujúcemu zhromažďovaniu informácií prostredníctvom signálového spravodajstva a uplatňovať – od najvyšších úrovní našej vlády – zásadu primeranosti. PPD-28 a vykonávacie postupy agentúr objasňujú nové a existujúce obmedzenia zhromažďovania informácií prostredníctvom signálového spravodajstva a ich používania a podrobnejšie opisujú, na aké účely Spojené štáty zhromažďujú a používajú tieto informácie. Tie by mali poskytnúť záruku, že sa činnosti signálového spravodajstva vykonávajú a budú vykonávať len na účely plnenia legitímnych zahraničnopolitických cieľov.

c) Obmedzenia uchovávania a šírenia informácií

V oddiele 4 PPD-28 sa vyžaduje, aby sa pre každú zložku spravodajských služieb uplatňovali jasné obmedzenia, pokiaľ ide o uchovávanie a šírenie osobných informácií o osobách, ktoré nie sú americkými občanmi ani rezidentmi, zhromaždených prostredníctvom signálového spravodajstva, porovnateľné s obmedzeniami platiacimi pre amerických občanov. Tieto pravidlá sú zapracované do postupov pre každú spravodajskú agentúru, ktoré boli vydané vo februári 2015 a sú verejne prístupné. Aby osobné informácie spĺňali požiadavky na uchovávanie a šírenie z hľadiska zahraničného spravodajstva, musia sa týkať schválenej spravodajskej požiadavky, ako sa stanovuje v rámci procesu NIPF opísaného vyššie; musí existovať opodstatnený dôvod domnievať sa, že sú dôkazom zločinu; alebo musia spĺňať jednu z ďalších noriem na uchovávanie informácií o občanoch USA identifikovaných v oddiele 2.3 vykonávacieho nariadenia č. 12333.

Informácie, v súvislosti s ktorými sa neprijalo žiadne takéto rozhodnutie, sa nesmú uchovávať dlhšie ako päť rokov, pokiaľ DNI jednoznačne nerozhodne, že pokračujúce uchovávanie je v záujme národnej bezpečnosti Spojených štátov. To znamená, že zložky spravodajských služieb musia vymazať informácie o osobách, ktoré nie sú americkými občanmi ani rezidentmi, zhromaždené prostredníctvom signálového spravodajstva päť rokov po ich zhromaždení, pokiaľ sa o informácii nerozhodne, že je, napríklad, relevantná z hľadiska schválenej požiadavky na zahraničné spravodajstvo, alebo pokiaľ DNI nerozhodne, po zohľadnení stanoviska úradníka pre ochranu občianskych slobôd ODNI a úradníkov agentúry pre ochranu osobných údajov a občianskych slobôd, že pokračujúce uchovávanie je v záujme národnej bezpečnosti.

Navyše v rámci všetkých pravidiel agentúr, ktorými sa vykonáva PPD-28, sa teraz výslovne vyžaduje, aby sa informácie o fyzických osobách nešírili len z toho dôvodu, že daná osoba nie je občanom ani rezidentom USA, a ODNI vydal smernicu pre všetky spravodajské agentúry⁽¹⁾, aby túto požiadavku zohľadňovali. Od pracovníkov spravodajských služieb sa osobitne vyžaduje, aby pri vypracovávaní a šírení spravodajských správ zohľadňovali záujmy americkými občanmi ani rezidentmi, týkajúce sa súkromia. Zvlášť informácie o každodenných činnostiach zahraničného štátneho príslušníka získané prostredníctvom signálového spravodajstva by sa nepovažovali za zahraničné spravodajské informácie, ktoré by sa mohli šíriť alebo trvalo uchovávať len na základe tejto skutočnosti, pokiaľ inak nezodpovedajú schválenej požiadavke na zahraničné spravodajstvo. Týmto sa uznáva dôležité obmedzenie a reaguje sa tým na obavy Európskej komisie v súvislosti s rozsahom vymedzenia zahraničného spravodajstva, ako sa stanovuje vo vykonávacom nariadení č. 12333.

⁽¹⁾ Smernica o spravodajských službách (Intelligence Community Directive – ICD) 203, dostupná na adrese <http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf>.

d) Dodržiavanie pravidiel a dohľad

V rámci amerického systému dohľadu nad zahraničným spravodajstvom sa zabezpečuje prísny a viacvrstvový dohľad na zaistenie dodržiavania príslušných zákonov a postupov vrátane zákonov a postupov týkajúcich sa zhromažďovania, uchovávanía a šírenia informácií osobách, ktoré nie sú americkými občanmi, získaných prostredníctvom signálového spravodajstva, ako sa stanovuje v PPD-28. Patria sem:

- Spravodajské služby zamestnávajú stovky pracovníkov dohľadu. Len NSA zamestnáva viac ako 300 ľudí zaoberajúcich sa dodržiavaním pravidiel a aj ďalšie zložky majú oddelenia pre dohľad. Okrem toho aj ministerstvo spravodlivosti zabezpečuje rozsiahly dohľad nad spravodajskými činnosťami a dohľad zabezpečuje aj ministerstvo obrany.
- Každá zložka spravodajských služieb má svoj úrad generálneho inšpektora, ktorý okrem iného zodpovedá za dohľad nad zahraničnou spravodajskou činnosťou. Generálni inšpektori sú zo zákona nezávislí, majú širokú právomoc vykonávať vyšetrovanie, audity a preskúmania programov vrátane podvodov, zneužitia alebo porušenia zákona a môžu odporúčať nápravné opatrenia. Hoci odporúčania generálneho inšpektora nie sú záväzné, správy generálneho inšpektora sa často zverejňujú a v každom prípade sa poskytujú Kongresu; zahŕňa to následné správy v prípade, ak nápravné opatrenia odporúčané v predchádzajúcich správach ešte neboli dokončené. To znamená, že Kongres je informovaný o každom nedodržaní a môže vyvinúť tlak, aj rozpočtovými prostriedkami, s cieľom dosiahnuť vykonanie nápravných opatrení. Zverejnených bolo niekoľko správ generálnych inšpektorov o spravodajských programoch ⁽¹⁾.
- Úlohou Kancelárie pre ochranu občianskych slobôd a súkromia (Civil Liberties and Privacy Office – CLPO) ODNI je zaistiť, aby spravodajské služby pracovali spôsobom, ktorým sa posilňuje národná bezpečnosť a zároveň sa zaručuje ochrana občianskych slobôd a práv na ochranu súkromia ⁽²⁾. Svojich vlastných úradníkov pre ochranu osobných údajov majú aj jednotlivé spravodajské agentúry.
- Úlohou Rady pre dohľad nad ochranou súkromia a občianskych slobôd (Privacy and Civil Liberties Oversight Board – PCLOB), nezávislého orgánu zriadeného zákonom, je analyzovanie a preskúmavanie protiteroristických programov a politík vrátane používania signálového spravodajstva s cieľom zaistiť, aby sa v rámci nich náležite chránilo súkromie a občianske slobody. Vydala niekoľko verejných správ o spravodajských činnostiach.
- Ako sa hovorí podrobnejšie ďalej, Súd pre sledovanie v rámci zahraničného spravodajstva, ktorý je zložený z nezávislých federálnych sudcov, je zodpovedný za dohľad nad všetkými činnosťami zhromažďovania informácií prostredníctvom signálového spravodajstva v súlade s FISA a zaistenie dodržiavania pravidiel v rámci týchto činností.
- A nakoniec, významné úlohy dohľadu nad činnosťami amerického zahraničného spravodajstva vrátane amerického signálového spravodajstva plní Kongres USA, konkrétne výbory pre spravodajskú činnosť a výbory pre súdnictvo Snemovne reprezentantov a Senátu.

Okrem týchto formálnych mechanizmov dohľadu disponujú spravodajské služby početnými mechanizmami na zaistenie toho, aby sa dodržiavali vyššie opísané obmedzenia zhromažďovania informácií. Napríklad:

- Ich požiadavky v oblasti signálového spravodajstva musia každý rok schvaľovať vládni úradníci.
- NSA kontroluje ciele signálového spravodajstva počas celého procesu zhromažďovania informácií s cieľom určiť, či skutočne poskytujú cenné zahraničné spravodajské informácie zodpovedajúce prioritám, a zastaví zhromažďovanie, ak to tak nie je. Ďalšími postupmi sa zaisťuje pravidelné preskúmavanie selektorov.

⁽¹⁾ Pozri napríklad správu generálneho inšpektora Ministerstva spravodlivosti USA „Preskúmanie činností Federálneho úradu pre vyšetrovanie na základe oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva z roku 2008“ (september 2012), dostupná na adrese <https://oig.justice.gov/reports/2016/o1601a.pdf>.

⁽²⁾ Pozri www.dni.gov/clpo.

- Na základe odporúčania nezávislej revíznej skupiny menovanej prezidentom Obamom zaviedol DNI nový mechanizmus na monitorovanie zhromažďovania informácií prostredníctvom signálového spravodajstva a ich šírenia v prípade informácií, ktoré sú zvlášť citlivé vzhľadom na povahu cieľa alebo spôsob zhromažďovania, aby sa zaistil súlad s rozhodnutiami politických činiteľov.
- A nakoniec, ODNI každoročne preskúmava vyčleňovanie zdrojov spravodajských služieb na základe priorít NIPF a celkové poslanie spravodajstva. Toto preskúvanie zahŕňa posudzovanie hodnoty všetkých druhov zhromažďovania informácií vrátane signálového spravodajstva a pozerá sa jednak dozadu – aké úspešné boli spravodajské služby v dosahovaní svojich cieľov? – a jednak dopredu – čo budú spravodajské služby potrebovať v budúcnosti? Tým sa zaistuje, že sa prostriedky vyčlenené na signálové spravodajstvo používajú na najdôležitejšie národné priority.

Ako vidieť z tohto komplexného prehľadu, spravodajské služby nerozhodujú samy o tom, ktoré rozhovory treba odpočúvať, nesnažia sa zhromažďovať všetky informácie ani nepracujú bez kontroly. Ich činnosti sú zamerané na priority stanovené politickými činiteľmi v rámci procesu, na ktorom sa zúčastňuje celá vládna štruktúra a na ktorý sa dohliada v rámci NSA, ako aj zo strany ODNI, ministerstva spravodlivosti a ministerstva obrany.

PPD-28 obsahuje aj množstvo ďalších ustanovení, ktorými sa zaisťuje ochrana osobných informácií zhromažďovaných prostredníctvom signálového spravodajstva bez ohľadu na štátnu príslušnosť. PPD-28 napríklad stanovuje postupy na zaistenie bezpečnosti údajov, prístupu k údajom a kvality údajov na účely ochrany osobných informácií zhromažďovaných prostredníctvom signálového spravodajstva a predpisuje povinnú odbornú prípravu s cieľom zaistiť, že pracovníci budú rozumieť potrebe chrániť osobné informácie bez ohľadu na štátnu príslušnosť. PPD stanovuje aj ďalšie mechanizmy dohľadu a mechanizmy na zabezpečenie dodržiavania pravidiel. Tie zahŕňajú pravidelné audity a preskúmania postupov ochrany osobných informácií získavaných v rámci signálového spravodajstva zo strany príslušných úradníkov poverených dohľadom a zabezpečovaním dodržiavania pravidiel. Týmto preskúmaniami sa musí posúdiť aj to, či agentúry dodržiavajú postupy na ochranu takýchto informácií.

Ďalej sa v PPD-28 stanovuje, že významné otázky dodržiavania pravidiel týkajúce sa osôb, ktoré nie sú americkými občanmi ani rezidentmi, sa budú riešiť na vyšších úrovniach vlády. Ak sa vyskytne významný problém s dodržiavaním pravidiel v súvislosti s osobnými informáciami o akejkoľvek osobe zhromaždenými v rámci činností signálového spravodajstva, nad rámec akýchkoľvek existujúcich požiadaviek na podávanie správ sa o takomto probléme musí čo najskôr podať správa DNI. Ak sa problém týka osobných informácií cudzieho štátneho príslušníka, DNI po porade s ministrom zahraničných vecí a vedúcim pracovníkom príslušnej zložky spravodajských služieb rozhodne, či je potrebné podniknúť príslušné kroky a informovať príslušnú zahraničnú vládu, pri zachovaní ochrany zdrojov a metód a amerických pracovníkov. Navyše na základe pokynov PPD-28 určil minister zahraničných vecí vysokú úradníčku, tajomníčku ministerstva Catherine Novelliiovú, ako kontaktnú osobu pre zahraničné vlády, ktoré budú chcieť vyjadriť znepokojenie v súvislosti s činnosťami signálového spravodajstva Spojených štátov. Tento záväzok k angažovanosti na vysokej úrovni dokladá úsilie, ktoré americká vláda v priebehu niekoľkých posledných rokov vynaložila s cieľom zvýšiť dôveru v početné a prelínajúce sa mechanizmy ochrany súkromia týkajúce sa informácií o amerických občanoch a rezidentoch, ako aj osôb, ktoré nie sú americkými občanmi ani rezidentmi.

e) Zhrnutie

Procesy uplatňované v Spojených štátoch pri zhromažďovaní, uchovávaní a šírení zahraničných spravodajských informácií poskytujú dôležité mechanizmy ochrany osobných informácií všetkých osôb bez ohľadu na štátnu príslušnosť. Týmto procesmi sa zabezpečuje zvlášť to, aby sa naše spravodajské služby zameriavali na svoje poslanie v oblasti národnej bezpečnosti len na základe oprávnení vyplývajúcich z príslušných zákonov, vykonávacích nariadení a prezidentských smerníc; chránili informácie pred neoprávneným prístupom, používaním a zverejnením a vykonávali svoje činnosti pod viacerými vrstvami kontroly a dohľadu, a to aj zo strany dozorných výborov Kongresu. PPD-28 a postupy na jej vykonávanie predstavujú naše úsilie o rozšírenie určitých zásad minimalizácie a iných základných zásad ochrany údajov na osobné informácie všetkých osôb bez ohľadu na štátnu príslušnosť. Osobné informácie zhromažďované prostredníctvom amerického signálového spravodajstva podliehajú zásadám a požiadavkám právnych predpisov USA a prezidentských usmernení vrátane mechanizmov ochrany stanovených v PPD-28. Týmto zásadami a požiadavkami sa zabezpečuje, že sa so všetkými osobami bude zaobchádzať dôstojne a s úctou bez ohľadu na ich štátnu príslušnosť alebo bydlisko, a uznáva sa nimi, že všetci ľudia majú pri spracovávaní ich osobných informácií oprávnené záujmy týkajúce sa ochrany súkromia.

II. ZÁKON O SLEDOVANÍ V RÁMCI ZAHRANIČNÉHO SPRAVODAJSTVA – ODDIEL 702

Zhromažďovanie informácií na základe oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva ⁽¹⁾ nie je „masové a nerozlišujúce“, ale je úzko zamerané na zhromažďovanie zahraničných spravodajských informácií o individuálne identifikovaných legitímnych cieľoch; existuje naň jasné oprávnenie na základe výslovnej zákonnej právomoci; a podlieha nezávislému súdnemu dohľadu, ako aj rozsiahlemu preskúmvaniu a dohľadu v rámci exekutívy a Kongresu. Zhromažďovanie informácií na základe oddielu 702 sa považuje za signálové spravodajstvo podliehajúce požiadavkám PPD-28 ⁽²⁾.

Zhromažďovanie informácií na základe oddielu 702 je jedným z najcennejších zdrojov spravodajských informácií slúžiacich na ochranu Spojených štátov aj európskych partnerov. Sú verejne dostupné rozsiahle informácie o uplatňovaní oddielu 702 a dohľade nad jeho uplatňovaním. Početné súdne podania, súdne rozhodnutia a správy o dohľade týkajúce sa programu boli odtajnené a zverejnené na webovej lokalite ODNI určenej na sprístupňovanie informácií verejnosti www.icontherecord.tumblr.com. Oddiel 702 okrem toho komplexne analyzovala PCLOB v správe, ktorá je dostupná na adrese <https://www.pclob.gov/library/702-Report.pdf> ⁽³⁾.

Oddiel 702 bol prijatý ako súčasť zákona o zmenách FISA z roku 2008 ⁽⁴⁾ po rozsiahlej verejnej diskusii v Kongrese. Oprávňuje k získavaniu zahraničných spravodajských informácií monitorovaním osôb, ktoré nie sú americkými občanmi ani rezidentmi, nachádzajúcich sa mimo Spojených štátov s nútenou spolupracou amerických poskytovateľov elektronických komunikačných služieb. Oddiel 702 oprávňuje generálneho prokurátora a DNI – dvoch úradníkov na vládnej úrovni menovaných prezidentom a potvrdzovaných Senátom – predkladať súdu FISA ročné certifikácie ⁽⁵⁾. Tieto certifikácie identifikujú konkrétne kategórie zahraničných spravodajských informácií, ktoré sa majú zhromažďovať, ako sú spravodajské informácie týkajúce sa terorizmu alebo zbraní hromadného ničenia, ktoré musia patriť do kategórií zahraničného spravodajstva vymedzených zákonom FISA ⁽⁶⁾. Ako konštatovala PCLOB, „[t]ieto obmedzenia neoprávňujú k neobmedzenému zhromažďovaniu informácií o cudzincoch“ ⁽⁷⁾.

Certifikácie musia tiež zahŕňať postupy „zacielenia“ a „minimalizácie“, ktoré musí preskúmať a schváliť súd FISA ⁽⁸⁾. Postupy zacielenia majú zaistiť, aby sa zhromažďovanie informácií uskutočňovalo len v súlade s oprávneniami stanovenými zákonom a neprekračovalo rámec certifikácií; postupmi minimalizácie sa má obmedziť získavanie, šírenie a uchovávanie informácií o občanoch USA, ale tiež obsahujú ustanovenia, ktorými sa poskytuje značná ochrana aj vo vzťahu k informáciám o osobách, ktoré nie sú americkými občanmi ani rezidentmi, ako sa opisuje ďalej. Okrem toho, ako sa uvádza vyššie, v PPD-28 prezident nariadil, aby spravodajské služby zabezpečili dodatočné ochranné mechanizmy pre osobné informácie o osobách, ktoré nie sú americkými občanmi ani rezidentmi, pričom tieto ochranné mechanizmy sa vzťahujú na informácie zhromažďované na základe oddielu 702.

Keď súd schváli postupy zacielenia a minimalizácie, nie je zhromažďovanie informácií podľa oddielu 702 hromadné alebo nerozlišujúce, ale „spočíva výlučne v zameraní sa na konkrétne osoby, v súvislosti s ktorými sa prijalo individualizované rozhodnutie“, ako sa vyjadrila PCLOB ⁽⁹⁾. Zhromažďovanie informácií sa zacielfuje prostredníctvom používania individuálnych selektorov, ako sú e-mailové adresy alebo telefónne čísla, v súvislosti s ktorými pracovníci amerických spravodajských služieb došli k záveru, že sa pravdepodobne používajú na odovzdávanie zahraničných spravodajských

⁽¹⁾ 50 U.S.C. § 1881a.

⁽²⁾ Spojené štáty môžu tiež na základe iných ustanovení FISA získavať súdne príkazy na poskytnutie údajov vrátane údajov prenášaných v súlade so štítom na ochranu osobných údajov. Pozri 50 U.S.C. § 1801 a nasl. Hlavy I a III FISA, ktoré oprávňujú na elektronické sledovanie, resp. na telesné prehliadky, si vyžadujú súdny príkaz (s výnimkou núdzových situácií) a vždy si vyžadujú pravdepodobný dôvod domnievať sa, že cieľom je zahraničná mocnosť alebo agent zahraničnej mocnosti. Hlava IV FISA oprávňuje k použitiu záznamníkov zdrojov a cieľov elektronickej komunikácie, na základe súdneho príkazu (s výnimkou núdzových situácií) v rámci schváleného zahraničného spravodajstva, kontrašpionážnych činností alebo protiteroristických vyšetrovaní. Hlava V FISA povoľuje FBI získavať, na základe súdneho príkazu (s výnimkou núdzových situácií), obchodné záznamy, ktoré sú relevantné z hľadiska zahraničného spravodajstva, kontrašpionážnej činnosti alebo protiteroristických vyšetrovaní. Ako sa hovorí ďalej, v zákone USA o slobode (USA FREEDOM Act) sa konkrétne zakazuje používanie príkazov na použitie záznamníkov zdrojov a cieľov elektronickej komunikácie alebo získanie obchodných záznamov na hromadné zhromažďovanie informácií a stanovuje sa v ňom požiadavka „špecifického selektora“ s cieľom zaistiť ciele použitia daných právomocí.

⁽³⁾ Rada pre dohľad nad ochranou súkromia a občianskych slobôd, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Správa o programe sledovania uskutočňovaného na základe oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva) (2. júl 2014) (ďalej len „správa PCLOB“).

⁽⁴⁾ Pozri Pub. L. č. 110 – 261, 122 Stat. 2436 (2008).

⁽⁵⁾ Pozri 50 U.S.C. § 1881a písm. a) a b).

⁽⁶⁾ Pozri *tamže*, § 1801 písm. e).

⁽⁷⁾ Pozri správu PCLOB na s. 99.

⁽⁸⁾ Pozri 50 U.S.C. § 1881a písm. d) a e).

⁽⁹⁾ Pozri správu PCLOB na s. 111.

informácií druhu, na ktorý sa vzťahuje certifikácia predložená súdu ⁽¹⁾. Základ pre výber cieľa sa musí zdokumentovať a dokumentáciu pre každý selektor následne preskúma ministerstvo spravodlivosti ⁽²⁾. Vláda Spojených štátov zverejnila informácie, podľa ktorých boli v roku 2014 na základe oddielu 702 zhromažďované informácie o približne 90 000 fyzických osobách, čo je nepatrný zlomok vyše 3 miliárd používateľov internetu na celom svete ⁽³⁾.

Informácie zhromažďované na základe oddielu 702 podliehajú postupom minimalizácie schváleným súdom, ktorými sa poskytuje ochrana osobám, ktoré nie sú americkými občanmi ani rezidentmi, ako aj americkým občanom a rezidentom, a ktoré boli zverejnené ⁽⁴⁾. Napríklad komunikácie získané na základe oddielu 702, či už sa týkajú osôb, ktoré nie sú americkými občanmi ani rezidentmi, alebo amerických občanov a rezidentov, sa uchovávajú v databázach s prísnu kontrolou prístupu. Môžu ich preskúmať len pracovníci spravodajských služieb, ktorí boli vyškolení v minimalizačných postupoch na ochranu súkromia a ktorí boli špecificky schválení na takýto prístup, aby mohli vykonávať svoje schválené funkcie ⁽⁵⁾. Používanie týchto údajov sa obmedzuje na identifikáciu zahraničných spravodajských informácií alebo dôkazov zločinu ⁽⁶⁾. Podľa PPD-28 sa tieto informácie môžu šíriť len v prípade existencie platného účelu z hľadiska zahraničného spravodajstva alebo presadzovania práva; samotná skutočnosť, že jedna zo strán komunikácie nie je občanom USA, nestačí ⁽⁷⁾. A minimalizačné postupy a PPD-28 tiež stanovujú obmedzenia obdobia uchovávania údajov získaných na základe oddielu 702 ⁽⁸⁾.

Dohľad nad uplatňovaním oddielu 702 je rozsiahly a vykonávajú ho všetky tri zložky našej štátnej moci. Agentúry vykonávajúce zákon disponujú viacerými úrovňami vnútorného preskúmania, vrátane preskúmania generálnymi inšpektormi, a technologickej kontroly prístupu k údajom. Ministerstvo spravodlivosti a ODNI overujú dodržiavanie právnych predpisov dôkladným preskúmaním uplatňovania oddielu 702; na agentúry sa tiež vzťahuje nezávislá povinnosť hlásiť možné prípady nedodržiavania pravidiel. Takéto prípady sa vyšetrí a všetky prípady nedodržiavania sa nahlásia Súdu pre sledovanie v rámci zahraničného spravodajstva, prezidentovmu Výboru pre dohľad nad spravodajskou službou a Kongresu a v prípade potreby sa vykoná ich náprava ⁽⁹⁾. Doteraz sa nevyskytli žiadne úmyselné pokusy porušiť zákon alebo obísť zákonné požiadavky ⁽¹⁰⁾.

Súd FISA zohráva v uplatňovaní oddielu 702 dôležitú úlohu. Je zložený z nezávislých federálnych sudcov, ktorých funkčné obdobie v rámci súdu FISA trvá sedem rokov, ale ktorých sudcovské funkčné obdobie trvá doživotne, ako u všetkých federálnych sudcov. Ako sa uvádza vyššie, súd musí preskúmať, či sú ročné certifikácie a postupy zacielenia a minimalizácie v súlade so zákonom. Okrem toho, ako sa tiež uvádza vyššie, vláda musí súd okamžite informovať o problémoch súvisiacich s dodržiavaním pravidiel ⁽¹¹⁾, pričom na niekoľkých rozhodnutiach súdu, ktoré boli odtajnené a zverejnené, vidieť mimoriadny stupeň súdnej kontroly a nezávislosti, ktorý uplatňuje pri preskúmaní týchto prípadov.

Náročné postupy Súdu opísal jeho bývalý predsedajúci sudca v liste Kongresu, ktorý bol zverejnený ⁽¹²⁾. A na základe zákona USA o slobode (USA FREEDOM Act), ktorý je opísaný ďalej, disponuje súd teraz výslovnou právomocou menovať externého právnik za nezávislého advokáta na ochranu súkromia v prípadoch, v ktorých vyvstávajú nové alebo významné právne otázky ⁽¹³⁾. Tento stupeň zapojenia nezávislého súdnictva krajiny do činností zahraničného spravodajstva zameraného na osoby, ktoré nie sú ani občanmi krajiny ani v nej nemajú bydlisko, je nezvyčajný, ak nie bezprecedentný, a pomáha zaistiť, aby sa zhromažďovanie informácií na základe oddielu 702 uskutočňovalo v príslušných právnych medziach.

⁽¹⁾ Tamže.

⁽²⁾ Tamže na s. 8; 50 U.S.C. § 1881a písm. l); pozri tiež správu riaditeľa Úradu NSA pre ochranu občianskych slobôd a súkromia, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 (Vykonávanie oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva Národnou bezpečnostnou agentúrou) (ďalej len „správa NSA“) na s. 4, dostupná na adrese <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

⁽³⁾ Správa riaditeľa národnej spravodajskej služby o transparentnosti z roku 2014, dostupná na adrese http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

⁽⁴⁾ Minimalizačné postupy dostupné na adrese: <http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf> (ďalej len „minimalizačné postupy NSA“); <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⁾ Pozri správu NSA na s. 4.

⁽⁶⁾ Pozri, napr., minimalizačné postupy NSA na s. 6.

⁽⁷⁾ Postupy spravodajských agentúr podľa PPD-28 dostupné na adrese <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

⁽⁸⁾ Pozri minimalizačné postupy NSA; PPD-28 oddiel 4.

⁽⁹⁾ Pozri 50 U.S.C. § 1881 písm. l). pozri aj správu PCLOB na s. 66 – 76.

⁽¹⁰⁾ Pozri poločné posúdenie otázok súvisiacich s dodržiavaním postupov a usmernení podľa oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva predložené generálnym prokurátorom a riaditeľom Národnej spravodajskej služby na s. 2 – 3, dostupné na adrese <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 rokovacieho poriadku Súdu pre sledovanie v rámci zahraničného spravodajstva, dostupné na <http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

⁽¹²⁾ List ctihodného Reggieho B. Waltona ctihodnému Patrickovi J. Leahymu z 29. júla 2013, dostupný na adrese <http://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

⁽¹³⁾ Pozri oddiel 401 zákona USA o slobode, P.L. 114 – 23.

Kongres vykonáva dohľad prostredníctvom predkladania zákonom vyžadovaných správ výborom pre spravodajskú činnosť a pre súdnicstvo a častých informatívnych schôdzok a výpočutí. To zahŕňa polročnú správu generálneho prokurátora dokumentujúcu uplatňovanie oddielu 702 a všetky prípady nedodržiavania pravidiel ⁽¹⁾; osobitné polročné posúdenie generálnym prokurátorom a DNI dokumentujúce dodržiavanie postupov zacielenia a minimalizácie vrátane dodržiavania postupov, ktoré majú zaistiť, že sa zhromažďovanie uskutočňuje na základe platného účelu z hľadiska zahraničného spravodajstva ⁽²⁾; a ročnú správu vedúcich pracovníkov zložiek spravodajských služieb, čo zahŕňa certifikáciu, že zhromažďovanie informácií na základe oddielu 702 naďalej vedie k získavaniu zahraničných spravodajských informácií ⁽³⁾.

Stručne povedané, na zhromažďovanie informácií na základe oddielu 702 je povolené zákonom; podlieha viacerým úrovňam preskúmania, súdneho dozoru a dohľadu; a, ako sa súd FISA vyjadril v nedávno odtajnenom stanovisku, „neuskutočňuje sa hromadným alebo nerozlišujúcim spôsobom“, ale „prostredníctvom... samostatných rozhodnutí o zacielení pre konkrétne [komunikačné] zariadenia“ ⁽⁴⁾.

III. ZÁKON USA O SLOBODE

Zákon USA o slobode (USA FREEDOM Act), prijatý v júni 2015, významným spôsobom zmenil právomoci v oblasti sledovania a ďalšie právomoci v oblasti národnej bezpečnosti a zvýšil verejnú transparentnosť uplatňovania týchto právomocí a rozhodnutí súdu FISA, ako sa uvádza ďalej ⁽⁵⁾. Zákomom sa zabezpečuje, aby naši profesionáli v oblasti spravodajstva a presadzovania práva disponovali právomocami, ktoré potrebujú na ochranu krajiny, a zároveň aby bolo pri uplatňovaní týchto právomocí náležité chránené súkromie fyzických osôb. Posilňuje sa ním ochrana súkromia a občianskych slobôd a zvyšuje sa transparentnosť.

Zákomom sa zakazuje hromadné zhromažďovanie akýchkoľvek záznamov, týkajúcich sa amerických občanov a rezidentov a osôb, ktoré nie sú americkými občanmi ani rezidentmi, na základe rôznych ustanovení FISA alebo prostredníctvom príkazov na vydanie informácií z dôvodu (national security letters), ktoré sú formou zákonom schválených administratívnych výziev ⁽⁶⁾. Tento zákaz sa konkrétne týka telefónnych metaúdajov týkajúcich sa hovorov medzi osobami v rámci USA a osobami mimo USA a zahŕňa by aj zhromažďovanie informácií v rámci štítu na ochranu osobných údajov na základe týchto právomocí. Zákomom sa vyžaduje, aby bola každá žiadosť vlády o záznamy na základe týchto právomocí založená na „konkrétnom selektore“ – pojme, ktorý konkrétne identifikuje osobu, účet, adresu alebo osobné zariadenie spôsobom, ktorý v čo najväčšej uskutočniteľnej miere obmedzuje rozsah požadovaných informácií ⁽⁷⁾. Tým sa ďalej zabezpečuje presné zameranie a zacielenie zhromažďovania informácií na spravodajské účely.

Zákomom sa tiež prijali významné zmeny v konaní pred súdom FISA, ktorými sa jednak zvyšuje transparentnosť a jednak sa nimi poskytujú ďalšie záruky ochrany súkromia. Ako sa uvádza vyššie, oprávňuje na vytvorenie stáleho výboru zloženého z bezpečnostne preverených právnikov špecializovaných na ochranu súkromia a občianskych slobôd, zhromažďovanie spravodajských informácií, komunikačné technológie alebo iné relevantné oblasti, ktorí môžu byť menovaní, aby predstúpili pred súd ako *amicus curiae* v prípadoch týkajúcich sa významných alebo nových výkladov zákona. Títo právnicki sú oprávnení predkladať právne argumenty na podporu ochrany súkromia a občianskych slobôd fyzických osôb a majú prístup ku všetkým informáciám, vrátane tajných informácií, o ktorých súd rozhodne, že sú potrebné na vykonávanie ich úloh ⁽⁸⁾.

Zákom tiež stavia na bezprecedentnej transparentnosti vlády USA, pokiaľ ide o spravodajské činnosti, a to tým, že vyžaduje, aby DNI, po porade s generálnym prokurátorom, buď odtajnil, alebo zverejnil odtajnené zhrnutie každého rozhodnutia, príkazu alebo stanoviska vydaného súdom FISA alebo Odvolacím súdom pre sledovanie v rámci zahraničného spravodajstva, ktoré obsahuje závažné vysvetlenie alebo výklad akéhokoľvek ustanovenia zákona.

⁽¹⁾ Pozri 50 U.S.C. § 1881f.

⁽²⁾ Pozri tamže § 1881a písm. l) bod (1).

⁽³⁾ Pozri tamže § 1881a písm. l) bod (3). Niektoré z týchto správ sú tajné.

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

⁽⁵⁾ Pozri zákon USA o slobode (USA FREEDOM Act) z roku 2015, Pub. L. č. 114 – 23, § 401, 129 Stat. 268.

⁽⁶⁾ Pozri tamže, §§ 103, 201, 501. Príkazy na vydanie informácií z dôvodu národnej bezpečnosti sa vydávajú na základe rôznych zákonov a umožňujú FBI získať informácie obsiahnuté v informáciách o úverovej schopnosti, finančných záznamoch a záznamoch o elektronickom odbere a transakciách od určitých druhov spoločností výlučne s cieľom zabezpečiť ochranu pred medzinárodným terorizmom alebo nezákonnými spravodajskými činnosťami. Pozri 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u – 1681v; 18 U.S.C. § 2709. Príkazy na vydanie informácií z dôvodu národnej bezpečnosti zvyčajne používa FBI na zhromažďovanie kritických neobsahových informácií v počiatočných štádiách protiteroristických a kontrašpiónážnych vyšetrovaní – ako je totožnosť majiteľa konta, ktorý môže komunikovať s agentmi teroristickej skupiny, ako je ISIL. Prijemcovia príkazov na vydanie informácií z dôvodu národnej bezpečnosti majú právo napadnúť ich na súde. Pozri 18 U.S.C. § 3511.

⁽⁷⁾ Pozri tamže.

⁽⁸⁾ Pozri tamže, § 401.

Zákon okrem toho požaduje rozsiahle zverejnenia o zhromažďovaní informácií na základe zákona FISA a žiadostiach prostredníctvom príkazov na vydanie informácií z dôvodu národnej bezpečnosti. Spojené štáty musia Kongresu a verejnosti každý rok poskytnúť informácie o počte príkazov na základe zákona FISA a požadovaných a získaných certifikácií; o odhadoch počtu amerických občanov a rezidentov a osôb, ktoré nie sú americkými občanmi ani rezidentmi, na ktorých bolo zamerané a ktorých sa dotklo sledovanie; a o počte vymenovaní *amici curiae*, okrem iných informácií ⁽¹⁾. Zákonom sa tiež stanovujú ďalšie požiadavky na to, aby vláda zverejňovala informácie o počtoch žiadostí prostredníctvom príkazov na vydanie informácií z dôvodu národnej bezpečnosti v súvislosti s americkými občanmi a rezidentmi a osobami, ktoré nie sú americkými občanmi ani rezidentmi ⁽²⁾.

Pokiaľ ide o transparentnosť podnikov, poskytuje zákon spoločnostiam rad možností zverejňovania súhrnného počtu príkazov na základe zákona FISA a smerníc alebo listov o národnej bezpečnosti, ktoré dostanú od vlády, ako aj počtu zákaznických účtov, ktorých sa tieto príkazy týkali ⁽³⁾. Niekoľko spoločností už takéto informácie zverejnilo a odhalilo tak, že počet zákazníkov, ktorých záznamy sa požadovali, je obmedzený.

Z týchto správ spoločností na účely zabezpečenia transparentnosti vyplýva, že žiadosti v rámci amerického spravodajstva sa dotýkajú len nepatrného zlomku údajov. Z nedávnej správy jednej významnej spoločnosti na účely zabezpečenia transparentnosti napríklad vyplýva, že dostala žiadosti týkajúce sa národnej bezpečnosti (na základe zákona FISA alebo prostredníctvom príkazov na vydanie informácií z dôvodu národnej bezpečnosti) v súvislosti s menej ako 20 000 z jej účtov, a to v čase, keď mala najmenej 400 miliónov odberateľov. Inými slovami, všetky žiadosti týkajúce sa národnej bezpečnosti USA, o ktorých táto spoločnosť informovala, sa týkali menej ako 0,005 % jej odberateľov. Ak by sa aj každá z daných žiadostí týkala údajov v rámci systému bezpečného prístavu, čo tak, samozrejme, nie je, je jasné, že žiadosti sú cielené, majú primeraný rozsah a nie sú ani hromadné ani nerozlišujúce.

Nakoniec treba uviesť, že hoci sa už zákonmi, ktoré oprávňujú na vydávanie príkazov na vydanie informácií z dôvodu o národnej bezpečnosti, obmedzili okolnosti, za ktorých by sa príjemcovi takéhoto príkazu bránilo v tom, aby ho zverejnil, zákonom sa ďalej stanovilo, že takéto požiadavky na nezverejnenie je potrebné pravidelne preskúmať; vyžaduje sa ním, aby boli príjemcovia príkazov na vydanie informácií z dôvodu národnej bezpečnosti informovaní, keď už skutočnosti neodôvodňujú na požiadavku nezverejnenia; a kodifikovali sa ním postupy, ktorými môžu príjemcovia napadnúť požiadavky nezverejnenia ⁽⁴⁾.

Stručne povedané, dôležité zmeny právomocí spravodajských služieb Spojených štátov, ktoré priniesol zákon USA o slobode, sú jasným dôkazom toho, že Spojené štáty vynakladajú rozsiahle úsilie, aby urobili z ochrany osobných informácií, súkromia, občianskych slobôd a transparentnosti ústredný prvok všetkých amerických spravodajských postupov.

IV. TRANSPARENTNOSŤ

Okrem transparentnosti požadovanej zákonom USA o slobode poskytujú spravodajské služby USA verejnosti mnoho ďalších informácií, čím idú veľmi dobrým príkladom, pokiaľ ide o transparentnosť ich spravodajských činností. Spravodajské služby zverejnili mnohé zo svojich pravidiel, postupov, rozhodnutí Súdu pre sledovanie v rámci zahraničného spravodajstva a iné odtajnené materiály, čím zabezpečili mimoriadny stupeň transparentnosti. Spravodajské služby okrem toho značne zvýšili zverejňovanie štatistických údajov v súvislosti s uplatňovaním právomocí zhromažďovania informácií týkajúcich sa národnej bezpečnosti zo strany vlády. Dňa 22. apríla 2015 vydali spravodajské služby svoju druhú výročnú správu uvádzajúcu štatistické údaje o tom, ako často vláda uplatňuje tieto dôležité právomoci. ODNI tiež zverejnil, na stránke ODNI a na stránke *IC On the Record*, súbor konkrétnych zásad transparentnosti ⁽⁵⁾ a plán realizácie, ktorým sa zásady premietajú do konkrétnych, merateľných iniciatív ⁽⁶⁾. V októbri 2015, riaditeľ Národnej spravodajskej služby nariadil, aby každá spravodajská agentúra spomedzi svojich vedúcich pracovníkov vymenovala úradníka pre transparentnosť spravodajstva, ktorého úlohou má byť podpora transparentnosti a vedenie iniciatív v oblasti transparentnosti ⁽⁷⁾. Úradník pre transparentnosť bude úzko spolupracovať s úradníkom pre ochranu súkromia a občianskych slobôd každej spravodajskej agentúry s cieľom zaistiť, aby transparentnosť, ochrana súkromia a občianskych slobôd naďalej zostali hlavnými prioritami.

⁽¹⁾ Pozri tamže, § 602.

⁽²⁾ Pozri tamže.

⁽³⁾ Pozri tamže, § 603.

⁽⁴⁾ Pozri tamže, §§ 502 písm. 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⁾ Pozri tamže

Príkladom tohto úsilia je zverejnenie niekoľkých odtajnených správ hlavným úradníkom NSA pre ochranu súkromia a občianskych slobôd v priebehu niekoľkých posledných rokov vrátane správ o činnostiach na základe oddielu 702, vykonávacieho nariadenia č. 12333 a zákona USA o slobode⁽¹⁾. Spravodajské služby okrem toho úzko spolupracujú s PCLOB, Kongresom a americkou komunitou advokátov v oblasti ochrany súkromia, aby zabezpečili ešte väčšiu transparentnosť spravodajských činností USA tam, kde je to možné a je to v súlade s ochranou citlivých spravodajských zdrojov a metód. Celkovo možno povedať, že spravodajské činnosti Spojených štátov sú také transparentné alebo viac transparentné ako spravodajské činnosti ktorejkoľvek inej krajiny na svete a sú také transparentné, ako je to možné vzhľadom na zabezpečenie ochrany citlivých zdrojov a metód.

Rozsiahlu transparentnosť, ktorá existuje v súvislosti so spravodajskými činnosťami USA, možno zhrnúť nasledovne:

- Spravodajské služby zverejnili a sprístupnili online tisíce strán súdnych stanovísk a postupov agentúr, v ktorých sa poskytuje prehľad konkrétnych postupov a požiadaviek našich spravodajských činností. Tiež sme zverejnili správy o dodržiavaní príslušných obmedzení spravodajskými agentúrami.
- Vysokí spravodajskí úradníci pravidelne verejne hovoria o úlohách a činnostiach svojich organizácií, čo zahŕňa aj opisovanie režimov a ochranných opatrení, ktorými sa riadi ich práca.
- Spravodajské služby zverejnili veľké množstvo ďalších dokumentov o spravodajských činnostiach na základe nášho zákona o slobode informácií.
- Prezident vydal PPD-28, čím verejne stanovil ďalšie obmedzenia pre naše spravodajské činnosti, a ODNI vydal dve verejné správy o uplatňovaní týchto obmedzení.
- Spravodajské služby sú teraz zo zákona povinné zverejňovať významné právne stanoviská vydávané súdom FISA alebo súhrny týchto stanovísk.
- Vláda je povinná každoročne podávať správy o rozsahu jej uplatňovania určitých právomocí v oblasti národnej bezpečnosti a právo robiť to majú aj spoločnosti.
- PCLOB vydala niekoľko podrobných verejných správ o spravodajských činnostiach a bude to robiť aj naďalej.
- Spravodajské služby poskytujú rozsiahle tajné informácie dozorným výborom Kongresu.
- DNI vydal zásady transparentnosti, ktorými sa majú riadiť činnosti spravodajských služieb.

Táto rozsiahla transparentnosť sa bude ďalej posilňovať. Všetky informácie sprístupnené verejnosti budú, samozrejme, k dispozícii ministerstvu obchodu aj Európskej komisii. Ročné preskúmanie uplatňovania štítu na ochranu osobných údajov ministerstvom obchodu a Európskou komisiou poskytne Európskej komisii príležitosť prediskutovať všetky otázky nastolené v súvislosti s akýmikoľvek novými zverejnenými informáciami, ako aj všetky ostatné záležitosti týkajúce sa štítu na ochranu osobných údajov a jeho fungovania, pričom chápeme, že ministerstvo môže, na základe vlastného uváženia, prizvať k účasti na preskúmaní zástupcov iných agentúr vrátane spravodajských služieb. Toto je, samozrejme, doplnok k mechanizmu stanovenému v PPD-28, na základe ktorého môžu členské štáty EÚ určenému úradníkovi ministerstva zahraničných vecí predkladať otázky v súvislosti so sledovaním.

V. NÁPRÁVNÉ OPATRENIA

Právne predpisy USA poskytujú fyzickým osobám, ktoré sa stali predmetom nezákonného elektronického sledovania na účely národnej bezpečnosti, viacero možností nápravy. Podľa zákona FISA sa právo žiadať nápravu na súdoch USA neobmedzuje na občanov USA. Fyzická osoba, ktorá môže preukázať aktívnu legitímáciu, by mala opravné prostriedky

⁽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.

na napadnutie nezákonného elektronického sledovania na základe zákona FISA. FISA napríklad umožňuje osobám, ktoré sa stali predmetom nezákonného elektronického sledovania, žalovať konkrétnych úradníkov vlády USA ako súkromné osoby o peňažnú náhradu škody vrátane represívnej náhrady škody a náhrady nákladov na právneho zástupcu. Pozri 50 U.S.C. § 1810. Fyzické osoby, ktoré môžu preukázať svoju aktívnu legitimitáciu, môžu tiež prostredníctvom občianskoprávnej žaloby požadovať peňažnú náhradu, vrátane nákladov na súdny spor, od Spojených štátov, ak došlo k nezákonnému alebo úmyselnému použitiu alebo zverejneniu informácií, ktoré boli o nich získané prostredníctvom elektronického sledovania na základe zákona FISA. Pozri 18 U.S.C. § 2712. V prípade, že chce vláda použiť alebo zverejniť akékoľvek informácie získané alebo odvodené z elektronického sledovania akejkoľvek poškodenej osoby na základe zákona FISA proti tejto osobe v rámci súdneho alebo správneho konania v Spojených štátoch, musí o svojom zámere dopredu informovať súd aj danú osobu, ktorá potom môže napadnúť zákonnosť sledovania a žiadať o vylúčenie použitia daných informácií. Pozri 50 U.S.C. § 1806. A nakoniec, zákon FISA tiež stanovuje trestné sankcie pre fyzické osoby, ktoré zámerne uskutočňujú nezákonné elektronické sledovanie pod zámienkou zákona alebo ktorí zámerne použijú alebo zverejnia informácie získané nezákonným sledovaním. Pozri 50 U.S.C. § 1809.

Občania EÚ disponujú inými možnosťami, ako sa domáhať právnej nápravy proti úradníkom americkej vlády za nezákonné použitie údajov alebo prístup k údajom vrátane úradníkov vlády, ktorí porušia zákon v priebehu nezákonného prístupu k údajom alebo použitia údajov na údajné účely národnej bezpečnosti. Zákonom o počítačových podvodoch a zneužívaní sa zakazuje úmyselný neoprávnený prístup (alebo prekročenie oprávneného prístupu) s cieľom získať informácie od finančnej inštitúcie, z počítačového systému vlády USA alebo počítača, ku ktorému možno získať prístup prostredníctvom internetu, ako aj hrozby poškodiť chránené počítače na účely vydierania alebo podvodu. Pozri 18 U.S.C. § 1030. Každá osoba, bez ohľadu na štátnu príslušnosť, ktorá utrpí škodu alebo stratu z dôvodu porušenia tohto zákona, môže na porušovateľa (vrátane úradníka vlády) podať žalobu o náhradu škody a zdržováciu alebo inú satisfakčnú žalobu na základe oddielu 1030 písm. g) bez ohľadu na to, či sa začalo trestné stíhanie, za predpokladu, že dané konanie zahŕňa aspoň jednu z viacerých okolností stanovených v zákone. Zákonom o ochrane súkromia v rámci elektronickej komunikácie (Electronic Communications Privacy Act – ECPA) sa upravuje prístup vlády k uchovávaným elektronickým komunikáciám, záznamom o transakciách a informáciám o odberateľoch uchovávaným tretími stranami poskytujúcimi komunikačné služby. Pozri 18 U.S.C. §§ 2701 – 2712. Zákon ECPA oprávňuje poškodenú fyzickú osobu zažalovať úradníkov vlády za úmyselný nezákonný prístup k uchovávaným údajom. Zákon ECPA sa vzťahuje na všetky osoby bez ohľadu na štátnu príslušnosť, pričom poškodené osoby môžu získať náhradu škody a náhradu nákladov na právneho zástupcu. Zákonom o práve na ochranu osobných finančných údajov (Right to Financial Privacy Act – RFPA) sa obmedzuje prístup vlády USA k bankovým záznamom a záznamom maklérov/obchodníkov týkajúcich sa jednotlivých zákazníkov. Pozri 12 U.S.C. §§ 3401 – 3422. Na základe zákona RFPA môže zákazník banky alebo makléra/obchodníka zažalovať vládu USA o zákonnú náhradu škody, náhradu za skutočne vzniknutú škodu alebo represívnu náhradu škody za neoprávnené získanie prístupu k záznamom zákazníka, pričom zistenie, že takýto neoprávnený prístup bol úmyselný, automaticky vedie k vyšetrovaniu novej potreby prijatia disciplinárnych opatrení proti dotýčným vládnym zamestnancom. Pozri 12 U.S.C. § 3417.

A nakoniec, v zákone o slobodnom prístupe k informáciám (Freedom of Information Act – FOIA) sa stanovuje prostriedok na to, aby každá osoba mohla požadovať prístup k existujúcim záznamom federálnych agentúr z akejkoľvek oblasti s výhradou určitých kategórií výnimiek. Pozri 5 U.S.C. § 552 písm. b). Tie zahŕňajú obmedzenia prístupu k tajným informáciám týkajúcim sa národnej bezpečnosti, osobným informáciám iných fyzických osôb a informáciám týkajúcim sa vyšetrovaní v rámci presadzovania práva a možno ich porovnať s obmedzeniami, ktoré uplatňujú krajiny v rámci svojich vlastných zákonov o prístupe k informáciám. Tieto obmedzenia sa uplatňujú rovnako voči americkým občanom, aj voči občanom iných štátov. Spory ohľadom zverejňovania záznamov, ktoré sa požaduje na základe zákona o slobodnom prístupe k informáciám, sa môžu riešiť správnu cestou a potom na federálnom súde. Súd musí prijať nanovo rozhodnúť o tom, či sa záznamy zadržiavajú oprávnene, 5 U.S.C. § 552 písm. a) bod 4)(B), a môže vláde nariadiť, aby poskytla prístup k záznamom. V niekoľkých prípadoch súdy zamietli tvrdenia vlády, že informácie by sa mali zamlčať ako tajné⁽¹⁾. Hoci nie je možné získať peňažnú náhradu škody, súdy môžu priznať náhradu nákladov na právneho zástupcu.

VI. ZÁVER

Spojené štáty uznávajú, že v rámci nášho signálového spravodajstva a iných spravodajských činností sa musí zohľadňovať zásada, že so všetkými ľuďmi je potrebné zaobchádzať s dôstojnosťou a úctou bez ohľadu na ich štátnu príslušnosť alebo miesto bydliska a že všetci ľudia majú pri narábaní s ich osobnými informáciami oprávnené záujmy, pokiaľ ide o ochranu súkromia. Spojené štáty používajú signálové spravodajstvo len na posilňovanie svojej národnej bezpečnosti a realizáciu zahraničnopolitických záujmov a na ochranu svojich občanov a občanov svojich spojencov a partnerov pred újmou. Stručne povedané, spravodajské služby nesledujú nikoho bez rozlišovania, a to ani radových európskych občanov. Zhromažďovanie informácií prostredníctvom signálového spravodajstva sa uskutočňuje len vtedy, keď naň existuje riadne oprávnenie, a spôsobom, ktorý prísne spĺňa tieto obmedzenia; len po posúdení dostupnosti

⁽¹⁾ Pozri, napr., *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).

alternatívnych zdrojov vrátane diplomatických a verejných zdrojov; a spôsobom, pri ktorom sa uprednostňujú vhodné a uskutočniteľné alternatívy. A, pokiaľ je to možné, signálové spravodajstvo sa uskutočňuje len prostredníctvom zhromažďovania informácií zameraného na konkrétne ciele alebo témy zahraničného spravodajstva s použitím diskriminantov.

Politiku USA v tejto oblasti potvrdila smernica PPD-28. V medziach tohto rámca nemajú spravodajské agentúry USA zákonné oprávnenie, zdroje, technickú spôsobilosť alebo úmysel zachytávať všetku komunikáciu vo svete. Tieto agentúry nečítajú e-maily každej osoby v Spojených štátoch ani každého človeka na svete. V súlade s PPD-28 zabezpečujú Spojené štáty rozsiahlu ochranu osobných informácií osôb, ktoré nie sú americkými občanmi ani rezidentmi, ktoré sa zhromažďujú prostredníctvom činností signálového spravodajstva. To v čo najväčšom možnom rozsahu uskutočniteľnom v súlade s národnou bezpečnosťou zahŕňa politiky a postupy zamerané na minimalizovanie uchovávaní a šírenia osobných informácií týkajúcich sa osôb, ktoré nie sú americkými občanmi ani rezidentmi, porovnateľné s ochranou poskytovanou americkým občanom. Okrem toho, ako sa hovorí vyššie, komplexný režim dohľadu nad vykonávaním právomocí vyplývajúcich z predmetného oddielu 702 zákona FISA nemá obdobu. A nakoniec, ochrana súkromia a občianskych slobôd všetkých fyzických osôb bez ohľadu na ich štátnu príslušnosť sa výrazne posilňuje významnými zmenami právnych predpisov USA prijatými zákonom USA o slobode a iniciatívami na podporu transparentnosti v rámci spravodajských služieb uskutočňovanými pod vedením ODNI.

S úctou
Robert S. Litt

21. júna 2016

Pán Justin S. Antonipillai
poradca
Ministerstvo obchodu USA
1401 Constitution Avenue, N.W.
Washington, DC 20230

Pán Ted Dean
zástupca štátneho tajomníka
Správa zahraničného obchodu (ITA)
1401 Constitution Avenue, N.W.
Washington, DC 20230

Vážený pán Antonipillai, vážený pán Dean,

píšem, aby som Vám poskytol ďalšie informácie o spôsobe, akým Spojené štáty vykonávajú hromadné zhromažďovanie informácií prostredníctvom signálového spravodajstva. Ako je vysvetlené v poznámke 5 prezidentskej politickej smernice č. 28 (PPD-28), „hromadné“ zhromažďovanie sa vzťahuje na získavanie pomerne veľkého objemu informácií alebo údajov prostredníctvom signálového spravodajstva za okolností, keď spravodajské služby nemôžu použiť identifikátor spojený s konkrétnym cieľom (ako je napríklad e-mailová adresa alebo telefónne číslo cieľa), aby mohli presne zamerať zhromažďovanie informácií. To však neznamená, že tento druh zhromažďovania informácií je „masový“ alebo „nerozlišujúci“. V skutočnosti sa v smernici PPD-28 tiež vyžaduje, aby činnosť signálového spravodajstva bola čo najviac prispôbená konkrétnym situáciám. Spravodajské služby v rámci plnenia toho príkazu prijímajú opatrenia, ktoré majú zaistiť, že aj v prípadoch, keď nemôžeme použiť konkrétne identifikátory na zameranie zhromažďovania informácií, zhromažďované údaje pravdepodobne obsahujú zahraničné spravodajské informácie, ktoré budú zodpovedať požiadavkám vysloveným politickými činiteľmi USA, na základe postupu, ktorý som vysvetlil v predchádzajúcom liste, a minimalizujú množstvo zhromažďovaných nesúvisiacich informácií.

Spravodajské služby môžu napríklad dostať požiadavku, aby prostredníctvom signálového spravodajstva získali informácie o aktivitách teroristickej skupiny, ktorá operuje v oblasti určitej krajiny Blízkeho východu a je podozrivá, že plánuje útoky proti západoeurópskym krajinám, pričom však nemusia poznať mená, telefónne čísla, e-mailové adresy alebo iné konkrétne identifikátory jednotlivcov spojených s touto teroristickou skupinou. Mohli by sme si zvoliť postup zacielenia tejto skupiny zhromažďovaním komunikácie smerujúcej do a z daného regiónu na ďalšie preskúmanie a analýzu s cieľom identifikovať komunikáciu, ktorá sa týka príslušnej skupiny. Spravodajské služby by sa pri tom snažili zhromažďovanie informácií čo najviac zúžiť. Takéto zhromažďovanie by sa považovalo za „hromadné“, pretože použitie diskriminantov nie je možné, ale nie je „masové“ ani „nerozlišujúce“, skôr je čo najpresnejšie zamerané.

Takže aj keď zacielenie prostredníctvom používania konkrétnych selektorov nie je možné, Spojené štáty nezhromažďujú celú komunikáciu zo všetkých komunikačných zariadení na celom svete, ale uplatňujú filtre a ďalšie technické nástroje, aby svoje zhromažďovanie informácií zamerali na tie zariadenia, ktoré pravdepodobne obsahujú komunikáciu hodnotnú z hľadiska zahraničného spravodajstva. Činnosť signálového spravodajstva Spojených štátov sa pri tomto postupe dotýka iba zlomku komunikácie vykonávanej prostredníctvom internetu.

Okrem toho, ako som uviedol v predchádzajúcom liste, keďže „hromadné“ zhromažďovanie vytvára väčšie riziko zhromažďovania nesúvisiacej komunikácie, v smernici PPD-28 sa spravodajským službám obmedzuje použitie hromadne zhromaždeného signálového spravodajstva na šesť konkrétnych účelov. V smernici PPD-28 a v politike agentúr na vykonávanie tejto smernice sú tiež stanovené obmedzenia pre uchovávanie a šírenie osobných informácií získaných prostredníctvom signálového spravodajstva, bez ohľadu na to, či boli informácie získané hromadným zhromažďovaním alebo cieľovým zhromažďovaním, a bez ohľadu na štátnu príslušnosť jednotlivca.

„Hromadné“ zhromažďovanie informácií spravodajskými službami nie je „masové“ ani „nerozlišujúce“, ale používajú sa pri ňom metódy a nástroje na filtrovanie zhromažďovania s cieľom zamerať zhromažďovanie na materiál, ktorý bude zodpovedať požiadavkám politických činiteľov na zahraničné spravodajstvo, pri súčasnom minimalizovaní zhromažďovania nesúvisiacich informácií, a sú stanovené prísne pravidlá na ochranu nesúvisiacich informácií, ktoré by sa mohli

získať. Stratégie a postupy opísané v tomto liste sa uplatňujú vo všetkých prípadoch hromadného zhromažďovania informácií prostredníctvom signálového spravodajstva vrátane hromadného zhromažďovania komunikácie smerujúcej do a z Európy, bez potvrdzovania alebo popierania, že nejaké takéto zhromažďovanie prebieha.

Požadovali ste tiež viac informácií o Rade pre dohľad nad ochranou osobných údajov a občianskych slobôd (Privacy and Civil Liberties Oversight Board) a o generálnych inšpektoroch a ich orgánoch. Rada je nezávislou agentúrou v rámci výkonnej zložky. Päťčlennú radu zloženú zo zástupcov dvoch politických strán vymenováva prezident a potvrdzuje Senát ⁽¹⁾. Funkčné obdobie každého člena rady je šesť rokov. Členovia rady a zamestnanci sa podrobujú príslušným bezpečnostným preverkam, aby mohli naplno vykonávať svoje zákonné povinnosti a úlohy ⁽²⁾.

Poslaním Rady pre dohľad nad ochranou osobných údajov a občianskych slobôd je zabezpečiť, aby úsilie federálnej vlády v oblasti predchádzania terorizmu bolo v rovnováhe s potrebou chrániť súkromie a občianske slobody. Rada má dve základné úlohy – dohľad a poradenstvo. Rada si určuje svoj program a rozhoduje, aké aktivity v oblasti dohľadu a poradenstva má v úmysle vykonávať.

Vo svojej úlohe *dohľadu* rada preskúmava a analyzuje opatrenia, ktoré výkonná zložka prijíma na ochranu krajiny pred terorizmom, čím zabezpečuje, že potreba takých opatrení je v rovnováhe s potrebou chrániť súkromie a občianske slobody ⁽³⁾. Najnovšie dokončené preskúmanie vykonávania dohľadu radou bolo zamerané na programy sledovania realizované podľa oddielu 702 zákona o sledovaní v rámci zahraničného spravodajstva ⁽⁴⁾. V súčasnosti rada vykonáva preskúmanie činnosti spravodajstva realizovanej podľa výkonného nariadenia č. 12333 ⁽⁵⁾.

Vo svojej úlohe *poradenstva* rada zabezpečuje, aby sa otázky ochrany slobody primerane zohľadňovali pri príprave a vykonávaní zákonov, nariadení a politik týkajúcich sa úsilia o ochranu krajiny pred terorizmom ⁽⁶⁾.

Aby mohla rada vykonávať svoje poslanie, má zákonom stanovené oprávnenie na prístup k všetkým relevantným záznamom, správam, auditom, preskúmaniam, dokumentom, listinám, odporúčaniam a všetkým ostatným relevantným materiálom vrátane tajných informácií v súlade so zákonom ⁽⁷⁾. Okrem toho môže rada vypočúvať úradníkov alebo zamestnancov výkonnej zložky, prijímať od nich vyhlásenia alebo verejné svedectvo ⁽⁸⁾. Rada môže navyše písomne požiadať generálneho prokurátora, aby v jej mene vydal výzvu, na základe ktorej budú príslušné strany mimo výkonnej zložky nútené poskytnúť relevantné informácie ⁽⁹⁾.

Napokon, pre radu platia zákonné požiadavky na verejnú transparentnosť. Patrí k nim informovanie verejnosti o jej činnosti prostredníctvom verejných výpočutí a verejným sprístupnením jej správ, pri zachovaní najväčšieho možného súladu so zásadami ochrany tajných informácií ⁽¹⁰⁾. Rada je okrem toho povinná podať správu, keď sa agentúra výkonných zložiek odmieta riadiť jej odporúčaniami.

Generálni inšpektori v spravodajských službách vykonávajú audity, inšpekcie a preskúmania programov a činnosti spravodajských služieb s cieľom zisťovať a riešiť prípady systémových rizík, napadnuteľnosti a nedostatkov. Generálni inšpektori okrem toho vyšetrojú sťažnosti alebo informácie o obvineniach z porušovania zákonov, pravidiel alebo nariadení, alebo prípady zlého hospodárenia, veľkého mrhania finančnými prostriedkami, zneužívania právomoci alebo

⁽¹⁾ 42 U.S.C. 2000ee písm. a) a h).

⁽²⁾ 42 U.S.C. 2000ee písm. k).

⁽³⁾ 42 U.S.C. 2000ee písm. d) bod 2.

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

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

⁽⁶⁾ 42 U.S.C. 2000ee písm. d) bod 1; pozri aj PCLOB Advisory Function Policy and Procedure, Policy 2015-004, dostupné na https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.

⁽⁷⁾ 42 U.S.C. 2000ee písm. g) bod 1. písm. A).

⁽⁸⁾ 42 U.S.C. 2000ee písm. g) bod 1. písm. B).

⁽⁹⁾ 42 U.S.C. 2000ee písm. g) bod 1. písm. D).

⁽¹⁰⁾ 42 U.S.C. 2000ee písm. f).

veľkého a konkrétneho ohrozenia verejného zdravia a bezpečnosti v programoch a činnosti spravodajských služieb. Nezavislosť generálneho inšpektora je rozhodujúcou zložkou objektivity a integrity každej správy, zistenia a odporúčania, ktoré generálny inšpektor vydá. K najdôležitejším prvkom pre zachovanie nezávislosti generálneho inšpektora patrí postup vymenovania a odvolania generálneho inšpektora, oddelené prevádzkové, rozpočtové a personálne orgány a požiadavky na dvojité podávanie správ vedúcim pracovníkom agentúry výkonných zložiek a Kongresu.

Kongres zriadil nezávislý úrad generálneho inšpektora v každej agentúre výkonných zložiek vrátane každej zložky spravodajskej služby ⁽¹⁾. Po prijatí zákona o verejnom obstarávaní v spravodajských službách na rozpočtový rok 2015 (Intelligence Authorization Act for Fiscal Year 2015) takmer všetkých generálnych inšpektorov poverených dohľadom nad zložkami spravodajskej služby vymenováva prezident a potvrdzuje Senát, a to vrátane ministerstva spravodlivosti, Ústrednej spravodajskej služby (CIA), Národnej bezpečnostnej agentúry (NSA) a spravodajských služieb ⁽²⁾. Generálni inšpektori sú navyše nestranní úradníci so stálou pozíciou, ktorých môže odvolať iba prezident. Aj keď je v ústave Spojených štátov požiadavka, aby mal prezident právomoc odvolať generálneho inšpektora, táto právomoc sa uplatňuje zriedkavo a prezident musí predložiť Kongresu písomné odôvodnenie 30 dní pred odvolaním generálneho inšpektora ⁽³⁾. Postup vymenovania generálneho inšpektora zabezpečuje, že pri výbere, vymenovaní alebo odvolaní generálneho inšpektora nedochádza k žiadnemu neprípustnému ovplyvňovaniu zo strany úradníkov výkonných zložiek.

Po druhé, generálni inšpektori majú značné zákonné právomoci vykonávať audity, vyšetrovanie a preskúmania programov a činnosti výkonných zložiek. Okrem zákonom vyžadovaného vyšetrovania a preskúmania v rámci dohľadu majú generálni inšpektori široké právomoci vykonávať dohľad s cieľom preskúmať programy a činnosti podľa vlastného výberu ⁽⁴⁾. Zákonom je zabezpečené, že pri uplatňovaní tejto právomoci majú generálni inšpektori nezávislé zdroje na vykonávanie svojich úloh vrátane právomoci najať si vlastných zamestnancov a osobitne predkladať svoje rozpočtové požiadavky Kongresu ⁽⁵⁾. Zákonom je zabezpečené, že generálni inšpektori majú prístup k informáciám potrebným na vykonávanie úloh. Zahŕňa to oprávnenie na priamy prístup ku všetkým záznamom a informáciám týkajúcim sa podrobností o programoch a činnosti agentúry bez ohľadu na klasifikáciu; právomoc vyzvať na predloženie informácií a dokumentov a právomoc vziať jednotlivca pod prísahu ⁽⁶⁾. V obmedzených prípadoch môže vedúci pracovník agentúry výkonných zložiek zakázať činnosť generálneho inšpektora, napríklad ak by audit alebo vyšetrovanie výrazne nepriaznivo ovplyvnilo národné bezpečnostné záujmy Spojených štátov. Aj uplatňovanie tejto právomoci je mimoriadne zriedkavé a vedúci pracovník agentúry musí do 30 dní oznámiť Kongresu dôvody jej uplatnenia ⁽⁷⁾. V skutočnosti riaditeľ národnej spravodajskej služby nikdy neuplatnil túto obmedzujúcu právomoc voči akejkoľvek činnosti generálneho inšpektora.

Po tretie, generálni inšpektori majú za úlohu zabezpečiť, aby vedúci pracovníci agentúr výkonných zložiek a Kongres boli plne a včas informovaní prostredníctvom správ o podvodoch a ďalších závažných problémoch, o prípadoch zneužívania a nedostatkoch týkajúcich sa programov a činnosti výkonných zložiek ⁽⁸⁾. Dvojité podávanie správ posilňuje nezávislosť generálneho inšpektora, keďže zavádza transparentnosť do jeho postupu dohľadu a umožňuje vedúcim pracovníkom agentúry realizovať odporúčania generálneho inšpektora skôr, než Kongres prijme legislatívne opatrenie. Generálni inšpektori sú napríklad podľa zákona povinní vypracovávať polročné správy, v ktorých opisujú takéto problémy, ako aj doposiaľ prijaté nápravné opatrenia ⁽⁹⁾. Agentúry výkonných zložiek berú zistenia

⁽¹⁾ Oddiely 2 a 4 zákona o generálnych inšpektoroch (Inspector General Act) z roku 1978, v znení zmien (ďalej len „zákon o generálnych inšpektoroch“); oddiel 103H písm. b) a e) zákona o národnej bezpečnosti (National Security Act) z roku 1947, v znení zmien (ďalej len „zákon o národnej bezpečnosti“); oddiel 17 písm. a) zákona o Ústrednej spravodajskej službe (ďalej len „zákon o CIA“).

⁽²⁾ Pozri Pub. L. č. 113 – 293, 128 Stat. 3990, (19. decembra 2014). Prezident nevymenováva iba generálnych inšpektorov pre Obrannú spravodajskú agentúru (Defense Intelligence Agency) a Národnú agentúru pre geopriestorové spravodajstvo (National Geospatial-Intelligence Agency), spoločnú právomoc týkajúcu sa týchto agentúr však má generálny inšpektor ministerstva obrany a generálny inšpektor spravodajských služieb.

⁽³⁾ Oddiel 3 zákona o generálnych inšpektoroch (Inspector General Act) z roku 1978, v znení zmien; oddiel 103H písm. c) zákona o národnej bezpečnosti (National Security Act) a oddiel 17 písm. b) zákona o Ústrednej spravodajskej službe (CIA Act).

⁽⁴⁾ Pozri oddiel 4 písm. a) a oddiel 6 písm. a) bod 2 zákona o generálnych inšpektoroch z roku 1947; oddiel 103H písm. e) a písm. g) bod 2 ods. A zákona o národnej bezpečnosti; oddiel 17 písm. a) a c) zákona o CIA.

⁽⁵⁾ Oddiel 3 písm. d), 6 písm. a) bod 7 a oddiel 6 písm. f) zákona o generálnych inšpektoroch; oddiel 103H písm. d), i), j) a m) zákona o národnej bezpečnosti; oddiel 17 písm. e) bod 7 a písm. f) zákona o CIA.

⁽⁶⁾ Oddiel 6 písm. 1, 3, 4, 5 a 6 zákona o generálnych inšpektoroch; oddiel 103H písm. g) bod 2 zákona o národnej bezpečnosti; oddiel 17 písm. e) body 1, 2, 4 a 5 zákona o CIA.

⁽⁷⁾ Pozri napr. oddiel 8 písm. b) a oddiel 8E písm. a) zákona o generálnych inšpektoroch; oddiel 103H písm. f) zákona o národnej bezpečnosti; oddiel 17 písm. b) zákona o CIA.

⁽⁸⁾ Oddiel 4 písm. a) bod 5 zákona o generálnych inšpektoroch; oddiel 103H písm. a) a písm. b) bod 3 a 4 zákona o národnej bezpečnosti; oddiel 17 písm. a) bod 2 a 4 zákona o CIA.

⁽⁹⁾ Oddiel 2 bod 3, oddiel 4 písm. a) a oddiel 5 zákona o generálnych inšpektoroch; oddiel 103H písm. k) zákona o národnej bezpečnosti; oddiel 17 písm. d) zákona o CIA. Generálny inšpektor ministerstva spravodlivosti svoje zverejnené správy sprístupňuje na internete na adrese <http://oig.justice.gov/reports/all.htm>. Podobne generálny inšpektor spravodajských služieb zverejňuje svoje polročné správy na adrese <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

a odporúčania generálneho inšpektora vážne a generálni inšpektori sú často schopní zahrnúť prijatie a vykonávanie takýchto odporúčaní v príslušných správach a aj v ďalších správach predkladaných Kongresu a v niektorých prípadoch verejnosti ⁽¹⁾. Okrem tejto štruktúry dvojítých správ sú generálni inšpektori zodpovední aj za nasmerovanie oznamovateľov porušovania predpisov vo výkonných zložkách k príslušným výborom Kongresu pre dohľad, aby odhalili údajné podvody, plytvanie alebo zneužívanie v programoch a činnosti výkonných zložiek. Identita pracovníkov, ktorí predložili dôkazy, sa chráni pred odhalením výkonnej zložke, čím sa títo oznamovatelia ochraňujú pred prípadnými zakázanými akciami zamestnancov alebo pred vykonávaním bezpečnostných previerok ako odvety za hlásenie generálnemu inšpektorovi ⁽²⁾. Oznamovatelia porušovania predpisov sú často zdrojom informácií pre vyšetrowanie generálneho inšpektora, pričom možnosť podávať správy o obavách Kongresu bez vplyvu výkonnej zložky zvyšuje účinnosť dohľadu generálneho inšpektora. Vzhľadom na túto nezávislosť môžu generálni inšpektori podporovať hospodárnosť, efektívnosť a zodpovednosť v agentúrach výkonných zložiek s objektivitou a integritou.

Napokon, Kongres zriadil radu generálnych inšpektorov pre integritu a efektívnosť. Rada okrem iného pripravuje normy generálnych inšpektorov pre audity, vyšetrowanie a preskúmania, podporuje odbornú prípravu a má právomoc vykonávať preskúmania obvinení generálnych inšpektorov z pochybenia, čo slúži ako kritický pohľad na generálnych inšpektorov, ktorí sú poverení dohľadom nad všetkými ostatnými. ⁽³⁾

Dúfam, že tieto informácie sú pre Vás užitočné.

S pozdravom
Robert S. Litt
generálny poradca

⁽¹⁾ Oddiel 2 bod 3, oddiel 4 písm. a) a oddiel 5 zákona o generálnych inšpektoroch; oddiel 103H písm. k) zákona o národnej bezpečnosti; oddiel 17 písm. d) zákona o CIA. Generálny inšpektor ministerstva spravodlivosti svoje zverejnené správy sprístupňuje na internete na adrese <http://oig.justice.gov/reports/all.htm>. Podobne generálny inšpektor spravodajských služieb zverejňuje svoje polročné správy na adrese <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

⁽²⁾ Oddiel 7 zákona o generálnych inšpektoroch; oddiel 103H písm. g) bod 3 zákona o národnej bezpečnosti; oddiel 17 písm. e) bod 3 zákona o CIA.

⁽³⁾ Oddiel 11 zákona o generálnych inšpektoroch.

PRÍLOHA VII

**List od zástupcu námestníka generálnej prokurátorky a poradcu pre medzinárodné záležitosti
Brucea Swartza, ministerstvo spravodlivosti USA**

19. február 2016

Pán Justin S. Antonipillai
právny zástupca
Ministerstvo obchodu USA
1401 Constitution Ave., NW
Washington, DC 20230

Pán Ted Dean
zástupca námestníka
Správa zahraničného obchodu (ITA)
1401 Constitution Ave., NW
Washington, DC 20230

Vážený pán Antonipillai, vážený pán Dean,

tento list obsahuje stručný prehľad primárnych vyšetrovacích nástrojov používaných na získanie ekonomických údajov a ďalších zaznamenaných informácií od spoločností v USA na účely presadzovania trestného práva alebo verejného záujmu (občianskoprávneho a regulačného), vrátane obmedzení prístupu stanovených v týchto oprávneniach⁽¹⁾. Tieto zákonné postupy nie sú diskriminačné, pretože sa používajú na získanie informácií od spoločností v USA vrátane tých spoločností, ktoré predložia osvedčenie prostredníctvom rámca štítu na ochranu osobných údajov medzi EÚ a USA, bez ohľadu na štátnu príslušnosť dotknutej osoby. Okrem toho, spoločnosti, ktoré v USA dostanú súdny príkaz, môžu tento príkaz napadnúť na súde, ako je uvedené nižšie⁽²⁾.

Špeciálny význam vzhľadom na zaistenie údajov orgánmi verejnej moci má štvrtý dodatok k Ústave USA, v ktorom sa stanovuje, že „právo národa na ochranu osobnej a domovej slobody, písomností a majetku nesmie byť porušované neoprávnenými prehliadkami a konfiškáciami; nesmie byť vydaný ani žiadny príkaz, ktorý by sa neopieral o odôvodnené zistenia, doložené prisahou alebo potvrdené iným spôsobom, a ktorý by neobsahoval presné určenie miesta, ktoré má byť prehľadané, a presný opis osôb a vecí, ktoré majú byť zaistené. Ústava USA, IV. dodatok. Ako stanovil Najvyšší súd USA v prípade *Berger/Štát New York*, „základným účelom tohto dodatku, ako v mnohých rozhodnutiach potvrdil tento súd, je chrániť súkromie a bezpečnosť fyzických osôb voči svojvoľným zásahom vládnych úradníkov“. 388 U.S. 41, 53 (1967) (citát z rozhodnutia vo veci *Camara/Mestský súd San Francisca*, 387 U.S. 523, 528 (1967)). V prípade vnútroštátnych vyšetrovaní trestných činov sa vo štvrtom dodatku vo všeobecnosti vyžaduje, aby vyšetrovatelia získali pred vykonaním prehliadky súdny príkaz. Pozri vec *Katz/Spojené štáty americké*, 389 U.S. 347, 357 (1967). Ak sa neuplatňuje požiadavka súdneho príkazu, činnosť úradníkov vlády podlieha skúške „primeranosti“ podľa štvrtého dodatku. Samotná Ústava teda zaručuje, že vláda USA nemá neobmedzenú, či svojvoľnú, právomoc zaistiť súkromné informácie.

Orgány činné v trestnom konaní:

Federálni prokurátori, ktorí sú úradníkmi ministerstva spravodlivosti, a federálni vyšetrovací agenti vrátane agentov FBI (Federal Bureau of Investigation), orgánu presadzovania práva v rámci ministerstva spravodlivosti, si môžu vynútiť predloženie dokumentov a iných zaznamenaných informácií od spoločností v USA na účely vyšetrovania trestného činu

⁽¹⁾ V tomto prehľade sa neopisujú vyšetrovacie nástroje národnej bezpečnosti používané orgánmi presadzovania práva v prípadoch terorizmu a iných vyšetrovaní súvisiacich s národnou bezpečnosťou, vrátane príkazov na vydanie informácií z dôvodu národnej bezpečnosti (National Security Letters – NSL) pre niektoré informácie zaznamenané v správach o úverovej schopnosti, finančných záznamoch a záznamoch o elektronickom odbere a transakciách, pozri 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, a pre elektronické sledovanie, príkazy na domovú prehliadku, obchodné záznamy a ďalšie zhromažďovanie komunikácií podľa zákona o sledovaní v rámci zahraničného spravodajstva pozri 50 U.S.C. § 1801 a nasl.

⁽²⁾ Tento dokument obsahuje informácie o právomociach federálnych orgánov presadzovania práva a regulačných orgánov; porušovanie štátnych zákonov vyšetrujú jednotlivé štáty a súdne konania prebiehajú na štátnych súdoch. Štátne orgány presadzovania práva používajú súdne príkazy a predvolania vydané podľa štátnych zákonov v podstate rovnakým spôsobom ako je opísané tu, ale s možnosťou, že súdne konanie na úrovni štátu môže podliehať ochrane podľa ústavy daného štátu, ktorá môže ísť nad rámec Ústavy USA. Ochrana podľa štátneho práva musí byť minimálne na rovnakej úrovni ako ochrana podľa Ústavy USA vrátane štvrtého dodatku.

prostredníctvom niekoľkých typov zákonných konaní vrátane predvolania pred veľkú porotu, administratívnej výzvy a príkazu na domovú prehliadku a ďalšie komunikácie môžu získať prostredníctvom povolení na odpočúvanie a použitie záznamníkov zdrojov a cieľov elektronickej komunikácie na účely federálneho vyšetrovania trestného činu.

Predvolanie pred veľkú porotu alebo predvolanie na súd: Predvolania v trestnom konaní sa používajú na podporu cielených vyšetrovaní orgánov činných v trestnom konaní. Predvolanie pred veľkú porotu je oficiálna žiadosť vydaná veľkou porotou (zvyčajne na žiadosť federálneho prokurátora) na podporu vyšetrovania, ktoré veľká porota vedie v prípade určitého podozrenia z porušenia trestného práva. Veľké poroty sú vyšetrovacou zložkou súdu a zostavuje ich sudca alebo magistrátny sudca. Na predvolaní sa môže od niekoho vyžadovať, aby vypovedal na súde alebo aby predložil či sprístupnil obchodné záznamy, informácie uložené elektronicke alebo iné hmotné predmety. Informácie musia súvisieť s vyšetrovaním a predvolanie nemôže byť neoprávnené z dôvodu nekonkrétnosti, obmedzovania alebo neprimeraného zaťažovania. Prijemca môže na základe týchto dôvodov podať námietku voči predvolaniu. Pozri federálne pravidlá trestného konania, č. 17. V určitých prípadoch sa predvolania na súd z dôvodu predloženia dokumentov môžu použiť po tom, ako v prípade veľká porota vzniesla obvinenie.

Povolenie na administratívnu výzvu: Pri vyšetrovaniach trestných činov alebo občianskoprávných vyšetrovaniach je možné využiť povolenie na administratívnu výzvu. V súvislosti s trestným konaním viaceré federálne zákony povoľujú používanie administratívnych výziev na predloženie alebo sprístupnenie obchodných záznamov, informácií uložených elektronicke alebo iných hmotných položiek súvisiacich s vyšetrovaním podvodov v zdravotníctve, zneužívania detí, ochrany tajnej služby, prípadov kontrolovaných látok a vyšetrovaním generálneho inšpektora so zapojením vládnych agentúr. Ak sa štátny orgán pokúša presadiť na súde administratívnu výzvu, príjemca tejto výzvy, podobne ako príjemca predvolania pred veľkú porotu, môže argumentovať, že výzva nie je oprávnená, pretože je nekonkrétna, obmedzujúca alebo neprimerane zaťažujúca.

Súdne príkazy na použitie záznamníkov zdrojov a cieľov elektronickej komunikácie: Podľa ustanovení trestného práva o používaní záznamníkov zdrojov a cieľov elektronickej komunikácie môže orgán presadzovania práva získať súdny príkaz na zaobstaranie aktuálnych informácií o vytáčaní, smerovaní, adresovaní a signalizovaní týkajúcich sa určitého telefónneho čísla alebo e-mailu, bez obsahu samotnej komunikácie, na základe potvrdenia, že poskytnuté informácie súvisia s prebiehajúcim vyšetrovaním trestného činu. Pozri 18 U.S.C. §§ 3121-3127. Nezákonné použitie alebo inštalovanie takéhoto zariadenia je federálny zločin.

Zákon o ochrane súkromia v rámci elektronickej komunikácie (Electronic Communications Privacy Act, ECPA): Ďalšie pravidlá upravujú prístup vlády k informáciám o účastníkoch, údajom o prenosoch údajov a obsahu komunikácií uchovávanom telefónnymi spoločnosťami poskytovateľov internetových služieb, ako aj inými poskytovateľmi služieb, podľa hlavy II zákona ECPA, ktorá sa tiež nazýva Zákon o uložených komunikáciách (Stored Communications Act, SCA), 18 U.S.C. §§ 2701-2712. V zákone SCA sa stanovuje systém zákonných práv na ochranu súkromia, ktoré obmedzujú prístup orgánov presadzovania práva k údajom okrem tých, ktoré vyžaduje ústavné právo od zákazníkov a účastníkov poskytovateľov internetových služieb. Zákon SCA zaisťuje zvýšenú úroveň ochrany osobných údajov podľa stupňa zásahu do súkromia pri ich zhromažďovaní. Na získanie registračných údajov účastníkov, IP adres a príslušných časových pečiatok, ako aj fakturačných údajov, musia orgány činné v trestnom konaní získať príslušné predvolanie. Na získanie väčšiny iných uložených informácií bez obsahu komunikácie, ako sú napríklad hlavičky e-mailov bez predmetu, musia orgány presadzovania práva predložiť sudcovi konkrétne skutočnosti preukazujúce, že požadované informácie súvisia s prebiehajúcim vyšetrovaním trestného činu a sú preň významné. Na získanie uloženého obsahu elektronickej komunikácie musia vo všeobecnosti orgány činné v trestnom konaní získať od sudcu príkaz na základe odôvodnenej domnienky, že predmetné konto obsahuje dôkaz o zločine. V zákone SCA sa tiež stanovuje občianskoprávna zodpovednosť a trestné sankcie.

Súdne príkazy na sledovanie podľa federálneho zákona o odpočúvaní: Orgány presadzovania práva môžu okrem toho odpočúvať prebiehajúcu telefónickú, ústnu alebo elektronicke komunikáciu na účely vyšetrovania trestného činu podľa federálneho zákona o odpočúvaní. Pozri 18 U.S.C. §§ 2510-2522. Môžu tak robiť iba na základe súdneho príkazu,

v ktorom sudca dospel, okrem iného, k záveru, že existuje odôvodnená príčina domnievať sa, že odpočúvanie alebo elektronické zachytenie poskytne dôkaz o federálnom zločine alebo o pobyte utečenca unikajúceho pred stíhaním. V zákone sa stanovuje občianskoprávna zodpovednosť a trestné sankcie za porušenie ustanovení o odpočúvaní.

Príkaz na domovú prehliadku – pravidlo č. 41: Orgány presadzovania práva môžu fyzicky prehľadať priestory v USA, ak na to majú povolenie od sudcu. Vyšetrovateľ musí sudcovi preukázať na základe predloženia „odôvodnenej príčiny“, že bol spáchaný alebo má byť spáchaný trestný čin a predmety súvisiace s trestným činom sa pravdepodobne nachádzajú na mieste označenom v príkaze na prehliadku. Toto povolenie sa často používa vtedy, keď je potrebné fyzické prehľadanie priestorov políciou z dôvodu nebezpečenstva, že dôkazy môžu byť zničené, ak by bolo voči spoločnosti vydané predvolanie alebo iný príkaz na predloženie údajov. Pozri Ústavu USA, IV. dodatok (podrobnejšie opísaný vyššie), federálne pravidlá trestného konania, č. 41. Subjekt, voči ktorému bol vydaný príkaz na domovú prehliadku, môže podať návrh na jeho zrušenie na základe jeho nekonkrétnosti, obťažovania alebo iného neoprávneného získania, a príslušné poškodené strany môžu podať návrh na zákaz použitia akýchkoľvek dôkazov získaných prostredníctvom nezákonnej prehliadky. Pozri *vec Mapp/Ohio*, 367 U.S. 643 (1961).

Usmernenia a postupy ministerstva spravodlivosti: Okrem týchto ústavných a zákonných obmedzení a obmedzení založených na pravidlách, ktoré limitujú prístup vlády k údajom, vydal generálny prokurátor usmernenia, ktoré ešte viac obmedzujú prístup orgánov presadzovania práva k údajom, a zahŕňajú aj ochranu súkromia a občianskych slobôd. Napríklad Usmernenia generálneho prokurátora pre domáce operácie FBI [Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations] (september 2008) (ďalej len „Usmernenia GP pre FBI“), k dispozícii na stránke <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, stanovujú limity na používanie vyšetrovacích prostriedkov na získanie informácií súvisiacich s vyšetrovaniami, ktoré sa týkajú federálnych zločinov. V týchto usmerneniach sa vyžaduje, aby FBI používala najmenej obťažujúce dostupné vyšetrovacie metódy so zohľadnením ich účinku na súkromie a občianske slobody a možné poškodenie dobrého mena. Okrem toho uvádzajú, že „je samozrejmé, že FBI musí viesť svoje vyšetrovania a ostatné činnosti zákonným a primeraným spôsobom, ktorý rešpektuje slobodu a súkromie a vyhýba sa nepotrebným zásahom do životov ľudí dodržiavajúcich zákony“. Pozri Usmernenia GP pre FBI v bode 5. FBI vykonáva tieto usmernenia prostredníctvom Príručky FBI pre domáce vyšetrovania a operácie (FBI Domestic Investigations and Operations Guide, DIOG), ktorá je k dispozícii na stránke [https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20\(DIOG\)](https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG)). Je to komplexná príručka, ktorá obsahuje podrobné limity používania vyšetrovacích nástrojov a usmernenie na zabezpečenie ochrany občianskych slobôd a súkromia v každom vyšetrovaní. Ďalšie pravidlá a politiky, ktoré predpisujú obmedzenia vyšetrovacích činností federálnych prokurátorov sú stanovené v **príručke pre prokurátorov USA (United States Attorneys' Manual)** (USAM), ktorá je k dispozícii online na adrese <http://www.justice.gov/usam/united-states-attorneys-manual>.

Občianskoprávne a regulačné orgány (verejný záujem):

Existujú aj významné obmedzenia prístupu občianskoprávných a regulačných orgánov (t. j. „verejný záujem“) k údajom v držbe spoločností v USA. Agentúry s občianskoprávnymi a regulačnými zodpovednosťami môžu spoločnostiam vydávať predvolania na predloženie obchodných záznamov, informácií uložených elektronicky a ďalších hmotných predmetov. Tieto agentúry majú obmedzenia pri výkone svojich právomocí na vydávanie úradných alebo občianskoprávných predvolaní, a to nielen na základe ich ustanovujúcich zákonov, ale aj z dôvodu nezávislého súdneho preskúmania predvolaní pred prípadným súdnym konaním. Pozri napr. federálne pravidlá občianskoprávneho konania, č. 45. Agentúry môžu vyžadovať prístup iba k údajom, ktoré súvisia so záležitosťami v rámci rozsahu pôsobnosti ich regulácie. Navyše, príjemca administratívnej výzvy môže podať námietku voči výkonu tejto výzvy na súde predložením dôkazu, že agentúra nekonala v súlade so základnými normami primeranosti, ako je uvedené vyššie.

Existujú ďalšie právne základy, podľa ktorých môžu spoločnosti podať námietku voči požiadavkám na poskytnutie údajov zo strany správnych agentúr v závislosti od ich konkrétnych odvetví a typov údajov, ktoré vlastnia. Napríklad finančné inštitúcie môžu podať námietku voči administratívnej výzve požadujúcej určité typy informácií z dôvodu porušenia zákona o bankovom tajomstve a jeho vykonávacích predpisov. Pozri 31 U.S.C. § 5318, 31 C.F.R. časť X. Ostatné podniky sa môžu opierať o zákon o korektnom nakladaní so spotrebiteľskými informáciami (Fair Credit Reporting Act), pozri 15 U.S.C. § 1681b, alebo môžu využiť celý rad odvetvových právnych predpisov. Zneužitie oprávnenia agentúry na vydanie predvolania môže mať za následok vyvodenie zodpovednosti voči agentúre alebo osobnej zodpovednosti jej úradníkov. Pozri napr. zákon o práve na ochranu osobných finančných údajov (Right to Financial Privacy Act), 12 U.S.C. §§ 3401–3422. Súd v USA teda chráni proti neoprávneným regulačným požiadavkám a poskytujú nezávislý dohľad nad činnosťami federálnych agentúr.

A napokon, akékoľvek zákonné oprávnenie, podľa ktorého správne orgány musia fyzicky zaistiť záznamy od spoločnosti v USA na základe úradnej prehliadky, musí spĺňať požiadavky Štvrtého dodatku. Pozri vec *See/City of Seattle*, 387 U.S. 541 (1967).

Záver

Všetky činnosti presadzovania práva a regulačné činnosti v USA musia byť v súlade s uplatniteľným právom vrátane Ústavy USA, zákonov, pravidiel a nariadení. Tieto činnosti musia tiež spĺňať uplatniteľné politiky vrátane všetkých usmernení generálneho prokurátora upravujúcich činnosti federálnych orgánov presadzovania práva. Právny rámec opísaný vyššie obmedzuje možnosti amerických orgánov presadzovania práva a regulačných orgánov zamerané na získanie informácií od spoločností v USA – bez ohľadu na to, či sa informácie týkajú občanov alebo rezidentov USA alebo občanov cudzích krajín – a navyše umožňuje právne preskúmanie akýchkoľvek žiadostí vlády o predloženie údajov na základe týchto oprávnení.

S úctou

Bruce C. Swartz

zástupca námestníka generálnej prokurátorky
a poradca pre medzinárodné záležitosti
