II.

(Nezakonodavni akti)

ODLUKE

PROVEDBENA ODLUKA KOMISIJE (EU) 2016/1250

od 12. srpnja 2016.

o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća

(priopćeno pod brojem dokumenta C(2016) 4176)

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Direktivu 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka ([1]), a posebno njezin članak 25. stavak 6.,

nakon savjetovanja s Europskim nadzornikom za zaštitu podataka ([2]),

1. UVOD

(1) Direktivom 95/46/EZ utvrđuju se pravila za prijenos osobnih podataka iz država članica u treće zemlje u mjeri u kojoj je takav prijenos obuhvaćen njezinim područjem primjene.

(2) Člankom 1. Direktive 95/46/EZ i uvodnim izjavama 2. i 10. njezine preambule nastoji se osigurati ne samo djelotvorna i potpuna zaštita temeljnih prava i sloboda fizičkih osoba, posebno temeljnog prava na poštovanje privatnog života u vezi s obradom osobnih podataka, već i visok stupanj zaštite tih temeljnih prava i sloboda ([3]).

(3) Važnost temeljnog prava na poštovanje privatnog života zajamčenog člankom 7. i temeljnog prava na zaštitu osobnih podataka zajamčenog člankom 8. Povelje Europske unije o temeljnim pravima u svojoj je praksi istaknuo Sud Europske unije ([4]).

(4) U skladu s člankom 25. stavkom 1. Direktive 95/46/EZ države članice dužne su osigurati da se prijenos osobnih podataka u treću zemlju može izvršiti samo ako predmetna treća zemlja osigura odgovarajuću razinu zaštite i ako se prije prijenosa poštuju zakoni države članice kojima se provode ostale odredbe Direktive. Komisija može utvrditi da predmetna treća zemlja osigurava odgovarajuću razinu zaštite svojim nacionalnim pravom ili međunarodnim obvezama koje je preuzela u cilju zaštite prava osoba. U tom slučaju, i ne dovodeći u pitanje usklađenost s nacionalnim odredbama donesenima u skladu s drugim odredbama Direktive, osobni podaci mogu se prenositi iz država članica bez dodatnih jamstava.

([1]) SL L 281, 23.11.1995., str. 31.
([2]) Vidjeti Mišljenje 4/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti, 30. svibnja 2016.
([3]) Predmet C-362/14, *Maximillian Schrems protiv Povjerenika za zaštitu podataka* (dalje u tekstu: *Schrems*), EU:C:2015:650, točka 39.
([4]) Predmet C-553/07, *Rijkeboer*, EU:C:2009:293, točka 47.; Spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland i dr.*, EU:C:2014:238, točka 53.; Predmet C-131/12, *Google Spain i Google*, EU:C:2014:317, točke 53., 66. i 74.

(5) U skladu s člankom 25. stavkom 2. Direktive 95/46/EZ razina zaštite koju osigurava treća zemlja procjenjuje se ovisno o svim okolnostima u vezi s postupkom prijenosa podataka ili skupom takvih postupaka, što uključuje zakonska pravila, opća i sektorska, koja su na snazi u predmetnoj trećoj zemlji.

(6) U odluci Komisije 2000/520/EZ ([5]), za potrebe članka 25. stavka 2. Direktive 95/46/EZ, uzeta su u obzir načela privatnosti „sigurne luke", koja se provode u skladu sa smjernicama iz takozvanih često postavljanih pitanja koje je izdalo Ministarstvo trgovine SAD-a, kako bi se osigurala odgovarajuća razina zaštite osobnih podataka koji se iz Unije prenose organizacijama s poslovnim nastanom u Sjedinjenim Američkim Državama.

(7) U svojim Komunikacijama COM(2013) 846 final ([6]) i COM(2013) 847 final od 27. studenoga 2013. ([7]) Komisija je smatrala da se temeljna osnova programa „sigurne luke" mora preispitati i pojačati u kontekstu niza čimbenika, uključujući eksponencijalni rast protoka podataka i njihovu presudnu važnost za transatlantsko gospodarstvo, brzo povećanje broja poduzeća iz SAD-a koja postupaju u skladu s programom „sigurne luke" te nove informacije o opsegu i području primjene određenih američkih obavještajnih programa, zbog čega se javljaju pitanja u pogledu razine zaštite koja se njima može osigurati. Komisija je utvrdila i niz nedostataka i manjkavosti u programu „sigurne luke".

(8) Na temelju dokaza koje je prikupila, uključujući informacije prikupljene u okviru rada Kontaktne skupine za zaštitu privatnosti EU-a i SAD-a ([8]) i informacije o američkim obavještajnim programima dobivenima u okviru *ad hoc* radne skupine EU-a i SAD-a ([9]), Komisija je oblikovala 13 preporuka za preispitivanje programa „sigurne luke". Te su preporuke bile usmjerene na jačanje materijalnih načela privatnosti, povećanje transparentnosti politika privatnosti samocertificiranih američkih poduzeća, bolji nadzor, praćenje i provedbu usklađenosti s tim načelima američkih nadležnih tijela, dostupnost pristupačnih mehanizama za rješavanje sporova i potrebu da se osigura ograničenje primjene izuzeća zbog nacionalne sigurnosti predviđenog u Odluci 2000/520/EZ na ono što je nužno i razmjerno.

(9) U svojoj presudi od 6. listopada 2015. u predmetu C-362/14, *Maximillian Schrems protiv Povjerenika za zaštitu podataka* ([10]), Sud Europske unije proglasio je Odluku 2000/520/EZ nevažećom. Ne razmatrajući sadržaj načela privatnosti „sigurne luke" Sud je smatrao da Komisija u toj Odluci nije izjavila da Sjedinjene Američke Države zapravo „osiguravaju" odgovarajuću razinu zaštite temeljem svog nacionalnog zakonodavstva ili preuzetih međunarodnih obveza ([11]).

(10) U tom pogledu Sud EU-a objasnio je da, iako izraz „odgovarajuća razina zaštite" iz članka 25. stavka 6. Direktive 95/46/EZ ne znači razinu zaštite koja je jednaka zaštiti zajamčenoj u pravnom poretku EU-a, on se mora tumačiti kao da se od treće zemlje zahtijeva da osigura razinu zaštite temeljnih prava i sloboda koja je „u osnovi jednakovrijedna" zaštiti zajamčenoj u Uniji temeljem Direktive 95/46/EZ kad se tumači u kontekstu Povelje o temeljnim pravima. Iako se u tom smislu sredstva kojima se služi treća zemlja mogu razlikovati od onih koja se primjenjuju u Uniji, ta se sredstva u praksi ipak moraju pokazati djelotvornima ([12]).

(11) Sud EU-a kritizirao je da u Odluci 2000/520/EZ nema dovoljno podataka o tome da u Sjedinjenim Američkim Državama postoje pravila namijenjena tome da se ograniči svako zadiranje u temeljna prava osoba čiji se podaci prenose iz Unije u SAD, za što bi državna tijela te zemlje bila ovlaštena pri ostvarivanju legitimnih ciljeva kao što je nacionalna sigurnost, ni o postojanju djelotvorne pravne zaštite protiv takvog zadiranja ([13]).

([5]) Odluka Komisije 2000/520/EZ od 26. srpnja 2000. u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke" i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a (SL L 215, 28.8.2000., str. 7.).

([6]) Komunikacija Komisije Europskom parlamentu i Vijeću „Ponovna uspostava povjerenja u protoku podataka između EU-a i SAD-a", COM(2013) 846 final, 27. studenoga 2013.

([7]) Komunikacija Komisije Europskom parlamentu i Vijeću o funkcioniranju „sigurne luke" iz perspektive građana EU-a i poduzeća s poslovnim nastanom u Europskoj uniji, COM(2013) 847 final od 27. studenoga 2013.

([8]) Vidjeti npr. Vijeće Europske unije, Završno izvješće Kontaktne skupine na visokoj razini za razmjenu informacija i zaštitu privatnosti i osobnih podataka EU-a i SAD-a, obavijest 9831/08, 28. svibnja 2008. dostupna na internetu na: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Izvješće o nalazima supredsjedatelja EU-a *ad hoc* radnom skupinom za zaštitu podataka EU-a i SAD-a od 27. studenoga 2013., dostupno na internetu na: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Vidjeti bilješku 3.

([11]) *Schrems*, točka 97.

([12]) *Schrems*, točke 73. i 74.

([13]) *Schrems*, točke 88. i 89.

(12) Komisija je 2014. započela pregovore s tijelima SAD-a o jačanju programa „sigurne luke" u skladu s 13 preporuka iz Komunikacije COM(2013) 847 final. Nakon presude Suda Europske unije u predmetu *Schrems* ti su se pregovori pojačali s ciljem donošenja nove odluke o odgovarajućoj zaštiti kojom bi se ispunili zahtjevi iz članka 25. Direktive 95/46/EZ kako ga je protumačio Sud EU-a. Ishod su tih pregovora dokumenti priloženi ovoj Odluci, koji će biti objavljeni i u saveznom registru SAD-a. Načela privatnosti (Prilog II.) zajedno sa službenim pisanim izjavama i obvezama različitih tijela SAD-a navedenima u Prilogu I. i prilozima od III. do VII. čine „europsko-američki sustav zaštite privatnosti".

(13) Komisija je pažljivo analizirala američko pravo i praksu, među ostalim i te službene izjave i obveze. Na temelju zaključaka razrađenih u uvodnim izjavama od 136. do 140. Komisija zaključuje da Sjedinjene Američke Države osiguravaju odgovarajuću razinu zaštite osobnih podataka koji se u okviru europsko-američkog sustava zaštite privatnosti iz Unije prenose samocertificiranim organizacijama u SAD-u.

2. **EUROPSKO-AMERIČKI SUSTAV ZAŠTITE PRIVATNOSTI**

(14) Europsko-američki sustav zaštite privatnosti temelji se na sustavu samocertificiranja kojim se američke organizacije obvezuju na poštovanje skupa načela privatnosti koji čine načela europsko-američkog sustava zaštite privatnosti i dodatna načela (dalje u tekstu zajedno: Načela), koja je izdalo Ministarstvo trgovine SAD-a i koja se nalaze u Prilogu II. ovoj Odluci. Primjenjuje se i na voditelje i na izvršitelje obrade (posrednike), uz posebnost da izvršitelji moraju biti ugovorno obvezani da djeluju samo prema uputama voditelja obrade u EU-u i pomažu mu pri odgovaranju pojedincima koji ostvaruju svoja prava u skladu s Načelima ([14]).

(15) Ne dovodeći u pitanje usklađenost s nacionalnim odredbama donesenima na temelju Direktive 95/46/EZ, ova Odluka znači da su dopušteni prijenosi od voditelja ili izvršitelja obrade u Uniji organizacijama u SAD-u koje su samocertificirale svoje pridržavanje Načela pri Ministarstvu trgovine i obvezala se poštovati ih. Načela se primjenjuju isključivo na obradu osobnih podataka u organizacijama iz SAD-a ako takva obrada nije obuhvaćena područjem primjene zakonodavstva Unije ([15]). Sustav zaštite privatnosti ne utječe na primjenu zakonodavstva Unije koje se odnosi na obradu osobnih podataka u državama članicama ([16]).

([14]) Vidjeti Prilog II. odjeljak III. točku 10. podtočku (a). Prema definiciji iz odjeljka I. točke 8. podtočke (c) voditelj obrade u EU-u određuje svrhu obrade i sredstva za obradu osobnih podataka. Nadalje, iz ugovora s posrednikom mora biti jasno jesu li dopušteni daljnji prijenosi (vidjeti odjeljak III. točku 10. podtočku (a) podtočku ii. podtočku 2.).

([15]) To vrijedi i kad je riječ o podacima o ljudskim resursima koji se prenose iz Unije u kontekstu radnog odnosa. Iako se u Načelima naglašava „glavna odgovornost" poslodavca u EU-u (vidjeti Prilog II. odjeljak III. točku 9. podtočku (d) podtočku i.), iz njih je jasno da njegovo postupanje podliježe pravilima koja su primjenjiva u Uniji i/ili predmetnoj državi članici, a ne Načelima. Vidjeti Prilog II. odjeljak III. točku 9. podtočku (a) podtočku i., podtočku (b) podtočku ii., podtočku (c) podtočku i. i podtočku (d) podtočku i.

([16]) To vrijedi i za obradu pri kojoj se organizacija s poslovnim nastanom izvan Unije koristi opremom smještenom u Uniji (vidjeti članak 4. stavak 1. točku (c) Direktive 95/46/EZ). Od 25. svibnja 2018. Opća uredba o zaštiti podataka primjenjivat će se na obradu i. osobnih podataka u okviru djelatnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u Uniji (čak i ako se podaci obrađuju u SAD-u) ili ii. osobnih podataka osoba u Uniji koju obavlja voditelj ili izvršitelj obrade bez poslovnog nastana u Uniji, ako su djelatnosti obrade povezane s (a) ponudom robe ili usluga osobama čiji se podaci obrađuju, bez obzira na to trebaju li ih oni platiti ili (b) praćenjem njihovih postupaka dokle god se oni odvijaju unutar Unije. Vidjeti članak 3. stavke 1. i 2. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

(16) Zaštita osobnih podataka koju pruža sustav zaštite privatnosti primjenjuje se na svaku osobu u EU-u ([17]) čiji se osobni podaci iz Unije prenose organizacijama u SAD-u koje su samocertificirale svoje pridržavanje Načela pri Ministarstvu trgovine.

(17) Načela se primjenjuju odmah nakon certificiranja. Jedina se iznimka odnosi na načelo odgovornosti za daljnji prijenos u slučaju kad organizacija koja se samocertificira za sustav zaštite privatnosti i prije toga ima trgovinske odnose s trećim osobama. Budući da usklađivanje takvih trgovinskih odnosa s pravilima primjenjivima u skladu s načelom odgovornosti za daljnji prijenos može potrajati, organizacija će to morati učiniti što prije, u svakom slučaju najkasnije devet mjeseci od samocertificiranja (ako se to odvija u prva dva mjeseca nakon datuma stupanja na snagu sustava zaštite privatnosti). U tom prijelaznom razdoblju organizacija mora primjenjivati načela obavješćivanja i izbora (čime osobi iz EU-a čiji se podaci obrađuju omogućuje izuzeće) te, ako se osobni podaci prenose trećoj osobi koja ima ulogu posrednika, mora osigurati da ona pruža barem jednaku razinu zaštite onoj koja se zahtijeva u skladu s Načelima ([18]). Prijelaznim se razdobljem uspostavlja razumna i primjerena ravnoteža između poštovanja temeljnog prava na zaštitu podataka i legitimne potrebe poduzeća da imaju dovoljno vremena za prilagodbu novom okviru ako to ovisi i o njihovim trgovinskim odnosima s trećim osobama.

(18) Sustavom će upravljati i pratit će ga Ministarstvo trgovine na temelju svojih obveza utvrđenih u izjavama ministra trgovine SAD-a (Prilog I. ovoj Odluci). U svrhu provedbe Načela Savezna trgovinska komisija (*Federal Trade Commission*, FTC) i Ministarstvo prometa dali su izjave koje su sadržane u prilozima IV. i V. ovoj Odluci.

2.1. *Načela privatnosti*

(19) U okviru svog samocertificiranja u skladu s europsko-američkim sustavom zaštite privatnosti organizacije se moraju obvezati na poštovanje Načela ([19]).

(20) U skladu s *načelom obavješćivanja* organizacije su dužne obavijestiti osobe čiji se podaci obrađuju o nizu ključnih elemenata koji se odnose na obradu njihovih osobnih podataka (npr. o vrsti prikupljenih podataka, svrsi obrade, pravu pristupa i izbora, uvjetima u pogledu daljnjeg prijenosa i odgovornosti). Primjenjuju se dodatne zaštitne mjere, posebno zahtjev da organizacije objave svoje politike zaštite privatnosti (temeljene na Načelima) i poveznice na internetske stranice Ministarstva trgovine (s dodatnim pojedinostima o samocertificiranju, pravima osoba čiji se podaci obrađuju i dostupnim mehanizmima pravne zaštite), Popis organizacija u sustava zaštite privatnosti (na koji se upućuje u uvodnoj izjavi 30.) i internetske stranice odgovarajućeg tijela za alternativno rješavanje sporova.

(21) U skladu s *načelom o cjelovitosti podataka i ograničenju svrhe* osobni podaci moraju biti ograničeni na ono što je relevantno za svrhu obrade, pouzdano za predviđenu upotrebu, točno, potpuno i ažurirano. Organizacija ne smije obrađivati osobne podatke na način koji nije u skladu sa svrhom za koju su prvotno prikupljeni ili koju je osoba čiji se podaci obrađuju naknadno odobrila. Organizacija mora osigurati da osobni podaci budu pouzdani za predviđenu upotrebu, točni, potpuni i ažurirani.

([17]) Ova je Odluka značajna za EGP. U Sporazumu o Europskom gospodarskom prostoru (Sporazum o EGP-u) predviđa se proširenje unutarnjeg tržišta Europske unije na tri države EGP-a: Island, Lihtenštajn i Norvešku. Zakonodavstvo Unije o zaštiti podataka, uključujući Direktivu 95/46/EZ, obuhvaćeno je Sporazumom o EGP-u i uključeno u Prilog XI. tom Sporazumu. Zajednički odbor EGP-a mora odlučiti o uključivanju ove Odluke u Sporazum o EGP-u. Kad se ova Odluka bude primjenjivala na Island, Lihtenštajn i Norvešku, europsko-američki sustav zaštite privatnosti obuhvaćat će i te tri zemlje, a upućivanja u paketu za zaštitu privatnosti na EU i njegove države članice odnosit će se i na Island, Lihtenštajn i Norvešku.

([18]) Vidjeti Prilog II. odjeljak III. točku 6. podtočku (e).

([19]) Posebna pravila kojima se osiguravaju dodatne zaštitne mjere primjenjuju se na podatke o ljudskim resursima prikupljene u kontekstu zapošljavanja, kako je utvrđeno u dodatnom načelu „Podaci o ljudskim resursima" iz načela privatnosti (vidjeti Prilog II. odjeljak III. točku 9.). Na primjer, poslodavci bi trebali poštovati želje zaposlenika u pogledu zaštite privatnosti ograničavanjem pristupa osobnim podacima, anonimizacijom određenih podataka ili dodjeljivanjem zaporki ili pseudonima. Što je najvažnije, organizacije su u pogledu takvih podataka dužne surađivati i postupati u skladu sa savjetima tijela Unije za zaštitu podataka.

(22) Ako je nova (izmijenjena) svrha bitno drukčija, ali još uvijek u skladu s prvotnom svrhom, prema *načelu izbora* osobe čiji se podaci obrađuju imaju pravo na prigovor (izuzeće). *Načelo izbora* ne zamjenjuje izričitu zabranu neusklađene obrade ([20]). Za izravni marketing ([21]) vrijede posebna pravila kojima se općenito dopušta izuzeće od upotrebe osobnih podataka „u bilo kojem trenutku". U slučaju osjetljivih podataka organizacije u pravilu moraju pribaviti izričitu suglasnost (pristanak) osobe čiji se podaci obrađuju.

(23) Budući da za njih još uvijek vrijedi *načelo o cjelovitosti podataka i ograničenju svrhe*, osobne informacije mogu se zadržati u obliku kojim se ta osoba identificira ili koji omogućuje njezinu identifikaciju (dakle u obliku osobnih podataka) samo dok služe svrsi za koje su prvotno prikupljene ili naknadno odobrene. Ta obveza ne sprečava organizacije u sustavu zaštite privatnosti da nastave obrađivati osobne informacije i dulje, ali samo onoliko dugo i u onoj mjeri u kojoj takva obrada realno služi jednoj od sljedećih posebnih svrha: arhiviranju u javnom interesu, novinarstvu, književnosti i umjetnosti, znanstvenim i povijesnim istraživanjima i statističkim analizama. Dulje zadržavanje osobnih podataka u te svrhe podliježe zaštitnim mjerama u okviru Načela.

(24) U skladu s *načelom sigurnosti* organizacije koje stvaraju, održavaju, upotrebljavaju ili šire osobne podatke moraju poduzeti „razumne i odgovarajuće" sigurnosne mjere uzimajući u obzir rizike povezane s obradom i prirodom podataka. U slučaju podobrade organizacije moraju sklopiti ugovor sa subjektom koji obavlja podobradu u kojem se jamči razina zaštite jednaka onoj koja je predviđena u Načelima te poduzeti korake za osiguravanje njegove primjerene provedbe.

(25) U skladu s *načelom pristupa* ([22]) osobe čiji se podaci obrađuju imaju pravo, bez potrebe za opravdanjem i samo uz naknadu koja nije pretjerana, pribaviti od organizacije potvrdu o tome obrađuje li podatke koji se na njih odnose te pravo da im se u razumnom roku priopći o kojim je podacima riječ. To se pravo može ograničiti samo u iznimnim okolnostima; svako uskraćivanje ili ograničavanje prava pristupa mora biti nužno i opravdano, a organizacija snosi teret dokazivanja ispunjenosti tih zahtjeva. Osobe čiji se podaci obrađuju moraju moći ispraviti, izmijeniti ili izbrisati osobne informacije ako su netočne ili su se njihovom obradom kršila Načela. U područjima gdje će poduzeća najvjerojatnije primijeniti automatiziranu obradu osobnih podataka radi donošenja odluka koje utječu na predmetnu osobu (npr. odobravanje kredita, ponude hipotekarnih kredita, zapošljavanje) pravo SAD-a nudi posebnu zaštitu od negativnih odluka ([23]). Tim se zakonima obično osigurava da pojedinci imaju pravo na informiranost o konkretnim razlozima na kojima se temelji odluka (npr. odbijanje kredita), pravo na osporavanje nepotpunih ili netočnih informacija (kao i oslanjanja na nezakonite čimbenike) i na pravnu zaštitu. Ta pravila pružaju zaštitu u vjerojatno ograničenom broju slučajeva kad bi automatizirane odluke donijela sama organizacija u sustavu zaštite privatnosti ([24]). Međutim, s obzirom na sve veću upotrebu automatizirane obrade (uključujući izradu profila) kao osnove za donošenje odluka koje utječu na pojedince u suvremenom digitalnom gospodarstvu, to je područje koje je potrebno pozorno pratiti. Kako bi se to praćenje olakšalo, s tijelima SAD-a dogovoreno je da će dijalog o automatiziranom donošenju odluka, uključujući razmjenu sličnosti i razlika u pristupu EU-a i SAD-a u tom pogledu, biti dijelom prvog godišnjeg preispitivanja, a prema potrebi i kasnijih.

([20]) To vrijedi za svaki prijenos podataka u okviru sustava zaštite privatnosti, i kad je riječ o podacima prikupljenima u radnom odnosu. Iako se samocertificirane organizacije iz SAD-a u načelu smiju koristiti podacima o ljudskim resursima za različite svrhe koje nisu povezane sa zapošljavanjem (npr. određene promidžbene sadržaje), moraju poštovati zabranu neusklađene obrade i smiju to činiti samo u skladu s *načelima obavještčivanja i izbora*. Zabranom za organizacije iz SAD-a da poduzimaju kaznene mjere protiv zaposlenika zbog ostvarivanja prava na taj izbor, uključujući svako ograničavanje mogućnosti zapošljavanja, osigurat će se da unatoč podređenom i suštinski ovisnom položaju zaposlenik bez pritiska može ostvariti pravo na slobodan izbor.

([21]) Vidjeti Prilog II. odjeljak III. točku 12.

([22]) Vidjeti i dodatno načelo „Pristup" (Prilog II. odjeljak III. točka 8.).

([23]) Vidjeti npr. Zakon o jednakim mogućnostima za dobivanje kredita (*Equal Credit Opportunity Act*, ECOA, 15 U.S.C. članak 1691. i dalje), Zakon o poštenom izvješčivanju o kreditnoj sposobnosti (*Fair Credit Reporting Act*, FRCA, 15 U.S.C. članak 1681. i dalje) ili Zakon protiv diskriminacije pri prodaji ili iznajmljivanju stambenog prostora (*Fair Housing Act*, FHA, 42 U.S.C. članak 3601. i dalje).

([24]) U kontekstu prijenosa osobnih podataka koji su prikupljeni u EU-u ugovorni odnos s pojedincem (klijentom) u većini će slučajeva biti s voditeljem obrade iz EU-a, koji mora poštovati pravila EU-a o zaštiti podataka, te će obično on donositi sve odluke koje se temelje na automatiziranoj obradi. To obuhvaća situacije u kojima podatke obrađuje organizacija u sustavu zaštite privatnosti koja ima ulogu posrednika i djeluje u ime voditelja obrade iz EU-a.

(26) U skladu s *načelom pravne zaštite, provedbe i odgovornosti* ([25]) organizacije sudionice moraju osigurati pouzdane mehanizme za osiguravanje usklađenosti s drugim Načelima i pravnu zaštitu osoba iz EU-a čiji su podaci obrađeni na neusklađen način, uključujući djelotvorna pravna sredstva. Ako se organizacija dobrovoljno odlučila na samocertificiranje ([26]) u skladu s europsko-američkim sustavom zaštite privatnosti, dužna je poštovati Načela. Da bi mogla i dalje primati osobne podatke iz Unije u okviru sustava zaštite privatnosti, takva organizacija svake godine mora ponovno proći certifikaciju za sudjelovanje u sustavu. Osim toga, organizacije moraju poduzeti mjere kako bi provjerile ([27]) jesu li njihove objavljene politike privatnosti u skladu s Načelima i potvrdile da se stvarno poštuju. To se može učiniti u okviru sustava samoprocjene, koji mora uključivati unutarnje postupke kojima se osigurava obuka zaposlenika o provedbi politika zaštite privatnosti organizacije te povremeno preispitivanje usklađenosti na objektivan način ili vanjsko preispitivanje usklađenosti, koje može uključivati reviziju ili nasumične provjere. Osim toga, organizacija mora uspostaviti djelotvoran mehanizam pravne zaštite za rješavanje pritužbi (u tom smislu vidjeti i uvodnu izjavu 43.) te podlijegati istražnim i provedbenim ovlastima FTC-a, Ministarstva prometa ili drugog ovlaštenog zakonskog tijela SAD-a koje će djelotvorno osigurati usklađenost s Načelima.

(27) Posebna pravila vrijede za tzv. „daljnje prijenose", tj. prijenose osobnih podataka iz organizacije trećoj strani koja djeluje kao voditelj ili izvršitelj obrade, bez obzira na to nalazi li se treća strana u SAD-u ili u trećoj zemlji izvan SAD-a (i EU-a). Svrha je tih pravila osigurati da se zajamčena zaštita osobnih podataka osoba iz EU-a čiji se podaci obrađuju ne dovodi u pitanje i da se ne može zaobići prosljeđivanjem trećoj strani. To je posebno važno u složenijim lancima obrade koji su tipični za današnje digitalno gospodarstvo.

(28) U skladu s *načelom odgovornosti za daljnji prijenos* ([28]) daljnji je prijenos dopušten samo i. u ograničene i određene svrhe, ii. na temelju ugovora (ili sličnog sporazuma skupine poduzeća ([29])) i iii. samo ako taj ugovor pruža razinu zaštite jednaku onoj koja je zajamčena Načelima, što uključuje zahtjev da se primjena Načela smije ograničiti samo onoliko koliko je nužno u svrhu nacionalne sigurnosti, kaznenog progona i u druge svrhe javnog interesa ([30]). To bi se trebalo tumačiti zajedno s *načelom obavještčivanja* i, u slučaju daljnjeg prijenosa trećoj strani koja djeluje kao voditelj obrade ([31]), s *načelom izbora*, prema kojem osobe čiji se podaci obrađuju moraju biti obaviještene (među ostalim) o vrsti/identitetu treće strane primatelja, o svrsi daljnjeg prijenosa kao i ponuđenom izboru te se mogu usprotiviti (zatražiti izuzeće) ili, u slučaju osjetljivih podataka, moraju izraziti „izričitu suglasnost" (dati pristanak) za daljnje prijenose. U skladu s *načelom o cjelovitosti podataka i ograničenju svrhe* obveza pružanja razine zaštite jednake onoj koja je zajamčena Načelima pretpostavlja da treća strana smije obrađivati samo osobne informacije koje su joj dostavljene za svrhe koje nisu u suprotnosti sa svrhama za koju su prvotno prikupljene ili koje je pojedinac naknadno odobrio.

(29) Obveza pružanja razine zaštite jednake onoj koja se zahtijeva u Načelima primjenjuje se na sve treće osobe uključene u obradu tako prenesenih podataka bez obzira na to gdje su smještene (u SAD-u ili drugoj trećoj zemlji), uključujući i kad sama prvotna treća strana primatelj prenese te podatke drugoj trećoj strani primatelju, primjerice u svrhu podobrade. U svakom slučaju, ugovorom s trećom stranom primateljem mora se osigurati da ona obavijesti organizaciju u sustavu zaštite privatnosti ako utvrdi da više ne može ispunjavati tu obvezu. Ako se

([25]) Vidjeti i dodatno načelo „Rješavanje sporova i provedba" (Prilog II. odjeljak III. točka 11.).
([26]) Vidjeti i dodatno načelo „Samocertificiranje" (Prilog II. odjeljak III. točka 6.).
([27]) Vidjeti i dodatno načelo „Provjera" (Prilog II. odjeljak III. točka 7.).
([28]) Vidjeti i dodatno načelo „Obvezni ugovori za daljnji prijenos" (Prilog II. odjeljak III. točka 10.).
([29]) Vidjeti i dodatno načelo „Obvezni ugovori za daljnji prijenos" (Prilog II. odjeljak III. točka 10. podtočka (b). Iako to načelo omogućuje prijenose i na osnovi izvanugovornih instrumenata (npr. usklađenost unutar skupine i programi kontrole), iz njegovog je teksta jasno da ti instrumenti moraju uvijek osigurati „kontinuitet zaštite osobnih podataka u skladu s Načelima". Nadalje, budući da će samocertificirane organizacije iz SAD-a i dalje biti odgovorne za usklađenost s Načelima, imat će jak poticaj za upotrebu instrumenata koji su doista djelotvorni u praksi.
([30]) Vidjeti Prilog II. odjeljak I. točku 5.
([31]) Pojedinci neće imati pravo zatražiti izuzeće ako se podaci prenose trećoj strani koja u ulozi posrednika izvršava zadaće u ime i prema uputama organizacije iz SAD-a. Međutim, to zahtijeva ugovor s posrednikom, a organizacija iz SAD-a snosi odgovornost za jamčenje zaštite u okviru Načela izvršavanjem svojih ovlasti za davanje uputa.

to utvrdi, obrada koju provodi treća strana prestaje ili se moraju poduzeti drugi razumni i odgovarajući koraci za rješavanje te situacije ([32]). Ako se u lancu (pod)obrade pojave problemi u pogledu usklađenosti, organizacija u sustavu zaštite privatnosti koja ima ulogu voditelja obrade osobnih podataka morat će dokazati da nije odgovorna za događaj kojim je uzrokovana šteta ili u protivnom snositi odgovornost u skladu s *načelom pravne zaštite, provedbe i odgovornosti*. Dodatna zaštita primjenjuje se u slučaju daljnjeg prijenosa trećoj strani posredniku ([33]).

2.2. *Transparentnost europsko-američkog sustava zaštite privatnosti, upravljanje njime i nadzor nad njime*

(30) Europsko-američki sustav zaštite privatnosti pruža mehanizme nadzora i provedbe kako bi se potvrdilo i osiguralo da samocertificirana poduzeća iz SAD-a poštuju Načela te reagiralo na svaku neusklađenost. Ti su mehanizmi navedeni u Načelima (Prilog II.) i obvezama Ministarstva trgovine (Prilog I.), FTC-a (Prilog IV.) i Ministarstva prometa (Prilog V.).

(31) Kako bi se osigurala pravilna primjena europsko-američkog sustava zaštite privatnosti, zainteresirane strane, kao što su osobe čiji se podaci obrađuju, izvoznici podataka i nacionalna tijela za zaštitu podataka, moraju moći prepoznati organizacije koje poštuju Načela. U tu se svrhu Ministarstvo trgovine SAD-a obvezalo da će voditi i objavljivati popis organizacija koje su samocertificirale svoje pridržavanje Načela i koje su u nadležnosti barem jednog provedbenog tijela iz priloga I. i II. ovoj Odluci (dalje u tekstu: Popis organizacija u sustavu zaštite privatnosti) ([34]). Ministarstvo trgovine ažurirat će taj popis na temelju godišnjih podnesaka organizacija o ponovnom certificiranju i svaki put kad se organizacija povuče ili je isključena iz europsko-američkog sustava zaštite privatnosti. Osim toga, vodit će i objavljivati evidenciju organizacija koje su uklonjene s popisa te za svaku navesti razlog zbog kojeg je uklonjena. Naposljetku, navest će poveznicu na popis slučajeva u kojima je FTC intervenirao radi osiguravanja provedbe propisa povezanih sa sustavom zaštite privatnosti, koji se nalazi na internetskim stranicama FTC-a.

(32) Ministarstvo trgovine objavit će i Popis organizacija u sustavu zaštite privatnosti i podneske za ponovno certificiranje na posebnoj internetskoj stranici. Samocertificirane organizacije moraju navesti internetsku adresu Ministarstva s Popisom organizacija u sustavu zaštite privatnosti. Nadalje, ako je dostupna na internetu, politika zaštite privatnosti određene organizacije mora uključivati poveznicu na internetske stranice sustava zaštite privatnosti te poveznicu na internetske stranice ili obrazac za podnošenje pritužbi neovisnog mehanizma pravne zaštite koji je dostupan za istraživanje neriješenih pritužbi. Ministarstvo trgovine će u kontekstu certificiranja i ponovnog certificiranja organizacije u skladu s okvirom sustavno provjeravati je li njezina politika zaštite privatnosti u skladu s Načelima.

(33) Organizacije koje ustrajno ne poštuju Načela bit će uklonjene s Popisa organizacija u sustavu zaštite privatnosti te moraju vratiti ili izbrisati osobne podatke zaprimljene u okviru europsko-američkog sustava zaštite privatnosti. U drugim slučajevima uklanjanja, kao što je dobrovoljno povlačenje iz sudjelovanja ili izostanak ponovnog certificiranja, organizacija smije zadržati takve podatke ako svake godine Ministarstvu trgovine potvrdi da se obvezuje primjenjivati Načela ili ako osigura odgovarajuću zaštitu osobnih podataka drugim odobrenim sredstvima (npr. upotrebom ugovora koji se temelji na zahtjevima relevantnih standardnih ugovornih odredaba koje je odobrila Komisija). U tom slučaju organizacija mora odrediti kontaktnu točku za sva pitanja povezana sa sustavom zaštite privatnosti.

(34) Ministarstvo trgovine pratit će organizacije koje više nisu članovi europsko-američkog sustava zaštite privatnosti, bilo zato što su se dobrovoljno povukle ili što im je istekao certifikat, kako bi provjerile hoće li vratiti, izbrisati ili zadržati ([35]) osobne podatke zaprimljene dok su još bile dio sustava. Zadrže li podatke, organizacije su dužne na

([32]) Situacija se razlikuje ovisno o tome je li treća strana voditelj ili izvršitelj obrade (posrednik). U prvom slučaju ugovorom s trećom stranom mora se osigurati da ona obustavi obradu ili poduzme druge razumne i odgovarajuće mjere za rješavanje situacije. U drugom slučaju te mjere mora poduzeti organizacija u sustavu zaštite privatnosti kao ona koja vodi obradu i prema čijim uputama djeluje posrednik.

([33]) U tom slučaju organizacija iz SAD-a osim toga mora poduzeti razumne i odgovarajuće mjere i. kako bi osigurala da posrednik učinkovito obrađuje osobne informacije prenesene u skladu s obvezama organizacije prema Načelima i ii. kako bi, nakon podnošenja obavijesti, zaustavila i ispravila neovlaštenu obradu nakon obavijesti.

([34]) Informacije o vođenju Popisa organizacija u sustavu zaštite privatnosti mogu se naći u Prilogu I. i Prilogu II. (odjeljak I. točka 3., odjeljak I. točka 4., odjeljak III. točka 6. podtočka (d) i odjeljak III. točka 11. podtočka (g).

([35]) Vidjeti npr. Prilog II. odjeljak I. točku 3., odjeljak III. točku 6. podtočku (f) i odjeljak III. točku 11. podtočku (g) podtočku i.

njih i dalje primjenjivati Načela. Ako je Ministarstvo trgovine uklonilo organizacije iz sustava zbog ustrajnog nepoštovanja Načela, ono će osigurati da te organizacije vrate ili izbrišu osobne podatke koje su zaprimile u okviru sustava.

(35) Ako organizacija napusti europsko-američki sustav zaštite privatnosti iz bilo kojeg razloga, mora ukloniti sve javne izjave iz kojih bi se moglo zaključiti da i dalje sudjeluje u tom sustavu ili da ima pravo na pogodnosti koje iz njega proizlaze, a posebno upućivanja na taj sustav u svojoj objavljenoj politici zaštite privatnosti. Ministarstvo trgovine tražit će i uklanjati lažne tvrdnje o sudjelovanju u sustavu, među ostalim i bivših članova ([36]). Svako lažno predstavljanje javnosti organizacija u pogledu svog pridržavanja Načela u obliku zavaravajuće izjave ili prakse podliježe provedbenim mjerama FTC-a, Ministarstva prometa ili drugih provedbenih tijela u SAD-u; lažno predstavljanje Ministarstvu trgovine kažnjivo je u skladu sa Zakonom o lažnim izjavama (*False Statements Act*, 18 U.S.C. članak 1001.) ([37]).

(36) Ministarstvo trgovine po službenoj dužnosti prati lažne tvrdnje o sudjelovanju u sustavu zaštite privatnosti ili o neprimjerenoj upotrebi certifikacijske oznake tog sustava, a tijela za zaštitu privatnosti mogu uputiti organizacije na preispitivanje posebnoj kontaktnoj točki u Ministarstvu. Ako se organizacija povukla iz europsko-američkog sustava zaštite privatnosti, nije se ponovno samocertificirala ili je uklonjena s Popisa organizacija u sustavu zaštite privatnosti, Ministarstvo trgovine redovito će provjeravati je li ta organizacija iz svoje objavljene politike o zaštiti privatnosti izbrisala upućivanja na sustav zaštite privatnosti iz kojih bi se moglo zaključiti da i dalje sudjeluje u tom sustavu, a ako ona nastavi davati lažne tvrdnje, uputit će predmet FTC-u, Ministarstvu prometa ili drugom nadležnom tijelu radi mogućih provedbenih mjera. Slat će i upitnike organizacijama čije je samocertificiranje isteklo ili koje su se dobrovoljno povukle iz europsko-američkog sustava privatnosti kako bi provjerilo hoće li vratiti ili izbrisati osobne podatke zaprimljene tijekom sudjelovanja u tom sustavu ili će na njih i dalje primjenjivati načela privatnosti te, ako ih zadrži, provjeriti tko će u organizaciji biti stalna kontaktna točka za pitanja povezana s tim sustavom.

(37) Ministarstvo trgovine redovito će po službenoj dužnosti provoditi preispitivanja usklađenosti ([38]) samocertificiranih organizacija, uključujući slanjem detaljnih upitnika. Sustavno će provoditi preispitivanja i kad god zaprimi konkretnu (ozbiljnu) pritužbu, kad organizacija ne da zadovoljavajući odgovor na upite ili kad postoje vjerodostojni dokazi koji upućuju na to da organizacija možda ne poštuje Načela. Prema potrebi će se o takvim preispitivanjima usklađenosti Ministarstvo trgovine savjetovati i s tijelima za zaštitu podataka.

2.3. *Mehanizmi pravne zaštite, rješavanje pritužbi i provedba*

(38) U skladu s *načelom pravne zaštite, provedbe i odgovornosti* europsko-američkog sustava zaštite privatnosti organizacije moraju osigurati pravnu zaštitu osoba na koje utječe neusklađenost te mora postojati mogućnost da osobe čiji se podaci obrađuju podnesu prigovor u pogledu neusklađenosti samocertificiranih poduzeća u SAD-u i da se njihove pritužbe riješe, prema potrebi odlukom kojom se pruža djelotvorno pravno sredstvo.

(39) U okviru svog samocertificiranja organizacije moraju ispunjavati zahtjeve načela pravne zaštite, provedbe i odgovornosti osiguravanjem učinkovitih i dostupnih neovisnih mehanizama pravne zaštite u okviru kojih se pritužbe i sporovi svake osobe mogu istražiti bez troška za nju.

(40) Organizacije mogu odabrati neovisne mehanizme pravne zaštite u Uniji ili u SAD-u. To uključuje mogućnost da se dobrovoljno obvežu na suradnju s tijelima za zaštitu podataka u EU-u. Međutim, takva mogućnost ne postoji

([36]) Vidjeti Prilog I. odjeljak „Tražiti i uklanjati lažne tvrdnje o sudjelovanju".
([37]) Vidjeti Prilog II. odjeljak III. točku 6. podtočku (h) i odjeljak III. točku 11. podtočku (f).
([38]) Vidjeti Prilog I.

ako organizacije obrađuju podatke o ljudskim resursima jer je u tom slučaju suradnja s tijelima za zaštitu podataka obvezna. Druge su mogućnosti neovisno alternativno rješavanje sporova ili *programi za zaštitu privatnosti* razvijeni u privatnom sektoru u čija su pravila ugrađena Načela. Takvi programi moraju obuhvaćati učinkovite provedbene mehanizme u skladu sa zahtjevima načela pravne zaštite, provedbe i odgovornosti. Organizacije su dužne riješiti svaki problem neusklađenosti. Moraju navesti i da podliježu istražnim i provedbenim ovlastima FTC-a, Ministarstva prometa ili drugog ovlaštenog zakonskog tijela SAD-a.

(41) Stoga se u okviru sustava zaštite privatnosti osobama čiji se podaci obrađuju nudi niz mogućnosti za ostvarenje njihovih prava, podnošenje pritužbi zbog neusklađenosti samocertificiranih poduzeća u SAD-u i rješavanje pritužbi, prema potrebi odlukom kojom se pruža djelotvorno pravno sredstvo. Pojedinci mogu podnijeti pritužbu izravno organizaciji, neovisnom tijelu za rješavanje sporova koje određuje organizacija, nacionalnim tijelima za zaštitu podataka ili FTC-u.

(42) Ako se njihove pritužbe ne razriješe nijednim od tih mehanizama pravne zaštite ili provedbe, pojedinci imaju pravo zatražiti i obvezujuću arbitražu u okviru Odbora za sustav zaštite privatnosti (Prilog 1. Priloga II. ove Odluke). Osim arbitražnog odbora, na koji se moguće pozvati tek kad se prije toga iscrpe određena pravna sredstva, pojedinci se mogu poslužiti bilo kojim ili svim mehanizmima pravne zaštite po svom izboru i ne moraju odabrati samo jedan ili pratiti poseban redoslijed. Međutim, postoji određeni logičan redoslijed koji se preporučuje, kako je navedeno u nastavku.

(43) Prvo, osobe iz EU-a čiji se podaci obrađuju mogu rješavati slučajeve neusklađenosti s Načelima izravnim obraćanjem *samocertificiranom poduzeću u SAD-u*. Kako bi olakšala pronalaženje rješenja, organizacija mora uspostaviti učinkovit mehanizam pravne zaštite za rješavanje takvih pritužbi. Stoga organizacija svojom politikom zaštite privatnosti pojedince mora jasno obavijestiti o unutarnjoj ili vanjskoj kontaktnoj točki koja će rješavati pritužbe (uključujući sve relevantne subjekte u Uniji koji mogu odgovarati na upite ili pritužbe) i o neovisnim mehanizmima za rješavanje pritužbi.

(44) Po primitku pritužbe, izravno od pojedinca ili preko Ministarstva trgovine nakon što je uputi tijelo za zaštitu podataka, organizacija mora odgovoriti osobi iz EU-a čiji se podaci obrađuju u roku od 45 dana. Odgovor mora uključivati procjenu osnovanosti pritužbe i informacije o tome kako će organizacija riješiti problem. Isto tako, organizacije moraju brzo odgovoriti na upite i druge zahtjeve za informacije Ministarstva trgovine ili tijela za zaštitu podataka ([39]) (ako se organizacija obvezala na suradnju s tijelom za zaštitu podataka) u pogledu svojeg pridržavanja Načela. Organizacije moraju voditi evidenciju o provedbi svojih politika zaštite privatnosti i na zahtjev ih staviti na raspolaganje neovisnom mehanizmu pravne zaštite ili FTC-u (ili drugom tijelu SAD-a nadležnom za istraživanje nepoštene i prijevarne prakse) u okviru istrage ili pritužbe o neusklađenosti.

(45) Drugo, pojedinci mogu podnijeti pritužbu izravno *neovisnom tijelu za rješavanje sporova* (u SAD-u ili u EU-u) koje organizacija odredi za istragu i rješavanje pojedinačnih pritužbi (osim ako su očito neutemeljene ili neozbiljne) te za pružanje primjerene i besplatne pravne zaštite pojedincu. Sankcije i pravna sredstva koje određuje takvo tijelo moraju biti dovoljno strogi da se njima osigura da organizacije poštuju Načela i njima bi trebalo biti predviđeno da organizacija poništi ili ispravi učinke neusklađenosti i, ovisno o okolnostima, prekine daljnju obradu osobnih podataka o kojima je riječ i/ili ih izbriše te objavi informacije o utvrđenoj neusklađenosti. Neovisna tijela za rješavanje sporova koja odredi organizacija morat će na svojim javnim internetskim stranicama navesti odgovarajuće informacije o europsko-američkom sustavu zaštite privatnosti i uslugama koje pružaju u okviru tog sustava. Ona svake godine moraju objaviti godišnje izvješće s objedinjenim podacima o tim uslugama ([40]).

([39]) To je tijelo za rješavanje pritužbi koje određuje odbor tijela za zaštitu podataka predviđen u dodatnom načelu „Uloga tijela za zaštitu podataka" (Prilog II. odjeljak III. točka 5.).

([40]) Godišnje izvješće mora sadržavati informacije o sljedećem: 1. ukupnom broju pritužbi povezanih sa sustavom zaštite privatnosti zaprimljenih tijekom izvještajne godine; 2. vrstama zaprimljenih pritužbi; 3. mjerama kvalitete rješavanja sporova, kao što je trajanje obrade zahtjeva i 4. ishodu zaprimljenih pritužbi, posebno o broju i vrstama pravnih sredstava ili izrečenih sankcija.

(46) U okviru svojih postupaka preispitivanja usklađenosti Ministarstvo trgovine provjerit će i jesu li se samocertificirana američka poduzeća doista registrirala kod neovisnih mehanizama pravne zaštite kod kojih tvrde da su registrirana. Organizacije i odgovorni neovisni mehanizmi pravne zaštite moraju brzo odgovoriti na upite i zahtjeve Ministarstva trgovine za informacije povezane sa sustavom zaštite privatnosti.

(47) Ako organizacija ne postupi u skladu s odlukom tijela za rješavanje sporova ili samoregulatornog tijela, potonje mora o tome obavijestiti Ministarstvo trgovine i FTC (ili drugo tijelo SAD-a nadležno za istragu nepoštene ili prijevarne prakse) ili nadležni sud ([41]). Ako organizacija odbije pridržavati se konačne odluke bilo kojeg samoregulatornog tijela za zaštitu privatnosti, neovisnog tijela za rješavanje sporova ili državnog tijela, ili ako takvo tijelo utvrdi da organizacija ne djeluje u skladu s Načelima, to će se smatrati ustrajnim nepoštovanjem Načela te će Ministarstvo trgovine, nakon što joj da rok od 30 dana i priliku da odgovori, organizaciju koja ne djeluje u skladu s Načelima ukloniti s popisa ([42]). Ako i nakon što je uklonjena s popisa organizacija i dalje tvrdi da je certificirana u okviru sustava zaštite podataka, Ministarstvo će je uputiti FTC-u ili drugoj provedbenoj agenciji ([43]).

(48) Treće, pojedinci mogu podnijeti pritužbe i nacionalnom *tijelu za zaštitu podataka*. Organizacije su dužne surađivati s tijelima za zaštitu podataka pri istrazi i rješavanju pritužbi ako se one odnose na obradu podataka o ljudskim resursima prikupljenima u kontekstu radnog odnosa ili ako se predmetna organizacija dobrovoljno podvrgnula nadzoru tijela za zaštitu podataka. Organizacije svakako moraju odgovarati na upite, postupati u skladu sa savjetima tijela za zaštitu podatka, uključujući u pogledu mjera za zaštitu prava ili naknadu štete, i dostaviti tijelu za zaštitu podataka pisanu potvrdu da su te mjere poduzete.

(49) Savjet tijela za zaštitu podataka dostavit će neslužbeni odbor tijela za zaštitu podataka uspostavljen na razini Unije ([44]), što će pridonijeti usklađenom i dosljednom pristupu predmetnoj pritužbi. Savjet će se objaviti nakon što su obje stranke u sporu imale razumnu mogućnost dati primjedbe i dostaviti dokaze koje žele. Odbor će dati savjet čim to bude moguće u skladu sa zahtjevom za primjerenim postupkom i u pravilu u roku od 60 dana nakon primitka pritužbe. Ako organizacija ne postupi u skladu sa savjetom u roku od 25 dana od njegova primitka i ako nije ponudila zadovoljavajuće objašnjenje za kašnjenje, odbor će je obavijestiti o svojoj namjeri da slučaj podnese FTC-u (ili drugom nadležnom provedbenom tijelu u SAD-u) ili da zaključi kako je došlo do ozbiljne povrede obveze suradnje. U prvom slučaju to može dovesti do pokretanja postupka za provedbu obveza u skladu s odjeljkom 5. Zakona o FTC-u (ili sličnim zakonom). U drugom slučaju odbor će obavijestiti Ministarstvo trgovine, koje će odbijanje organizacije da se pridržava savjeta odbora tijela za zaštitu podataka smatrati ustrajnim nepoštovanjem Načela, što će dovesti do uklanjanja organizacije s Popisa organizacija u sustavu zaštite privatnosti.

(50) Ako tijelo za zaštitu podataka kojem je upućena pritužba nije poduzelo mjere za rješavanje pritužbe ili ih nije poduzelo dovoljno, podnositelj pritužbe zbog toga može pokrenuti postupak pred nacionalnim sudovima nadležne države članice.

(51) Pojedinci mogu podnijeti pritužbe tijelima za zaštitu podataka čak i ako organizacija nije odredila njihov odbor kao tijelo za rješavanje svojih sporova. U tim slučajevima tijelo za zaštitu podataka takve pritužbe može uputiti Ministarstvu trgovine ili FTC-u. Kako bi olakšalo i ojačalo suradnju u pogledu pojedinačnih pritužbi i neusklađenosti organizacija u sustavu zaštite podataka, Ministarstvo trgovine uspostavit će posebnu kontaktnu točku koja će služiti kao točka za vezu i pomagati u istragama tijela za zaštitu podataka o tome djeluje li organizacija u skladu s Načelima ([45]). FTC se isto tako obvezao uspostaviti posebnu kontaktnu točku ([46]) i pomagati tijelima za zaštitu podataka pri istrazi u skladu s američkim Zakonom o sigurnosti interneta (*U.S. SAFE WEB Act*) ([47]).

([41]) Vidjeti Prilog II. odjeljak III. točku 11. podtočku (e).
([42]) Vidjeti Prilog II. odjeljak III. točku 11. podtočku (g), posebno podtočke ii. i iii.
([43]) Vidjeti Prilog I. odjeljak „Tražiti i uklanjati lažne tvrdnje o sudjelovanju".
([44]) Tijela za zaštitu podataka bi na temelju svoje sposobnosti za organizaciju rada i međusobnu suradnju trebala uspostaviti poslovnik svog neslužbenog odbora.
([45]) Vidjeti Prilog I., odjeljke „Pojačati suradnju s tijelima za zaštitu podataka" i „Olakšati rješavanje pritužbi o neusklađenosti" te Prilog II. odjeljak II. točku 7. podtočku (e).
([46]) Vidjeti Prilog IV. str. 6.
([47]) *Ibid*.

(52) Četvrto, *Ministarstvo trgovine* obvezalo se da će primati i preispitivati pritužbe o tome da organizacija ne poštuje Načela te ih koliko god je to moguće nastojati riješiti. U tu svrhu Ministarstvo trgovine predviđa posebne postupke kojima tijela za zaštitu podataka upućuju pritužbe posebnoj kontaktnoj točki, prate ih i surađuju s poduzećima u pronalaženju rješenja. Kako bi se ubrzala obrada pojedinačnih pritužbi, kontaktna točka izravno će se povezati s odgovarajućim tijelom za zaštitu podataka u vezi s pitanjima poštovanja Načela te ga posebno informirati o statusu pritužbi u roku od najviše 90 dana nakon upućivanja. Tako će se osobama čiji se podaci obrađuju omogućiti da svojim nacionalnim tijelima za zaštitu podataka izravno podnesu pritužbe o neusklađenosti američkih samocertificiranih poduzeća te da ih ona proslijede Ministarstvu trgovine kao tijelu SAD-a nadležnom za upravljanje europsko-američkim sustavom zaštite privatnosti. Ministarstvo trgovine obvezalo se, u okviru godišnjeg preispitivanja funkcioniranja europsko-američkog sustava zaštite privatnosti, dostavljati i izvješće s analizom zahtjeva u agregiranom obliku koje zaprima svake godine ([48]).

(53) Ako na temelju provjera pritužbi ili bilo kojih drugih informacija po službenoj dužnosti Ministarstvo trgovine zaključi da organizacija ustrajno ne poštuje Načela, uklonit će je s Popisa organizacija u sustavu zaštite privatnosti. Nepoštovanje konačne odluke bilo kojeg samoregulatornog tijela za zaštitu privatnosti, neovisnog tijela za rješavanje sporova ili državnog tijela, uključujući tijelo za zaštitu privatnosti, smatrat će se ustrajnim nepoštovanjem Načela.

(54) Peto, organizacija u sustavu zaštite privatnosti podliježe istražnim i provedbenim ovlastima tijela SAD-a, posebno *Savezne trgovinske komisije* ([49]) (FTC-a), koja će učinkovito osigurati usklađenost s Načelima. FTC će davati prednost razmatranju slučajeva neusklađenosti s načelima privatnosti koje su joj uputila neovisna tijela za rješavanje sporova ili samoregulatorna tijela, Ministarstvo trgovine i tijela za zaštitu podataka (djelujući na vlastitu inicijativu ili na temelju pritužbi) kako bi utvrdio je li prekršen odjeljak 5. Zakona o FTC-u ([50]). FTC se obvezao na to da će uspostaviti standardizirani postupak upućivanja, odrediti kontaktnu točku kojoj tijela za zaštitu podataka mogu upućivati predmete i da će razmjenjivati informacije o upućenim predmetima. Osim toga, prihvaćat će pritužbe izravno od pojedinaca i pokretat će istrage u okviru sustava zaštite privatnosti na vlastitu inicijativu, posebno u okviru svojih opsežnijih istraga o pitanjima zaštite privatnosti.

(55) FTC može osigurati usklađenost upravnim rješenjima („*consent orders*", rješenjima kojima se nalaže usklađivanje) i sustavno će pratiti usklađenost s tim rješenjima. Ako organizacije ne postupe u skladu s tim, FTC može uputiti predmet nadležnom sudu tražeći sudske penale ili neku drugu vrstu pravne zaštite, među ostalim za štetu uzrokovanu nezakonitim postupanjem. Osim toga, FTC može izravno od saveznog suda tražiti privremenu ili trajnu zabranu ili neku drugu vrstu pravne zaštite. Svaki nalog za suglasnost izdan organizaciji u sustavu zaštite privatnosti sadržavat će odredbe o izvješćivanju samih organizacija ([51]), a organizacije će morati objaviti sve relevantne odjeljke izvješća o usklađenosti ili procjeni dostavljenog FTC-u koji su povezani sa sustavom zaštite privatnosti. Osim toga, FTC će voditi internetski popis poduzeća pod nalogom FTC-a ili sudskim nalogom u predmetima povezanima sa sustavom zaštite privatnosti.

(56) Šesto, kao posljednji mehanizam pravne zaštite koji se upotrebljava samo ako se drugim dostupnim oblicima pravne zaštite pritužba ne riješi na zadovoljavajući način, osoba iz EU-a čiji se podaci obrađuju može zatražiti obvezujuću arbitražu pred „*Odborom za sustav zaštite privatnosti*". Organizacija mora obavijestiti pojedince o mogućnosti da, pod određenim uvjetima, zatraže obvezujuću arbitražu te su, odabere li osoba tu mogućnost, dužne odgovoriti slanjem obavijesti predmetnoj organizaciji ([52]).

([48]) Vidjeti Prilog I., odjeljak „Olakšati rješavanje pritužbi o neusklađenosti".

([49]) Organizacija u sustavu zaštite privatnosti mora javno izjaviti da se obvezala uskladiti s Načelima, javno objaviti svoju politiku zaštite privatnosti u skladu s Načelima i potpuno je provesti. Neusklađenost je kažnjiva u skladu s odjeljkom 5. Zakona o FTC-u kojim se zabranjuju nepoštene i prijevarne radnje u trgovini ili koje utječu na trgovinu.

([50]) Prema informacijama iz FTC-a on nema ovlasti provoditi inspekcije na terenu u području zaštite privatnosti. Međutim, ovlašten je zahtijevati od organizacija da dostave dokumente i pribave izjave svjedoka (vidjeti odjeljak 20. Zakona o FTC-u) te se u slučaju neusklađenosti može koristiti sudskim sustavom za provedbu takvih naloga.

([51]) Nalozima FTC-a ili sudskim nalozima može se zahtijevati od poduzeća da provode programe zaštite privatnosti i redovito dostavljaju izvješća o usklađenosti ili neovisne procjene tih programa koje provodi treća strana i koje su dostupne FTC-u.

([52]) Vidjeti Prilog II. odjeljak II. točku 1. podtočku xi. i odjeljak III. točku 7. podtočku (c).

(57) Arbitražni odbor bit će sastavljen od najmanje 20 arbitara koje imenuju Ministarstvo trgovine i Komisija na temelju njihove neovisnosti, integriteta i iskustva u području prava o zaštiti privatnosti SAD-a i prava o zaštiti podataka EU-a. Za svaki pojedini spor stranke biraju jednog ili tri arbitra iz te skupine ([53]). Na postupak se primjenjuju uobičajena pravila o arbitraži dogovorena između Ministarstva trgovine i Komisije. Tim će se pravilima dopuniti već sklopljeni okvir koji sadržava više značajki za povećanje dostupnosti tog mehanizma osobama u EU-u čiji se podaci obrađuju: i. pri pripremi zahtjeva za odbor osobi čiji se podaci obrađuju smije pomoći njezino nacionalno tijelo za zaštitu podataka; ii. arbitraža će se odvijati u SAD-u, ali osobe iz EU-a čiji se podaci obrađuju mogu odlučiti sudjelovati putem videokonferencije ili telefonske konferencije, koja im je besplatno osigurana; iii. jezik na kojem će se odvijati arbitraža u pravilu će biti engleski, ali bi pri arbitražnom saslušanju osobi čiji se podaci obrađuju na obrazložen zahtjev trebala ([54]) biti pružena besplatna usluga prevođenja; iv. iako svaka stranka mora snositi vlastite odvjetničke troškove, ako stranku pred Odborom zastupa odvjetnik, Ministarstvo trgovine osniva fond u koji organizacije u sustavu zaštite privatnosti svake godine uplaćuju doprinose i kojim se pokrivaju prihvatljivi troškovi arbitražnog postupka, do najvećeg iznosa koji određuju nadležna tijela SAD-a u dogovoru s Komisijom.

(58) Odbor za sustav zaštite privatnosti ima ovlasti odrediti „pojedinačnu nenovčanu pravičnu naknadu" ([55]) koja je nužna za ispravljanje neusklađenosti s Načelima. Iako će Odbor pri donošenju odluke uzeti u obzir druge vrste pravne zaštite koje već postoje u okviru drugih mehanizama u sustavu zaštite privatnosti, osobe svejedno mogu pokrenuti arbitražni postupak ako smatraju da druge vrste pravne zaštite nisu dovoljne. Time će se osobama iz EU-a čiji se podaci obrađuju omogućiti da pokrenu arbitražni postupak u svim slučajevima kad nadležna tijela SAD-a (na primjer FTC) nisu djelovanjem ili nedjelovanjem na zadovoljavajući način riješila njihove pritužbe. Nije moguće pokrenuti arbitražni postupak ako tijelo za zaštitu podatka ima pravne ovlasti riješiti predmetno pitanje u vezi sa samocertificiranim poduzećem u SAD-u, posebno u slučajevima u kojima je organizacija dužna surađivati i postupati u skladu sa savjetima tijela za zaštitu podataka u pogledu obrade podataka o ljudskim resursima prikupljenih u kontekstu zapošljavanja ili se na to dobrovoljno obvezala. Pojedinci mogu zatražiti provedbu arbitražne odluke pred američkim sudovima u skladu sa Saveznim zakonom o arbitraži i tako osigurati pravnu zaštitu u slučaju da poduzeće ne postupi u skladu s odlukom.

(59) Sedmo, ako organizacija ne ispuni svoju obvezu u skladu s Načelima i objavljenom politikom zaštite privatnosti, u pravu američkih saveznih država mogu biti dostupni drugi oblici pravne zaštite u skladu s pravom naknade štete i u slučajevima lažnog prikazivanja, nepoštenih ili prijevarnih radnji ili prakse ili kršenja ugovora.

(60) Osim toga, ako tijelo za zaštitu podataka po primitku zahtjeva osobe u EU-u čiji se podaci obrađuju smatra da se prijenosom njezinih osobnih podataka organizaciji u SAD-u krši pravo EU-a o zaštiti podataka, uključujući i kad izvoznik podataka u EU-u ima razloga vjerovati da ta organizacija ne djeluje u skladu s Načelima, ono može izvršavati svoje ovlasti i prema izvozniku podataka te, prema potrebi, zatražiti suspenziju prijenosa podataka.

(61) Na temelju informacija iz ovog odjeljka Komisija smatra da se Načelima koja je izdalo američko Ministarstvo trgovine osigurava razina zaštite osobnih podataka koja je u osnovi jednakovrijedna razini zajamčenoj materijalnim osnovnim načelima iz Direktive 95/46/EZ.

(62) Nadalje, djelotvorna primjena Načela zajamčena je obvezama transparentnosti, upravljanjem sustavom zaštite privatnosti i provjerom usklađenosti koje provodi Ministarstvo trgovine.

(63) Nadalje, Komisija smatra da se mehanizmima nadzora, pravne zaštite i provedbe u cjelini, koji se osiguravaju u okviru sustava zaštite privatnosti, omogućuje otkrivanje i kažnjavanje u praksi organizacija u tom sustavu koje krše Načela te se osobi čiji se podaci obrađuju osiguravaju pravna sredstva za ostvarivanje pristupa njezinim osobnim podacima te za ispravak ili brisanje takvih podataka.

([53]) Stranke se dogovaraju i o broju arbitara u Odboru.

([54]) Međutim, Odbor može utvrditi da bi, u okolnostima određenog arbitražnog postupka, pokrivanje troškova bilo neopravdano ili nerazmjerno.

([55]) Osobe ne mogu u postupku arbitraže tražiti naknadu štete, ali pokretanjem arbitražnog postupka ne gubi se mogućnost traženja naknade štete na redovnim američkim sudovima.

3. PRISTUP AMERIČKIH JAVNIH TIJELA OSOBNIM PODACIMA PRENESENIMA U OKVIRU EUROPSKO-AMERIČKOG SUSTAVA ZAŠTITE PRIVATNOSTI I NJIHOVA UPOTREBA TIH PODATAKA

(64) U skladu s Prilogom II. odjeljkom I. točkom 5. pridržavanje Načela ograničeno je na mjeru koja je nužna da se ispune zahtjevi u pogledu nacionalne sigurnosti, javnog interesa ili kaznenog progona.

(65) Komisija je procijenila ograničenja i zaštitne mjere dostupne u američkom pravu u vezi s pristupom američkih javnih tijela osobnim podacima prenesenima u okviru europsko-američkog sustava zaštite privatnosti i upotrebom tih podataka u svrhu nacionalne sigurnosti, kaznenog progona i drugih javnih interesa. Nadalje, američka vlada je posredstvom svog Ureda direktora nacionalne obavještajne službe (*Office of the Director of National Intelligence*, ODNI) ([56]) Komisiji dostavila detaljne izjave i obveze koji se nalaze u Prilogu VI. ovoj Odluci. Dopisom koji je potpisao ministar vanjskih poslova (*Secretary of State*) (Prilog III. ovoj Odluci) američka vlada obvezala se uvesti novi mehanizam za nadzor povreda nacionalne sigurnosti, naime Pravobranitelja za sustav zaštite privatnosti, koji je neovisan o obavještajnoj zajednici. Naposljetku, u izjavi američkog Ministarstva pravosuđa, koja se nalazi u Prilogu VII. ovoj Odluci, opisana su ograničenja i zaštitne mjere koji se primjenjuju na pristup javnih tijela podacima i na njihovu upotrebu tih podataka u svrhu kaznenog progona i u druge svrhe od javnog interesa. Kako bi se povećala transparentnost i pokazala pravna priroda tih obveza, svi dokumenti popisani i priloženi ovoj Odluci objavljuju se u saveznom registru SAD-a.

(66) Zaključci Komisije o ograničenjima pristupa američkih javnih tijela osobnim podacima prenesenima iz Europske unije u Sjedinjene Američke Države i o upotrebi tih podataka te o postojanju učinkovite pravne zaštite dodatno su razrađeni u nastavku.

3.1. *Pristup američkih javnih tijela podacima i njihova upotreba za potrebe nacionalne sigurnosti*

(67) Komisija je analizom utvrdila da u američkom pravu postoji niz ograničenja pristupa osobnim podacima prenesenima u okviru europsko-američkog sustava zaštite privatnosti i upotrebe tih podataka te mehanizmi nadzora i pravne zaštite kojima se osigurava dovoljna zaštita tih podataka od nezakonitih radnji i rizika od zloupotrebe ([57]). Od 2013., kad je Komisija objavila svoje dvije Komunikacije (vidjeti uvodnu izjavu 7.), ovaj pravni okvir znatno je pojačan, kako je opisano u nastavku.

3.1.1. Ograničenja

(68) U skladu s američkim Ustavom za osiguranje nacionalne sigurnosti nadležan je Predsjednik kao glavni zapovjednik i glavni predstavnik izvršne vlasti, kao i za američke vanjske poslove u pogledu stranih obavještajnih podataka ([58]). Iako Kongres ima ovlasti određivati ograničenja i to je u mnogo pogleda i činio, unutar tih granica Predsjednik može usmjeravati rad američke obavještajne zajednice, posebno izvršnim nalozima ili predsjedničkim ukazima. To se dakako primjenjuje i u područjima u kojima Kongres ne daje smjernice. Trenutačno su dva najvažnija pravna instrumenta u tom pogledu Izvršni nalog br. 12333 (*Executive Order 12333*) ([59]) i Predsjednički ukaz br. 28. (*Presidential Policy Directive 28*.)

([56]) Direktor nacionalne obavještajne službe (DNI) voditelj je obavještajne zajednice i glavni savjetnik Predsjednika i Vijeća za nacionalnu sigurnost. Vidjeti Zakon o reformi obavještajnog sustava i sprečavanju terorizma (*Intelligence Reform and Terrorism Prevention Act*), 2004., Pub. L. 108-458 od 17. prosinca 2004. ODNI među ostalim utvrđuje zahtjeve za zadaće, prikupljanje, analizu, davanje na uvid i širenje nacionalnih obavještajnih podataka u obavještajnoj zajednici, upravlja njima i usmjerava ih, među ostalim razvojem smjernica o načinu pristupa informacijama i obavještajnim podacima te o njihovoj upotrebi i razmjeni. Vidjeti odjeljak 1.3. točke (a) i (b) Izvršnog naloga br. 12333.

([57]) Vidjeti *Schrems*, točka 91.

([58]) Ustav SAD-a, članak II. Vidjeti i uvod u PPD-28.

([59]) Izvršni nalog br. 12333: Obavještajne aktivnosti Sjedinjenih Država (*United States Intelligence Activities*), Savezni registar, svezak 40., br. 235 (8. prosinca 1981.). U mjeri u kojoj je Izvršni nalog javno dostupan njime se određuju ciljevi, usmjerenje, dužnosti i odgovornosti u pogledu američkih obavještajnih aktivnosti (uključujući ulogu različitih subjekata obavještajne zajednice) i utvrđuju se opći parametri za obavljanje obavještajnih aktivnosti (posebno potreba za proglašenjem posebnih postupovnih pravila). U skladu s odjeljkom 3.2. Izvršnog naloga br. 12333. Predsjednik, uz potporu Vijeća za nacionalnu sigurnost, i DNI, donose odgovarajuće upute, postupke i smjernice koji su potrebni za provođenje naloga.

(69) Predsjedničkim ukazom br. 28 (dalje u tekstu: PPD-28), koji je objavljen 17. siječnja 2014., određuje se niz ograničenja za operacije „prikupljanja informacija elektroničkim izviđanjem” ([60]). Taj predsjednički ukaz obvezujuć je za američka obavještajna tijela ([61]) i ostaje na snazi i nakon promjene vlade SAD-a ([62]). PPD-28 od posebne je važnosti za osobe koje nisu državljani SAD-a, među ostalim za osobe iz EU-a čiji se podaci obrađuju. U njemu je, među ostalim, predviđeno sljedeće:

(a) prikupljanje informacija elektroničkim izviđanjem mora se temeljiti na zakonu ili predsjedničkom odobrenju i mora se provoditi u skladu s američkim Ustavom (posebno Četvrtim amandmanom) i američkim pravom;

(b) prema svim osobama trebalo bi postupati s dostojanstvom i poštovanjem, neovisno o njihovom državljanstvu ili mjestu prebivališta;

(c) sve osobe imaju legitimne interese u pogledu zaštite privatnosti pri postupanju s njihovim osobnim podacima;

(d) privatnost i građanske slobode ključni su elementi u planiranju američkih aktivnosti prikupljanja informacija elektroničkim izviđanjem;

(e) američke obavještajne aktivnosti prikupljanja informacija elektroničkim izviđanjem stoga moraju uključivati odgovarajuće mjere zaštite osobnih podataka svih osoba, neovisno o njihovu državljanstvu ili mjestu prebivališta.

(70) PPD-28 propisuje da se obavještajni podaci mogu prikupljati elektroničkim izviđanjem samo u obavještajne ili protuobavještajne svrhe za podupiranje nacionalnih misija ili misija ministarstava i ni u koju drugu svrhu (npr. za osiguravanje konkurentne prednosti američkim poduzećima). U tom pogledu ODNI objašnjava da bi subjekti obavještajne zajednice „trebali tražiti da, kad god je to izvedivo, prikupljanje bude usmjereno na određene ciljeve ili teme u pogledu stranih obavještajnih podataka upotrebom razlikovnih čimbenika (npr. konkretnih komunikacijskih sredstava, čimbenika za odabir i identifikatora.)” ([63]). Nadalje, u izjavama se navode jamstva da se odluke o prikupljanju obavještajnih podataka ne prepuštaju pojedinim agentima već da se na takve odluke primjenjuju politike i postupci koje su različiti subjekti američke obavještajne zajednice (agencije) dužni uspostaviti za provedbu PPD-28 ([64]). U skladu s tim, istraživanje i utvrđivanje odgovarajućih čimbenika za odabir odvija se unutar općeg „Okvira prioriteta nacionalne obavještajne službe” (*National Intelligence Priorities Framework*, NIPF), kojim se osigurava da obavještajne prioritete utvrđuju tvorci politika na visokoj razini i da se oni redovito preispituju kako bi mogli odgovarati na stvarne prijetnje nacionalnoj sigurnosti i uzimajući u obzir moguće rizike, uključujući rizike za privatnost ([65]). Na osnovi toga zaposlenici agencije istražuju i utvrđuju posebne čimbenike za odabir za koje se očekuje da će pridonijeti prikupljanju obavještajnih podataka koji odgovaraju prioritetima ([66]). Čimbenici za odabir redovito se preispituju radi provjere mogu li se njima još uvijek osigurati vrijedni obavještajni podaci u skladu s prioritetima ([67]).

([60]) Prema Izvršnom nalogu br. 12333 direktor Nacionalne sigurnosne agencije (NSA) funkcionalni je upravitelj prikupljanja informacija elektroničkim izviđanjem i djeluje kao jedinstvena organizacija za taj tip aktivnosti.

([61]) Za definiciju pojma „obavještajna zajednica” vidjeti odjeljak 3.5. (h) Izvršnog naloga br. 12333 i PPD-28., b. 1.

([62]) Vidjeti Memorandum Ureda pravnog savjetnika pri Ministarstvu pravosuđa predsjedniku Clintonu, 29. siječnja 2000. Prema tom pravnom mišljenju predsjednički ukazi imaju „jednakovrijedni materijalni pravni učinak kao i izvršni nalog”.

([63]) Vidjeti izjave ODNI-ja (Prilog VI.), str. 3.

([64]) Vidjeti PPD-28, odjeljak 4. točke (b) i (c). Prema javno dostupnim informacijama preispitivanjem iz 2015. potvrđeno je šest postojećih svrha. Vidjeti ODNI, Reforma prikupljanja informacija elektroničkim izviđanjem (*Signals Intelligence Reform*), Izvješće o napretku, 2016.

([65]) Izjave ODNI-ja (Prilog VI.), str. 6. (s uputom na Ukaz o obavještajnoj zajednici br. 204.). Vidjeti i PPD-28, odjeljak 3.

([66]) Izjave ODNI-ja (Prilog VI.), str. 6. Vidjeti npr. Ured NSA-a za građanske slobode i privatnost (*NSA Civil Liberties and Privacy Office*, NSA CLPO), NSA-ova zaštita građanskih sloboda i privatnosti za ciljane aktivnosti SIGINT-a u skladu s Izvršnim nalogom br. 12333, 7. listopada 2014. Vidjeti i Izvješće o stanju ODNI-ja iz 2014. Na zahtjeve za pristup u skladu s odjeljkom 702. FISA-e primjenjuju se postupci ograničavanja prikupljanja na minimalnu nužnu količinu podataka koje je odobrio FISC. Vidjeti NSA CLPO, NSA-ova provedba odjeljka 702. Zakona o nadzoru stranih obavještajnih službi, 16. travnja 2014.

([67]) Vidjeti Reforma prikupljanja informacija elektroničkim izviđanjem, Izvješće povodom godišnjice, 2015. Vidjeti i Izjave ODNI-ja (Prilog VI.), str. 6., 8.–9., 11.

(71) Nadalje, zahtjevi utvrđeni u PPD-28, da prikupljanje obavještajnih podataka uvijek ([68]) mora biti „što usmjerenije" i da obavještajna zajednica daje prednost dostupnosti drugih informacija te odgovarajućim i izvedivim alternativnim izvorima ([69]), odražavaju opće pravilo davanja prednosti ciljanom prikupljanju pred skupnim. U skladu s jamstvima ODNI-ja, njima se posebno osigurava da skupno prikupljanje ne bude „masovno" ni „neselektivno" i da iznimka ne postane pravilo ([70]).

(72) Iako je u PPD-28 objašnjeno da subjekti obavještajne zajednice ponekad moraju skupno prikupljati obavještajne informacije, na primjer radi utvrđivanja i procjene nove prijetnje ili prijetnje u nastanku, u skladu s njim ti subjekti moraju dati prednost drugim mogućnostima koje će omogućiti ciljano prikupljanje informacija elektroničkim izviđanjem ([71]). Prema tome, skupno prikupljanje provodit će se samo kad ciljano prikupljanje upotrebom razlikovnih čimbenika, odn. identifikatora povezanih s konkretnom ciljanom osobom (kao što je adresa elektroničke pošte ili broj telefona), nije moguće „zbog tehničkih ili operativnih razloga" ([72]). To se primjenjuje na način prikupljanja informacija elektroničkim izviđanjem i na ono što se prikuplja ([72]).

(73) Prema izjavama ODNI-ja čak i ako se obavještajna zajednica ne može koristiti posebnim identifikatorima za ciljano prikupljanje, nastojat će ograničiti prikupljanje „što je više moguće". Kako bi se to osiguralo, ona „primjenjuje filtre i druge tehničke alate za usmjeravanje prikupljanja na ona komunikacijska sredstva koja vjerojatno sadržavaju komunikaciju povezanu sa stranim obavještajnim aktivnostima" (te prema tome uzima u obzir zahtjeve američkih tvoraca politika u skladu s postupkom opisanim u uvodnoj izjavi 70.). Stoga će se skupno prikupljanje usmjeravati na najmanje dva načina. Prvo, uvijek će se odnositi na konkretne ciljeve u pogledu stranih obavještajnih podataka (npr. na prikupljanje informacija elektroničkim izviđanjem o aktivnostima terorističke skupine koja djeluje u određenoj regiji) te će prikupljanje biti usmjereno na komunikaciju povezanu s tim. U skladu s jamstvima ODNI-ja to se odražava u činjenici da se „američke obavještajne aktivnosti prikupljanja informacija elektroničkim izviđanjem odnose samo na mali dio komunikacije koja se odvija na internetu" ([73]). Drugo, u izjavama ODNI-ja objašnjava se da će filtri i drugi tehnički alati biti oblikovani tako da „što preciznije" usmjere prikupljanje kako bi se osiguralo da se količina „nerelevantnih informacija" svede na minimum.

(74) Naposljetku, čak i ako Sjedinjene Američke Države smatraju da je skupno prikupljanje obavještajnih informacija elektroničkim izviđanjem nužno, u skladu s uvjetima iz uvodnih izjava od 70. do 73., PPD-28 ograničava upotrebu takvih podataka na posebni popis šest svrha nacionalne sigurnosti u cilju zaštite privatnosti i građanskih sloboda svih osoba, bez obzira na njihovo državljanstvo i mjesto prebivališta ([74]). Te dopustive svrhe obuhvaćaju mjere za otkrivanje i suzbijanje prijetnji koje proizlaze iz špijunaže, terorizma, oružja za masovno

([68]) Vidjeti bilješku 63.

([69]) Treba također napomenuti da, u skladu s odjeljkom 2.4. Izvršnog naloga br. 12333, subjekti obavještajne zajednice „upotrebljavaju tehnike prikupljanja podataka u Sjedinjenim Američkim Državama kojima se najmanje zadire u privatnost." U pogledu ograničenja za zamjenu svakog skupnog prikupljanja ciljanim vidjeti rezultate procjene Nacionalnog vijeća za istraživanja prema izvješću Agencije Europske unije za temeljna prava, Nadzor obavještajnih službi: temeljna prava, zaštitne mjere i pravna sredstva u EU-u (2015.) (*Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU (2015)*), str. 18.

([70]) Izjave ODNI-ja (Prilog VI.), str. 4.

([71]) Vidjeti i PPD-28, odjeljak 5. točku (d), kojim se propisuje da direktor Nacionalne obavještajne službe, u dogovoru s čelnicima relevantnih subjekata obavještajne zajednice i Uredom za politiku znanosti i tehnologije, Predsjedniku mora dostaviti „izvješće s procjenom izvedivosti izrade računalnog programa kojim bi se obavještajnoj zajednici omogućilo lakše pribavljanje informacija ciljanim nego skupnim prikupljanjem." Prema objavljenim informacijama zaključak izvješća bio je da „ne postoji programska alternativa kojom će se osigurati potpuna zamjena za skupno prikupljanje u slučaju otkrivene prijetnje nacionalnoj sigurnosti". Vidjeti Reformu prikupljanja informacija elektroničkim izviđanjem, Izvješće povodom godišnjice, 2015.

([72]) Vidjeti bilješku 68.

([73]) Izjave ODNI-ja (Prilog VI.). To je reakcija posebno na zabrinutost koju su nacionalna tijela za zaštitu podataka izrazila u svojem mišljenju o nacrtu odluke o primjerenosti. Vidjeti Radna skupina za zaštitu podataka prema članku 29., Mišljenje 01/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti (doneseno 13. travnja 2016.), str. 38. s b. 47.

([74]) Vidjeti PPD-28 odjeljak 2.

uništenje, prijetnji kibersigurnosti, oružanim snagama ili vojnom osoblju i transnacionalnih kriminalnih prijetnji povezanih s ostalih pet svrha te će se preispitivati najmanje svakih godinu dana. U skladu s izjavama američke vlade subjekti obavještajne zajednice pojačali su svoju analitičku praksu i standarde istrage neocijenjenih obavještajnih podataka prikupljenih elektroničkim izviđanjem kako bi se uskladili s tim zahtjevima; ciljanim istragama „osigurava se da se analitičarima na ispitivanje dostavljaju samo podaci za koje se vjeruje da imaju obavještajnu vrijednost" ([75]).

(75) Navedena su ograničenja posebno važna u pogledu osobnih podataka koji se prenose u okviru europsko-američkog sustava zaštite privatnosti, posebno ako se prikupljanje osobnih podataka odvija izvan SAD-a, uključujući tijekom njihova prijenosa transatlantskim kablovima iz Unije u SAD. Kako su potvrdila američka tijela u izjavama ODNI-ja, na takav se prijenos primjenjuju ograničenja i zaštitne mjere koje su tamo navedene, uključujući one iz Predsjedničkog ukaza br. 28 ([76]).

(76) Iako nisu oblikovana u takvom pravnom obliku, tim je načelima obuhvaćena bit načela nužnosti i proporcionalnosti. Velika prednost daje se ciljanom prikupljanju, a skupno prikupljanje ograničeno je na (iznimne) situacije u kojima ciljano prikupljanje nije moguće iz tehničkih ili operativnih razloga. Čak i ako se *skupno prikupljanje* ne može izbjeći, čini se da je daljnja „upotreba" takvih podataka pristupom *strogo ograničena* na posebne, legitimne potrebe nacionalne sigurnosti ([77]).

(77) Budući da je riječ o ukazu Predsjednika kao glavnog predstavnika izvršne vlasti, tim se zahtjevima obvezuje cijela obavještajna zajednica te se oni dalje provode s pomoću pravila agencije i postupaka kojima se opća načela prenose u posebne upute za svakodnevni rad. Nadalje, iako PPD-28 ne obvezuje sam Kongres, i on je poduzeo korake kako bi osigurao da prikupljanje osobnih podataka i pristup tim podacima u SAD-u budu ciljani, a ne „opći".

(78) Na temelju dostupnih informacija, uključujući izjave američke vlade, može se zaključiti da američke obavještajne službe mogu tražiti osobne podatke nakon što su ti podaci preneseni organizacijama u SAD-u koje su se samocertificirale u skladu s europsko-američkim sustavom zaštite privatnosti samo ([78]) ako je njihov zahtjev u skladu sa Zakonom o nadzoru stranih obavještajnih službi (*Foreign Intelligence Surveillance Act*, FISA) ili ako ih je zatražio Savezni istražni ured (FBI) na temelju takozvanog dopisa o nacionalnoj sigurnosti (*National Security Letter*, NSL) ([79]). Postoji nekoliko pravnih osnova u skladu s FISA-om koje se mogu upotrijebiti za prikupljanje (i potom za obradu) osobnih podataka osoba iz EU-a prenesenih u okviru europsko-američkog sustava zaštite podataka.

([75]) Vidjeti izjave ODNI-ja (Prilog VI.), str. 4. Vidjeti i Ukaz o obavještajnoj zajednici br. 203.

([76]) Izjave ODNI-ja (Prilog VI.), str. 2. Isto tako primjenjuju se i ograničenja iz Izvršnog naloga br. 12333 (npr. potreba da prikupljeni podaci odgovaraju obavještajnim prioritetima koje je utvrdio Predsjednik).

([77]) Vidjeti *Schrems*, točka 93.

([78]) Nadalje, FBI može prikupljati podatke i na temelju odobrenja za kazneni progon (vidjeti odjeljak 3.2. ove Odluke).

([79]) Za daljnja objašnjenja o upotrebi NSL-a vidjeti izjave ODNI-ja (Prilog VI.), str. 13–14. s b. 38. Kako je tamo navedeno, FBI može upotrijebiti NSL-ove samo za traženje informacija bez sadržaja relevantnih za ovlaštenu istragu u području nacionalne sigurnosti radi zaštite od međunarodnog terorizma ili tajnih obavještajnih aktivnosti. U pogledu prijenosa podataka u okviru europsko-američkog sustava zaštite privatnosti čini se da je najrelevantnije pravno odobrenje Zakon o privatnosti u području elektroničke komunikacije (*Electronic Communications Privacy Act*) (18 U.S.C. članak 2709.), kojim je propisano da se u svakom zahtjevu za informacije o pretplatniku ili evidenciju transakcija upotrebljava „pojam kojim se posebno određuje osoba, subjekt, telefonski broj ili račun".

Osim tradicionalnog pojedinačnog elektroničkog nadzora u skladu s odjeljkom 104. FISA-e ([80]) i postavljanja uređaja za bilježenje ulaznih i izlaznih poziva u skladu s odjeljkom 402. FISA-e ([81]), dva su glavna instrumenta odjeljak 501. FISA-e (bivši odjeljak 215. američkog Zakona o borbi protiv terorizma (*U.S. PATRIOT ACT*)) i odjeljak 702. FISA-e ([82]).

(79) U tom pogledu Zakonom SAD-a o slobodi (*FREEDOM Act*), koji je donesen 2. lipnja 2015., zabranjuje se skupno prikupljanje evidencije na temelju odjeljka 402. FISA-e (ovlast za bilježenje ulaznih i izlaznih poziva), odjeljka 501. FISA-e (bivši odjeljak 215. američkog Zakona o borbi protiv terorizma) ([83]) i upotrebe NSL-a, a umjesto toga zahtijeva se upotreba posebnih „čimbenika za odabir" ([84]).

(80) Iako FISA sadržava dodatna zakonska odobrenja za obavljanje nacionalnih obavještajnih aktivnosti, uključujući prikupljanje informacija elektroničkim izviđanjem, Komisija je svojom procjenom utvrdila da, u pogledu prenošenja osobnih podataka u okviru europsko-američkog sustava zaštite privatnosti, ta ovlaštenja jednako ograničavaju utjecaj javnih tijela na ciljano prikupljanje i pristup.

(81) To je jasno za tradicionalan pojedinačni elektronički nadzor u skladu s odjeljkom 104. FISA-e ([85]). U pogledu odjeljka 702. FISA-e, koji služi kao osnova za dva važna obavještajna programa koje provode američke obavještajne agencije (PRISM, UPSTREAM), pretraživanja se provode na ciljani način upotrebom pojedinačnih čimbenika za odabir kojima se utvrđuju konkretna komunikacijska sredstva, kao što su adresa e-pošte ili telefonski broj ciljane osobe, ali ne ključne riječi ili čak imena ciljanih osoba ([86]). Prema tome, kako je

([80]) 50 U.S.C. članak 1804. Za to pravno ovlaštenje potrebna je „izjava o činjenicama i okolnostima na koje se podnositelj oslanja za opravdanje svog vjerovanja da je (A) objekt elektroničkog nadzora strana sila ili agent strane sile", a potonje može uključivati osobe izvan EU-a koje sudjeluju u međunarodnom terorizmu ili međunarodnom širenju oružja za masovno uništenje (uključujući pripremne radnje) (50 U.S.C. članak 1801. stavak (b) točka 1.). No ipak postoji samo teoretska veza s osobnim podacima koji se prenose u okviru europsko-američkog sustava zaštite privatnosti jer se izjavom o činjenicama mora opravdati vjerovanje da „svako mjesto ili komunikacijsko sredstvo na koje je usmjeren elektronički nadzor upotrebljava, ili će upotrebljavati, strana sila ili agent strane sile". U svakom slučaju, za upotrebu te ovlasti potrebno je podnijeti zahtjev FISC-u, koji će ocijeniti, među ostalim, postoji li na temelju podnesenih činjenica vjerojatnost da je doista tako.

([81]) 50 U.S.C. članak 1842. s člankom 1841. stavkom 2. i odjeljkom 3127. glave 18. Ta se ovlast ne odnosi na sadržaj komunikacije već joj je svrha informiranje o klijentu ili pretplatniku upotrebom usluge (poput imena, adrese, pretplatničkog broja, duljine/vrste primljene usluge, izvora/mehanizma plaćanja). Za to je potreban zahtjev za nalog FISC-a (ili američkog pomoćnog suca, *U.S. Magistrate Judge*) ili upotreba posebnog čimbenika za odabir u smislu članka 1841. stavka 4., odnosno čimbenika kojim se posebno određuje osoba, račun itd. i koji se u najvećoj razumno mogućoj mjeri upotrebljava za ograničavanje opsega traženih informacija.

([82]) Dok se odjeljkom 501. FISA-e (bivši odjeljak 215. američkog Zakona o borbi protiv terorizma) FBI ovlašćuje da zatraži sudski nalog u svrhu osiguravanja „opipljivih stvari" (posebno telefonskih metapodataka, ali i poslovne evidencije) u strane obavještajne svrhe, odjeljkom 702. FISA-e dopušta se subjektima obavještajne zajednice SAD-a da traže pristup informacijama, među ostalim sadržaju internetske komunikacije, unutar SAD-a, ali usmjeren na određene osobe izvan SAD-a koje nisu njegovi državljani.

([83]) Na temelju ove odredbe FBI može zatražiti „opipljive stvari" (npr. evidencije, spise, dokumente) dokazujući Sudu za nadzor stranih obavještajnih službi (*Foreign Intelligence Surveillance Court*, FISC) da postoje opravdani razlozi na temelju kojih se smatra da su relevantni za određenu istragu FBI-ja. Pri pretraživanju FBI mora upotrebljavati čimbenike za odabir koje je odobrio FISC za koje postoji „opravdana i utemeljena sumnja" da je taj čimbenik povezan s jednom ili više stranih sila ili njihovih agenata koji se bave međunarodnim terorizmom ili s aktivnostima pripreme terorističkih napada. Vidjeti PCLOB, *Sec. 215 Report*, str. 59.; NSA CLPO, *Transparency Report: The USA Freedom Act Business Records FISA Implementation* (Provedba poslovne evidencije u skladu s FISA-om na temelju američkog Zakona o slobodi), 15. siječnja 2016., str. 4.–6.

([84]) Izjave ODNI-ja (Prilog VI.), str. 13. (b. 38).

([85]) Vidjeti bilješku 81.

([86]) PCLOB, *Sec. 702 Report*, str. 32–33. s daljnjim upućivanjima. Prema svom uredu za zaštitu privatnosti NSA mora provjeriti postoji li veza između ciljane osobe i čimbenika za odabir, mora evidentirati strane obavještajne informacije za koje se očekuje da će se prikupiti, te informacije moraju preispitati i odobriti dva viša analitičara NSA-a, a cjelokupni postupak pratit će ODNI i Ministarstvo pravosuđa za potrebe naknadnih preispitivanja usklađenosti. Vidjeti NSA CLPO, *NSA's Implementation of Foreign Intelligence Act Section 702* (NSA-ova provedba odjeljka 702. Zakona o nadzoru stranih obavještajnih službi), 16. travnja 2014.

napomenuo Nadzorni odbor za zaštitu privatnosti i građanskih sloboda (*Privacy and Civil Liberties Oversight Board*, PCLOB), nadzor iz odjeljka 702. „u cijelosti se sastoji od usmjeravanja na određene osobe (koje nisu državljani SAD-a) za koje je donesena pojedinačna odluka" ([87]). Zbog klauzule o vremenskom ograničenju valjanosti odjeljak 702. FISA-e morat će se preispitati 2017., kad će Komisija morati ponovno procijeniti zaštitne mjere koje su dostupne osobama iz EU-a čiji se podaci obrađuju.

(82) Nadalje, američka vlada u svojim je izjavama dala Europskoj komisiji izričito jamstvo da američka obavještajna zajednica „nikoga neselektivno ne nadzire, uključujući obične europske građane" ([88]). U pogledu osobnih podatka prikupljenih u SAD-u, ta je izjava potkrijepljena empirijskim dokazima koji pokazuju da se *zahtjevi za pristup* na temelju NSL-a ili u skladu s FISA-om, pojedinačno i zajedno, odnose samo na relativno mali broj ciljanih osoba u usporedbi s ukupnim protokom podataka na internetu ([89]).

(83) Kad je riječ o *pristupu* prikupljenim podacima i *sigurnosti podataka*, u Predsjedničkom ukazu br. 28. propisano je da pristup „mora biti ograničen na ovlašteno osoblje koje mora znati informacije da bi moglo obavljati svoju dužnost" i da se osobni podaci „obrađuju i pohranjuju pod uvjetima koji osiguravaju odgovarajuću zaštitu i sprečavaju pristup neovlaštenim osobama u skladu s primjenjivim zaštitnim mjerama za osjetljive informacije". Zaposlenici obavještajnih službi prolaze odgovarajuću i primjerenu obuku u skladu s načelima iz PPD-28 ([90]).

(84) Naposljetku, u pogledu *pohrane* i daljnjeg *širenja* osobnih podataka osoba iz EU-a čiji se podaci obrađuju i koje su prikupila obavještajna tijela SAD-a, u PPD-28 navedeno je da se prema svim osobama (uključujući one koje nisu državljani SAD-a) treba postupati s dostojanstvom i poštovanjem, da sve osobe imaju legitimne interese u pogledu zaštite privatnosti pri postupanju s njihovim osobnim podacima i da subjekti obavještajne zajednice stoga moraju uspostaviti politike kojima će osigurati odgovarajuće zaštitne mjere za takve podatke „koje su u razumnoj mjeri oblikovane tako da se širenje i zadržavanje [podataka] svede na nužni minimum" ([91]).

([87]) PCLOB, *Sec. 702 Report*, str. 111. Vidjeti i izjave ODNI-ja (Prilog VI.), str. 9. (Prikupljanje u skladu s odjeljkom 702. [FISA-e] nije „masovno i neselektivno" već je strogo usmjereno na prikupljanje stranih obavještajnih podataka iz pojedinačno utvrđenih legitimnih izvora) i str. 13., b. 36. (uz upućivanje na Mišljenje FISC-a iz 2014.); NSA CLPO, NSA-ova provedba odjeljka 702. Zakona o nadzoru stranih obavještajnih službi, 16. travnja 2014. Čak i u slučaju programa UPSTREAM NSA može tražiti presretanje elektroničke komunikacije samo prema određenim zadanim čimbenicima za odabir, od njih ili o njima.

([88]) Izjave ODNI-ja (Prilog VI.), str. 18. Vidjeti i str. 6. prema kojoj primjenjivi postupci „upućuju na jasnu obvezu sprečavanja samovoljnog i neselektivnog prikupljanja informacija elektroničkim izviđanjem i provedbe načela razumnosti s najviših razina naše vlade".

([89]) Vidjeti Statističko izvješće o transparentnosti u vezi s upotrebom nacionalnih sigurnosnih tijela, 22. travnja 2015. Za opći protok podataka na internetu vidjeti npr. Agencija za temeljna prava (*Fundamental Rights Agency*), Nadzor obavještajnih službi: Mjere za zaštitu temeljnih prava i pravna sredstva u EU-u (2015.) (*Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015)*), na str. 15.–16. U pogledu programa UPSTREAM, u skladu s Mišljenjem FISC-a iz 2011. s kojeg je uklonjena oznaka tajnosti, više od 90 % elektroničke komunikacije prikupljene u skladu s odjeljkom 702. FISA-e potječe iz programa PRISM, a manje od 10 % iz programa UPSTREAM. Vidjeti FISC, Mišljenje, 2011. WL 10945618 (FISA Ct., 3. listopada 2011.), b. 21. (dostupno na: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Vidjeti odjeljak 4. stavak (a) točku ii. PPD-28. Vidjeti i ODNI, Zaštita osobnih informacija svih osoba: Izvješće o napretku u razvoju i provedbi postupaka u skladu s Predsjedničkim ukazom br. 28. (*Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*), srpanj 2014., str. 5. u skladu s kojim bi „subjekti obavještajne zajednice trebali pojačati postojeće analitičke prakse i standarde u skladu s kojima analitičari moraju nastojati strukturirati upite ili ostale izraze za pretraživanje i tehnike za utvrđivanje obavještajnih podataka koji su relevantni za opravdane obavještajne zadaće ili zadaće kaznenog progona; usmjeriti upite o osobama na kategorije obavještajnih podataka koje odgovaraju obavještajnim zahtjevima ili zahtjevima kaznenog progona; i svesti na minimum osobne podatke koji nisu relevantni za obavještajne zahtjeve ili zahtjeve kaznenog progona." Vidjeti npr. CIA, Obavještajne aktivnosti prikupljanja informacija elektroničkim izviđanjem (*Signals Intelligence Activities*), str. 5.; FBI, Predsjednički ukaz br. 28. Politike i postupci (*Policies and Procedures*), str. 3. Prema Izvješću o napretku reforme prikupljanja informacija elektroničkim izviđanjem iz 2016. subjekti obavještajne zajednice (uključujući FBI, CIA i NSA) poduzeli su korake za upoznavanje svojih zaposlenika sa zahtjevima iz PPD-28 izradom novih ili izmjenom postojećih politika obuke.

([91]) Prema izjavama ODNI-ja ta se ograničenja primjenjuju bez obzira na to jesu li informacije prikupljane skupno ili ciljano te neovisno o državljanstvu pojedinca.

(85) Američka vlada objasnila je da taj zahtjev razumnosti znači da subjekti obavještajne zajednice neće morati donijeti „sve teoretski moguće mjere", ali će morati „uspostaviti ravnotežu između svojih nastojanja da zaštite legitimne interese u pogledu zaštite privatnosti i građanskih sloboda i praktičnih potreba prikupljanja informacija elektroničkim izviđanjem" ([92]). U tom pogledu će se prema osobama koje nisu državljani SAD-a postupati jednako kao prema državljanima SAD-a na temelju postupaka koje je odobrio Glavni državni odvjetnik ([93]).

(86) U skladu s tim pravilima zadržavanje je općenito ograničeno na najviše pet godina, osim ako je zakonski posebno propisano ili ako je direktor Nacionalne obavještajne agencije nakon pažljive procjene pitanja privatnosti izričito odlučio, uzimajući u obzir stajališta službenika ODNI-ja za zaštitu građanskih sloboda te službenika agencija za zaštitu privatnosti i građanske slobode, da je trajno zadržavanje u interesu nacionalne sigurnosti ([94]). Širenje je ograničeno na slučajeve kad su informacije relevantne za svrhu prikupljanja i stoga odgovaraju zahtjevima ovlaštenog prikupljanja stranih obavještajnih podataka ili kaznenog progona ([95]).

(87) U skladu s jamstvima američke vlade osobni podaci ne smiju se širiti samo zato što predmetna osoba nije američki državljanin i „informacije prikupljene elektroničkim izviđanjem o uobičajenim aktivnostima stranca ne bi se smatrale stranim obavještajnim podacima koji bi se mogli širiti ili trajno zadržavati samo zbog te činjenice osim ako na neki drugi način odgovaraju ovlaštenom zahtjevu za strane obavještajne podatke" ([96]).

(88) Na temelju navedenoga Komisija zaključuje da u Sjedinjenim Američkim Državama postoje pravila za ograničavanje zadiranja u temeljna prava osoba čiji se podaci za potrebe nacionalne sigurnosti prenose iz Unije u Sjedinjene Američke Države u okviru europsko-američkog sustava zaštite privatnosti na ono što je nužno za postizanje predmetnog legitimnog cilja.

(89) Prema spomenutoj analizi pravo SAD-a osigurava da će se mjere nadzora koristiti samo za pribavljanje stranih obavještajnih informacija, što je legitiman politički cilj ([97]), i bit će maksimalno prilagođene svrsi. Konkretno,

([92]) Vidjeti izjave ODNI-ja (Prilog VI.).
([93]) Vidjeti odjeljak 4. točku (a) podtočku i. PPD-28 s odjeljkom 2.3. Izvršnog naloga br. 12333.
([94]) PPD-28., odjeljak 4. stavak (a) točka i. Izjave ODNI-ja (Prilog VI.), str. 7. Na primjer, za osobne podatke prikupljene u skladu s odjeljkom 702. FISA-e, NSA-ovim postupcima ograničavanja prikupljanja na najnužniju količinu podataka koje je odobrio FISC u pravilu se predviđa da se metapodaci i neprocijenjeni sadržaj za PRISM zadržavaju najdulje pet godina, dok se podaci u okviru programa UPSTREAM zadržavaju najdulje dvije godine. NSA poštuje ta ograničenja pohranjivanja upotrebom automatiziranog postupka kojim se prikupljeni podaci brišu na kraju predmetnog razdoblja zadržavanja. Vidjeti NSA odjeljak 702., Postupci ograničavanja prikupljanja na najnužniju količinu podataka u skladu s FISA-om, odjeljak 7. s odjeljkom 6. točkom (a) podtočkom 1.; NSA CLPO, NSA-ova provedba odjeljka 702. Zakona o nadzoru stranih obavještajnih službi, 16. travnja 2014. Slično tomu, zadržavanje u skladu s odjeljkom 501. FISA-e (bivši odjeljak 215. američkog Zakona o borbi protiv terorizma) ograničeno je na pet godina, osim ako osobni podaci čine dio primjereno odobrenog širenja stranih obavještajnih podataka ili ako Ministarstvo pravosuđa pisanim putem obavijesti NSA da postoji obveza čuvanja evidencije zbog tekućeg ili očekivanog sudskog postupka. Vidjeti NSA, CLPO, Izvješće o transparentnosti: Provedba poslovne evidencije u skladu s FISA-om na temelju američkog Zakona o slobodi, 15. siječnja 2016.
([95]) Posebno u slučaju odjeljka 501. FISA-e (bivši odjeljak 215. američkog Zakona o borbi protiv terorizma), širenje osobnih podataka moguće je samo u svrhu borbe protiv terorizma ili kao dokaz za kazneno djelo; u slučaju odjeljka 702. FISA-e samo ako postoji opravdana svrha u pogledu stranih obavještajnih aktivnosti ili kaznenog progona. Vidjeti NSA, CLPO, NSA-ova provedba odjeljka 702. Zakona o nadzoru stranih obavještajnih službi, 16. travnja 2014. Izvješće o transparentnosti: Provedba poslovne evidencije u skladu s FISA-om na temelju američkog Zakona o slobodi, 15. siječnja 2016. Vidjeti i NSA-ovu Zaštitu građanskih sloboda i privatnosti za ciljane aktivnosti SIGNIT-a u skladu s Izvršnim nalogom br. 12333, 7. listopada 2014.
([96]) Izjave ODNI-ja (Prilog VI.), str. 7. (s uputom na Ukaz o obavještajnoj zajednici (ICD) br. 203.).
([97]) Sud Europske unije pojasnio je da je nacionalna sigurnost legitiman politički cilj. Vidjeti *Schrems*, točka 88. Vidjeti i *Digital Rights Ireland i dr.*, točke 42. – 44. i 51., gdje je Sud EU-a smatrao da borba protiv teškog kriminala, posebno organiziranog kriminala i terorizma, može uvelike ovisiti o upotrebi modernih tehnika istraživanja. Nadalje, za razliku od kaznenih istraga koje se obično odnose na naknadno utvrđivanje odgovornosti i krivnje za prijašnje ponašanje, obavještajne aktivnosti često su usmjerene na sprečavanje prijetnji nacionalnoj sigurnosti prije nego što se one ostvare. Stoga takve istrage često moraju obuhvatiti širi krug mogućih sudionika („ciljanih osoba") i šire geografsko područje. Vidjeti Europski sud za ljudska prava, *Weber i Saravia protiv Njemačke*, odluka od 29. lipnja 2006., zahtjev br. 54934/00, točke 105. – 118. (o tzv. „strateškom praćenju").

skupno prikupljanje odobravat će se samo iznimno, ako nije moguće ciljano prikupljanje, i bit će popraćeno dodatnim zaštitnim mjerama radi što većeg smanjenja količine prikupljenih podataka i ograničenja naknadnog pristupa (koji će morati biti ciljan i dopušten samo za posebne svrhe).

(90) Prema procjeni Komisije to je u skladu sa standardom koji je utvrdio Sud EU-a u presudi u predmetu *Schrems*, prema kojemu zakonodavstvo koje zadire u temeljna prava zajamčena člancima 7. i 8. Povelje mora uvesti „minimum zaštitnih mjera" ([98]) te „nije ograničeno na ono što je nužno ako općenito dopušta pohranjivanje svih osobnih podataka svih osoba čiji su podaci preneseni iz Europske unije u Sjedinjene Američke Države bez ikakvog razlikovanja, ograničenja ili iznimke s obzirom na postavljeni cilj i bez utvrđenog objektivnog kriterija prema kojem bi se ograničio pristup javnih tijela podacima i njihova naknadna upotreba u svrhe koje su točno određene, strogo ograničene i mogu opravdati zadiranje kao posljedicu pristupa tim podacima i njihove upotrebe" ([99]). Neće biti ni neograničenog prikupljanja ni pohranjivanja podataka svih osoba bez ikakvih ograničenja, a ni neograničenog pristupa. Nadalje, izjave dostavljene Komisiji, uključujući jamstvo da se američke obavještajne aktivnosti prikupljanja informacija elektroničkim izviđanjem odnose samo na mali dio komunikacije koja se odvija na internetu, isključuju mogućnost „općeg" pristupa sadržaju elektroničke komunikacije ([100]).

3.1.2. Učinkovita pravna zaštita

(91) Komisija je ocijenila mehanizme nadzora koji postoje u SAD-u s obzirom na svako zadiranje američkih obavještajnih tijela u osobne podatke koji se prenose u SAD i oblike pravne zaštite koji su dostupni osobama iz EU-a čiji se podaci obrađuju.

Nadzor

(92) Obavještajna zajednica SAD-a podliježe raznim mehanizmima provjere i nadzora koje provode sve tri grane državne vlasti. Među njima su unutarnja i vanjska tijela izvršne vlasti, niz odbora Kongresa te sudski nadzor, posebno u odnosu na aktivnosti obuhvaćene Zakonom o nadzoru stranih obavještajnih službi.

(93) Prvo, obavještajne aktivnosti američkih tijela podliježu opsežnom nadzoru izvršne grane vlasti.

(94) U skladu s odjeljkom 4. točkom (a) podtočkom iv. Predsjedničkog ukaza br. 28. politike i postupci subjekata obavještajne zajednice „uključuju odgovarajuće mjere za olakšavanje nadzora nad provedbom zaštitnih mjera kojima se štite osobne informacije"; te mjere trebale bi uključivati povremene revizije ([101]).

([98]) *Schrems*, točka 91. s daljnjim upućivanjima.
([99]) *Schrems*, točka 93.
([100]) Usp. *Schrems*, točka 94.
([101]) ODNI, Zaštita osobnih informacija svih osoba: Izvješće o razvoju i provedbi postupaka u skladu s Predsjedničkim ukazom br. 28., str. 7. Vidjeti npr. CIA, Obavještajne aktivnosti prikupljanja informacija elektroničkim izviđanjem (*Signals Intelligence Activities*), str. 6. (Usklađenost); FBI, Predsjednički ukaz br. 28. Politike i postupci, odjeljak III. pododjeljak (A) točka 4., pododjeljak (B) točka 4. NSA, postupci iz odjeljka 4. PPD-28, 12. siječnja 2015., odjeljak 8.1. i odjeljak 8.6. točka (c).

(95) U tom je pogledu uspostavljeno više razina nadzora, među kojima su službenici za građanske slobode i privatnost, glavni inspektori, Ured direktora nacionalne obavještajne službe (ODNI) za građanske slobode i privatnost, Nadzorni odbor za zaštitu privatnosti i građanskih sloboda (PCLOB) i predsjednički Obavještajni nadzorni odbor (*President's Intelligence Oversight Board*). Te nadzorne funkcije podupire osoblje zaduženo za usklađenost u svim agencijama ([102]).

(96) Kako je objasnila vlada SAD-a ([103]), *službenici za građanske slobode i privatnost* koji imaju ovlasti nadzora postoje u različitim ministarstvima s obavještajnim odgovornostima i obavještajnim agencijama ([104]). Iako se konkretne ovlasti tih službenika mogu donekle razlikovati ovisno o zakonu kojim su propisane, one obično obuhvaćaju nadzor postupaka kojima se osigurava da predmetno ministarstvo/agencija na primjereni način štiti privatnost i građanske slobode te da je uspostavilo odgovarajuće postupke za rješavanje pritužbi osoba koje smatraju da im je ugrožena privatnost ili građanske slobode (a u nekim slučajevima, kao ODNI, mogu i sami imati ovlasti istražiti pritužbe ([105])). Čelnik ministarstva/agencije mora osigurati da službenik zaprimi sve informacije te da ima pristup svim materijalima koji su mu potrebni za izvršavanje njegovih dužnosti. Službenici za građanske slobode i privatnost povremeno izvješćuju Kongres i PCLOB, među ostalim o broju i prirodi pritužbi koje je zaprimilo ministarstvo/agencija, te im dostavljaju sažetak takvih pritužbi, provedenih preispitivanja i istraga te ih obavješćuju o učinku aktivnosti koje je službenik proveo ([106]). Prema procjeni nacionalnih tijela za zaštitu podataka unutarnji nadzor koji provode službenici za građanske slobode i privatnost može se smatrati „prilično pouzdanim", iako po njihovom mišljenju oni ne zadovoljavaju zahtijevanu razinu neovisnosti ([107]).

(97) Nadalje, svaki subjekt obavještajne zajednice ima vlastitog *glavnog inspektora* koji je, među ostalim, nadležan za nadzor stranih obavještajnih aktivnosti ([108]). Unutar ODNI-ja to je Ured glavnog inspektora koji ima sveobuhvatnu nadležnost nad cijelom obavještajnom zajednicom i ovlašten je za istrage pritužbi ili informacija povezanih s navodima o nezakonitom postupanju ili zloupotrebi ovlasti u vezi s ODNI-jem i/ili programima i aktivnostima obavještajne zajednice ([109]). Glavni inspektori zakonski su neovisne jedinice ([110]) nadležne za provođenje revizija i istraga povezanih s programima i operacijama koje u nacionalne obavještajne svrhe provodi predmetna agencija, uključujući zbog zloupotrebe ili kršenja zakona ([111]). Imaju pristup svoj evidenciji, izvješćima,

([102]) Na primjer, NSA u Upravi za usklađenost (*Directorate for Compliance*) zapošljava više od 300 osoba zaduženih za usklađenost. Vidjeti izjave ODNI-ja (Prilog VI.), str. 7.

([103]) Vidjeti mehanizam pravobranitelja (Prilog III.), odjeljak 6. točka (b) podtočke i. – iii.

([104]) Vidjeti 42 U.S.C. članak 2000.ee-1. To uključuje, na primjer, Ministarstvo vanjskih poslova, Ministarstvo pravosuđa (uključujući FBI), Ministarstvo domovinske sigurnosti, Ministarstvo obrane, NSA, CIA i ODNI.

([105]) Prema američkoj vladi, ako Ured ODNI-ja za građanske slobode i privatnost zaprimi pritužbu, koordinirat će djelovanje s drugim subjektima obavještajne zajednice u pogledu daljnjeg rješavanja pritužbe u obavještajnoj zajednici. Vidjeti mehanizam pravobranitelja (Prilog III.), odjeljak 6. točka (b) podtočka ii.

([106]) Vidjeti 42 U.S.C. članak 2000.ee-1. točka (f) podtočke 1. i 2.

([107]) Vidjeti Radna skupina za zaštitu podataka prema članku 29., Mišljenje 01/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti (doneseno 13. travnja 2016.), str. 41.

([108]) Izjave ODNI-ja (Prilog VI.), str. 7. Vidjeti na primjer NSA, postupci iz odjeljka 4. PPD-28, 12. siječnja 2015., odjeljak 8.1.; CIA, Obavještajne aktivnosti prikupljanja informacija elektroničkim izviđanjem (*Signals Intelligence Activities*), str. 7. (Odgovornosti).

([109]) Glavnog inspektora (čija je funkcija uspostavljena u listopadu 2010.) imenuje Predsjednik, potvrđuje Senat i može ga razriješiti samo Predsjednik, a ne DNI.

([110]) Ti glavni inspektori imaju siguran mandat i može ih razriješiti jedino Predsjednik, koji mora pisanim putem obavijestiti Kongres o razlozima za razrješenje. To ne znači nužno da im se uopće ne daju upute. U nekim slučajevima ministar može zabraniti glavnom inspektoru pokretanje, provođenje ili dovršenje revizije ili istrage ako se to smatra nužnim za zaštitu važnih interesa u pogledu nacionalne sigurnosti. Međutim, Kongres se mora obavijestiti o izvršavanju te ovlasti i na temelju toga može predmetnog direktora pozvati na odgovornost. Vidjeti, na primjer, Zakon o glavnom inspektoru iz 1978., članak 8. (glavni inspektor Ministarstva obrane); članak 8.E (glavni inspektor Ministarstva pravosuđa), članak 8.G točka (d) podtočka 2. slova (A) i (B) (glavni inspektor NSA-a); 50. U.S. C. članak 403.q točka (b) (glavni inspektor CIA-e); Zakon o odobrenju prikupljanja obavještajnih podataka za fiskalnu godinu 2010. (*Intelligence Authorization Act For Fiscal Year 2010*), odjeljak 405. točka (f) (glavni inspektor obavještajne zajednice). Prema procjeni nacionalnih tijela za zaštitu podataka glavni inspektori *vjerojatno će ispunjavati kriterij organizacijske neovisnosti kako su ga utvrdili Sud EU-a i Europski sud za ljudska prava, barem od trenutka kad se novi postupak imenovanja bude primjenjivao na sve*. Vidjeti Radna skupina za zaštitu podataka prema članku 29., Mišljenje 01/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti (doneseno 13. travnja 2016.), str. 40.

([111]) Vidjeti izjave ODNI-ja (Prilog VI.), str. 7. Vidjeti i Zakon o glavnom inspektoru iz 1978., kako je izmijenjen, Pub. L. 113-126 od 7. srpnja 2014.

revizijama, preispitivanjima, dokumentima, spisima, preporukama ili ostalim relevantnim materijalima, ako je potrebno na temelju sudskog naloga, i mogu uzimati iskaze ([112]). Iako glavni inspektori mogu izdavati samo neobvezujuće preporuke korektivnih mjera, njihova izvješća, među ostalim ona o daljnjim mjerama (ili nepostojanju takvih mjera) objavljuju se i šalju Kongresu, koji na osnovi toga može vršiti svoju nadzornu funkciju ([113]).

(98) Nadalje, *Nadzornom odboru za zaštitu privatnosti i građanskih sloboda* (PCLOB), neovisnoj agenciji ([114]) izvršne grane vlasti sastavljenoj od dvostranačkog, peteročlanog odbora ([115]) koji na fiksni šestogodišnji mandat imenuje Predsjednik uz odobrenje Senata, povjerena je nadležnost u području politika borbe protiv terorizma i njihove provedbe s ciljem zaštite privatnosti i građanskih sloboda. Za potrebe preispitivanja aktivnosti obavještajne zajednice taj odbor može pristupiti svim relevantnim evidencijama, izvješćima, revizijama, pregledima, dokumentima, spisima i preporukama agencije, uključujući klasificirane podatke, te obavljati razgovore i uzimati iskaze. Prima izvješća službenika za građanske slobode i privatnost nekoliko saveznih ministarstava/agencija ([116]), može im davati preporuke te redovito izvješćuje kongresne odbore i Predsjednika ([117]). PCLOB ima i zadaću u okviru svog mandata pripremiti izvješće o procjeni provedbe Predsjedničkog ukaza br. 28.

(99) Konačno, prethodno navedene mehanizme nadzora nadopunjuje *Obavještajni nadzorni odbor* (*Intelligence Oversight Board*) uspostavljen u okviru predsjedničkog savjetodavnog odbora za obavještajne aktivnosti (*President's Intelligence Advisory Board*), koji nadzire usklađenost obavještajnih tijela SAD-a s Ustavom i svim primjenjivim pravilima.

(100) U cilju olakšavanja nadzora subjekti obavještajne zajednice potiču se na oblikovanje informacijskih sustava koji će omogućiti praćenje, evidentiranje i preispitivanje upita ili drugih traženja osobnih informacija ([118]). Tijela za nadzor i usklađenost povremeno će provjeravati praksu subjekata obavještajne zajednice usmjerenu na zaštitu osobnih informacija prikupljenih elektroničkim izviđanjem i njihovu usklađenost s tim postupcima ([119]).

(101) Te nadzorne funkcije poduprte su opsežnim zahtjevima za izvješćivanje o neusklađenosti. Konkretno, agencija svojim postupcima mora osigurati da se, u slučaju znatnog problema s usklađenošću u vezi s osobnim informacijama bilo koje osobe, neovisno o državljanstvu, koje su prikupljene elektroničkim izviđanjem, o tom pitanju odmah obavijesti čelnik subjekta obavještajne zajednice, koji će potom obavijestiti direktora Nacionalne obavještajne agencije, a on će u skladu s PPD-28 utvrditi jesu li potrebne korektivne mjere ([120]). Nadalje, u skladu s Izvršnim nalogom br. 12333 svi subjekti obavještajne zajednice moraju izvješćivati Obavještajni nadzorni odbor o incidentima povezanima s neusklađenošću ([121]). Tim se mehanizmima osigurava da će se problem rješavati na

([112]) Vidjeti Zakon o glavnom inspektoru iz 1978., članak 6.
([113]) Vidjeti izjave ODNI-ja (Prilog VI.), str. 7. Vidjeti i Zakon o glavnom inspektoru iz 1978., članak 4. stavak 5. i članak 5. U skladu s odjeljkom 405. točkom (b) podtočkama 3. i 4. Zakona o odobrenju prikupljanja obavještajnih podataka za fiskalnu godinu 2010., Pub. L. 111-259 od 7. listopada 2010., glavni inspektor obavještajne zajednice obavješćuje DNI i Kongres o nužnosti i napretku korektivnih mjera.
([114]) Prema procjeni nacionalnih tijela za zaštitu podataka, PCLOB je dosad „dokazao svoje neovisne ovlasti". Vidjeti Radna skupina za zaštitu podataka prema članku 29., Mišljenje 01/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti (doneseno 13. travnja 2016.), str. 42.
([115]) Uz to PCLOB stalno zapošljava dvadesetak osoba. Vidjeti https://www.pclob.gov/about-us/staff.html.
([116]) Oni uključuju, u najmanju ruku, Ministarstvo pravosuđa, Ministarstvo obrane, Ministarstvo domovinske sigurnosti, direktora Nacionalne obavještajne agencije i Glavnu obavještajnu agenciju te sva druga ministarstva, agencije ili subjekte izvršne grane vlasti koje PCLOB smatra relevantnima.
([117]) Vidjeti 42 U.S.C. članak 2000.ee Vidjeti i mehanizam pravobranitelja (Prilog III.), odjeljak 6. točka (b) podtočka iv. Među ostalim, PCLOB je dužan izvijestiti kad agencija izvršne vlasti odbije njegov savjet.
([118]) ODNI, Zaštita osobnih informacija svih osoba: Izvješće o razvoju i provedbi postupaka u skladu s Predsjedničkim ukazom br. 28., str. 7–8.
([119]) *Ibid*. str. 8. Vidjeti i izjave ODNI-ja (Prilog VI.), str. 9.
([120]) ODNI, Zaštita osobnih informacija svih osoba: Izvješće o razvoju i provedbi postupaka u skladu s Predsjedničkim ukazom br. 28., str. 7. Vidjeti npr. NSA, postupci iz odjeljka 4. PPD-28, 12. siječnja 2015., odjeljci 7.3. i 8.7. točke (c) i (d); FBI, Predsjednički ukaz br. 28. Politike i postupci, odjeljak III. točka A podtočka 4. i točka B podtočka 4. CIA, Obavještajne aktivnosti prikupljanja informacija elektroničkim izviđanjem (*Signals Intelligence Activities*), str. 6. (Usklađenost) i str. 8. (Odgovornosti).
([121]) Vidjeti Izvršni nalog br. 12333, odjeljak 1.6. točka (c).

najvišoj razini obavještajne zajednice. Ako se problem odnosi na osobu koja nije američki državljanin, direktor Nacionalne obavještajne službe, u dogovoru s ministrom vanjskih poslova i čelnikom ministarstva ili agencije koja dostavlja obavijest, utvrđuje treba li poduzeti korake za obavješćivanje predmetne strane vlade, u skladu sa zaštitom izvora i metoda te američkog osoblja ([122]).

(102) Drugo, uz te mehanizme nadzora u izvršnoj grani vlasti američki Kongres, posebno *obavještajni i pravosudni odbori Zastupničkog doma i Senata* (*House and Senate Intelligence and Judiciary Committees*), zaduženi su za nadzor nad svim stranim obavještajnim aktivnostima u SAD-u, uključujući aktivnosti prikupljanja informacija elektroničkim izviđanjem. Prema Zakonu o nacionalnoj sigurnosti „Predsjednik osigurava potpuno i ažurno obavješćivanje kongresnih odbora za obavještajne aktivnosti o obavještajnim aktivnostima Sjedinjenih Američkih Država, uključujući o svim bitnim očekivanim obavještajnim aktivnostima u skladu s ovim pododjeljkom" ([123]). Nadalje, „Predsjednik osigurava žurno obavješćivanje kongresnih odbora za obavještajne aktivnosti o svim nezakonitim obavještajnim aktivnostima te o korektivnim mjerama koje su poduzete ili se planiraju u vezi s takvim nezakonitim aktivnostima" ([124]). Članovi tih odbora imaju pristup klasificiranim podacima te obavještajnim metodama i programima ([125]).

(103) Kasnijim zakonima proširili su se i razradili zahtjevi izvješćivanja u pogledu subjekata obavještajne zajednice, relevantnih glavnih inspektora i Glavnog državnog odvjetnika (*Attorney General*). Na primjer, u FISA-i je propisano da Glavni državni odvjetnik mora „u potpunosti obavijestiti" obavještajne i pravosudne odbore Senata i Zastupničkog doma o aktivnostima vlade u okviru određenih odjeljaka FISA-e ([126]). Njome se zahtijeva i od vlade da kongresnim odborima dostavi „preslike svih odluka, naloga ili mišljenja Suda za nadzor stranih obavještajnih službi ili Žalbenog suda za nadzor stranih obavještajnih službi koji uključuju znatno oblikovanje ili tumačenje" odredaba FISA-e. Konkretno, u pogledu nadzora iz odjeljka 702. FISA-e, nadzor se vrši u skladu sa zakonski propisanim izvješćima obavještajnim i pravosudnim odborima te čestim sastancima i saslušanjima. To uključuje polugodišnje izvješće Glavnog državnog odvjetnika o primjeni odjeljka 702. FISA-e popraćeno dokumentima koji posebno uključuju izvješća o usklađenosti koja dostavljaju Ministarstvo pravosuđa i ODNI i opis slučajeva neusklađenosti ([127]) te zasebnu polugodišnju procjenu Glavnog državnog odvjetnika i DNI-ja o usklađenosti s postupcima ciljanog prikupljanja i ograničavanja prikupljanja na nužni minimum, uključujući usklađenost s postupcima koji su osmišljeni kako bi se osiguralo da se podaci prikupljaju u opravdanu svrhu u pogledu stranih obavještajnih aktivnosti ([128]). Kongres dobiva izvješća i glavnih inspektora koji su ovlašteni ocijeniti usklađenost agencija s postupcima ciljanog prikupljanja i ograničavanja prikupljanja na nužni minimum te smjernicama Glavnog državnog odvjetnika.

(104) U skladu sa Zakonom SAD-a o slobodi iz 2015. američka vlada mora svake godine objaviti Kongresu (i javnosti) broj traženih i primljenih naloga i ukaza FISA-e te procjene broja američkih državljana i osoba koje nisu američki državljani, a koje su predmetom nadzora ([129]). Zakonom je propisano i dodatno izvješćivanje javnosti o broju

([122]) PPD-28, odjeljak 4. točka (a) podtočka iv.
([123]) Vidjeti odjeljak 501. točku (a) stavak 1. (50 U.S.C. članak 413. točka (a) podtočka 1.). Ta odredba sadržava opće zahtjeve u pogledu nadzora koji provodi Kongres u području nacionalne sigurnosti.
([124]) Vidjeti odjeljak 501. točku (b) (50 U.S.C. članak 413. točka (b)).
([125]) Usp. odjeljak 501. točku (d) (50 U.S.C. članak 413. točka (d)).
([126]) Vidjeti 50 U.S.C. članke 1808., 1846., 1862., 1871., 1881.f.
([127]) Vidjeti 50 U.S.C. članak 1881.f
([128]) Vidjeti 50 U.S.C. članak 1881.a točku 1. podtočku 1.
([129]) Vidjeti Zakon SAD-a o slobodi iz 2015., Pub. L. br. 114–23., odjeljak 602. točka (a). Nadalje, u skladu s odjeljkom 402. „direktor Nacionalne obavještajne službe, u dogovoru s Glavnim državnim odvjetnikom, provodi deklasifikacijsko preispitivanje svake odluke, naloga ili mišljenja Suda za nadzor stranih obavještajnih službi ili Žalbenog suda za nadzor stranih obavještajnih službi (kako je definiran u odjeljku 601. točki (e)) koji uključuju znatno oblikovanje ili tumačenje bilo koje zakonske odredbe, među ostalim novih ili znatnih oblikovanja ili tumačenja naziva ‚posebni čimbenik za odabir' te u skladu s tim preispitivanjem objavljuje, koliko god je to izvedivo, svaku takvu odluku, nalog ili mišljenje".

izdanih NSL-ova, i za američke državljane i one koji to nisu (istodobno omogućujući primateljima naloga i potvrda FISA-e te zahtjeva NSL-a da pod određenim uvjetima izdaju izvješća o transparentnosti) ([130]).

(105) Treće, obavještajnim aktivnostima američkih javnih tijela na osnovi FISA-e dopušteno je preispitivanje, a u nekim slučajevima i prethodno odobrenje mjera, koje provodi *Sud FISA-e* (FISC) ([131]), neovisni sud ([132]) čije se odluke mogu osporavati pred Žalbenim sudom za nadzor stranih obavještajnih službi (FISCR) ([133]) te u konačnici pred Vrhovnim sudom Sjedinjenih Američkih Država ([134]). U slučaju prethodnog odobrenja tijela koja podnose zahtjev (FBI, NSA, CIA itd.) morat će podnijeti nacrt zahtjeva odvjetnicima Odjela za nacionalnu sigurnost Ministarstva pravosuđa, koji će ga pregledati i prema potrebi zatražiti dodatne informacije ([135]). Zahtjev će po njegovom okončanju morati odobriti Glavni državni odvjetnik, zamjenik Glavnog državnog odvjetnika ili pomoćnik Glavnog državnog odvjetnika za nacionalnu sigurnost ([136]). Ministarstvo pravosuđa potom će podnijeti zahtjev FISC-u, koji će ga ocijeniti i donijeti privremenu odluku o daljnjem postupanju ([137]). Ako se održava saslušanje, FISC ima ovlasti uzimati iskaze, što može uključivati stručne savjete ([138]).

(106) FISC (i FISCR) imaju potporu stalnog odbora od pet osoba koje su stručne za pitanja nacionalne sigurnosti i građanskih sloboda ([139]). Sud iz te skupine imenuje pojedinca koji će služiti kao *amicus curiae* te pomagati pri razmatranju svakog zahtjeva za nalog ili preispitivanje koji, prema mišljenju suda, čini novo ili značajno tumačenje zakona, osim ako sud smatra da takvo imenovanje nije primjereno ([140]). Time se posebno osigurava da su pitanja zaštite privatnosti primjereno uključena u procjenu suda. Sud može imenovati i pojedinca ili organizaciju kao *amicus curiae* koji, među ostalim, pruža tehničke savjete kad god to smatra primjerenim ili na zahtjev dopušta pojedincu ili organizaciji da podnesu sažetak *amicus curiae* ([141]).

([130]) Zakon SAD-a o slobodi, odjeljak 602. točka (a), 603. točka (a).

([131]) Za određene vrste nadzora američki pomoćni sudac (*U.S. Magistrate Judge*) kojeg je javno imenovao predsjednik Vrhovnog suda Sjedinjenih Američkih Država može imati ovlasti saslušati zahtjeve i odobriti naloge.

([132]) FISC je sastavljen od jedanaest sudaca koje među okružnim sucima SAD-a imenuje predsjednik Vrhovnog suda SAD-a, a koje je prethodno imenovao Predsjednik i potvrdio Senat. Suci, koji imaju doživotni mandat i koje je moguće razriješiti samo iz valjanog razloga, imaju sedmogodišnji mandat u FISC-u. U skladu s FISA-om suci se imenuju iz najmanje sedam različitih sudačkih okruga SAD-a. Vidjeti odjeljak 103. FISA-e (50. U.S.C. članak 1803. stavak (a)); PCLOB, *Sec. 215 Report*, str. 174–187. Sucima pomažu iskusni sudski službenici koji su pravni stručnjaci suda i pripremaju pravnu analizu zahtjeva za prikupljanje podataka. Vidjeti PCLOB, *Sec. 215 Report*, str. 178.; Dopis časnog suca g. Reggiea B. Waltona, predsjedavajućeg suca, Sud SAD-a za nadzor stranih obavještajnih službi, časnom sucu g. Patricku J. Leahyju, predsjedniku Odbora za pravosuđe Senata SAD-a (29. srpnja 2013.) („Waltonov dopis"), str. 2.–3.

([133]) FISCR je sastavljen od tri suca s okružnih ili žalbenih sudova SAD-a koja je imenovao predsjednik Vrhovnog suda SAD-a i koji služe sedmogodišnji mandat. Vidjeti odjeljak 103. FISA-e (50 U.S.C. članak 1803. točka (b)).

([134]) Vidjeti 50 U.S.C. članak 1803. točka (b), članak 1861.a točka (f), članak 1881.a točka (h), članak 1881.a točka i. podtočka 4.

([135]) Na primjer, upotrebljavat će se i širiti dodatne činjenice o objektu nadzora, tehničke informacije o metodologiji nadzora ili jamstva o načinu pribavljanja informacija. Vidjeti PCLOB, *Sec. 215 Report*, str. 177.

([136]) 50 U.S.C., članak 1804. točka (a) i članak 1801. točka (g).

([137]) FISC može odobriti zahtjev, zatražiti dodatne informacije, utvrditi nužnost saslušanja ili upozoriti na moguće odbijanje zahtjeva. Na temelju te privremene odluke vlada izrađuje konačni zahtjev. To može uključivati znatne izmjene prvotnog zahtjeva na temelju prethodnih primjedbi suca. Iako FISC odobrava veliki postotak konačnih zahtjeva, znatan dio tih zahtjeva sadržava bitne izmjene prvotnog zahtjeva, npr. 24 % zahtjeva odobrenih za razdoblje od srpnja do rujna 2013. Vidjeti PCLOB, *Sec. 215 Report*, str. 179. Waltonov dopis, str. 3.

([138]) PCLOB, *Sec. 215 Report*, str. 179., b. 619.

([139]) Vidjeti 50 U.S.C. članak 1803. točka i. podtočka 1. i podtočka 3. slovo A. Tim novim zakonom provedene su preporuke PCLOB-a o uspostavi skupine stručnjaka za zaštitu privatnosti i građanske slobode koji mogu služiti kao *amicus curiae* kako bi sudu osigurali zakonske argumente za provedbu zaštite privatnosti i građanskih sloboda. Vidjeti PCLOB, *Sec. 215 Report*, str. 183.–187.

([140]) Vidjeti 50 U.S.C. članak 1803. točka i. podtočka 2. slovo A. Prema informacijama ODNI-ja takva su imenovanja već provedena. Vidjeti Reforma prikupljanja informacija elektroničkim izviđanjem, Izvješće o napretku, 2016.

([141]) Vidjeti 50 U.S.C. članak 1803. točka i. podtočka 2. slovo B.

(107) Nadzor FISC-a razlikuje se u pogledu dva zakonska odobrenja za nadzor u okviru FISA-e koji su najvažniji za prijenos podataka u okviru europsko-američkog sustava zaštite privatnosti.

(108) U skladu s odjeljkom 501. FISA-e ([142]), prema kojemu je dopušteno prikupljanje „svih opipljivih stvari (uključujući knjige, evidenciju, spise, dokumente i druge predmete)", zahtjev podnesen FISC-u mora sadržavati izjavu da postoje opravdani razlozi na temelju kojih se smatra da su opipljive stvari koje se traže relevantne za ovlaštenu istragu (osim za procjenu prijetnje) koja se provodi u cilju prikupljanja stranih obavještajnih informacija koje se ne odnose na američke državljane ili radi zaštite od međunarodnog terorizma ili tajnih obavještajnih aktivnosti. Zahtjev mora sadržavati popis postupaka ograničavanja prikupljanja na minimum koje je donio Glavni državni odvjetnik za zadržavanje i širenje prikupljenih obavještajnih informacija ([143]).

(109) S druge strane, u skladu s odjeljkom 702. FISA-e ([144]), FISC ne odobrava pojedinačne mjere nadzora, već odobrava programe nadzora (npr. PRISM, UPSTREAM) na temelju godišnjih certifikacija koje pripremaju Glavni državni odvjetnik i direktor Nacionalne obavještajne službe. Odjeljkom 702. FISA-e dopušteno je prikupljanje stranih obavještajnih podataka o osobama za koje se opravdano vjeruje da se nalaze izvan Sjedinjenih Američkih Država ([145]). Takvo ciljano prikupljanje provodi NSA u dva koraka: prvo, analitičari NSA-a identificirat će osobe u inozemstvu koje nisu državljani SAD-a i čijim nadzorom će se, na temelju procjene analitičara, prikupiti relevantni strani obavještajni podaci navedeni u certifikaciji. Drugo, kad se te izdvojene osobe identificiraju te se ciljano prikupljanje podataka o njima odobri opsežnim mehanizmom preispitivanja unutar NSA-a ([146]), „zadat" će se (odn. razviti i primijeniti) čimbenici za odabir kojima se utvrđuju komunikacijska sredstva (poput adresa e-pošte) kojima se koriste ciljane osobe ([147]). Kako je navedeno, certifikacije koje će odobriti FISC ne sadržavaju informacije o pojedinim osobama čiji će se podaci ciljano prikupljati već se u njima navode kategorije stranih obavještajnih informacija ([148]). Iako FISC ne procjenjuje – zbog opravdane sumnje ili na nekoj drugoj osnovi – jesu li osobe čiji se podaci prikupljaju radi pribavljanja stranih obavještajnih podataka ispravno odabrane, ([149]) on provodi kontrolu pod uvjetom da je „važna svrha prikupljanja pribaviti strane obavještajne informacije" ([150]). U skladu s odjeljkom 702. FISA-e NSA smije prikupljati komunikacijske podatke osoba izvan EU-a koje nisu američki državljani samo ako se opravdano vjeruje da se predmetno komunikacijsko sredstvo upotrebljava za dostavljanje stranih obavještajnih informacija (npr. povezanih s međunarodnim terorizmom, širenjem nuklearnog oružja ili neprijateljskim kibernetičkim aktivnostima). Zaključci u tom smislu podliježu sudskom preispitivanju ([151]). U certifikacijama moraju biti predviđeni postupci ciljanog prikupljanja i njegovog ograničavanja na minimum ([152]). Glavni državni odvjetnik i direktor Nacionalne obavještajne službe provjeravaju usklađenost,

([142]) 50 U.S.C. članak 1861.
([143]) 50 U.S.C. članak 1861. točka (b)
([144]) 50 U.S.C. članak 1881.
([145]) 50 U.S.C. članak 1881.a točka (a).
([146]) PCLOB, *Sec. 702 Report*, str. 46.
([147]) 50 U.S.C. članak 1881.a točka (h).
([148]) 50 U.S.C. članak 1881.a točka (g). Prema PCLOB-u te su se kategorije dosad uglavnom odnosile na međunarodni terorizam i teme poput nabavljanja oružja za masovno uništenje. Vidjeti PCLOB, *Sec. 702 Report*, str. 25.
([149]) PCLOB, *Sec. 702 Report*, str. 27.
([150]) 50 U.S.C. članak 1881.a.
([151]) „Sloboda i sigurnost u svijetu koji se mijenja", Izvješće i preporuke predsjedničke Skupine za preispitivanje obavještajnih i komunikacijskih tehnologija, 12. prosinca 2013., str. 152.
([152]) 50 U.S.C., članak 1881.a točka i.

a agencije su dužne o svim slučajevima neusklađenosti obavijestiti FISC ([153]) (kao i Kongres i predsjednički obavještajni nadzorni odbor), koji na osnovu toga može izmijeniti odobrenje ([154]).

(110) Nadalje, radi povećanja učinkovitosti FISC-ovog nadzora, američka vlada pristala je provesti preporuku PCLOB-a o dostavljanju FISC-u dokumentacije o odlukama o odabiru cilja iz odjeljka 702., uključujući nasumični uzorak radnih naloga, kako bi FISC mogao procijeniti kako se zahtjev u pogledu prikupljanja stranih obavještajnih informacija provodi u praksi ([155]). Istodobno je američka vlada prihvatila i poduzela mjere za reviziju NSA-ovih postupaka ciljanog prikupljanja kako bi mogla bolje evidentirati razloge za odluke o ciljanom prikupljanju povezane s prikupljanjem stranih obavještajnih informacija ([156]).

Pojedinačna pravna zaštita

(111) U američkom zakonu osobama iz EU-a čiji se podaci obrađuju dostupni su različiti oblici pravne zaštite ako ih zabrinjava obrađuju li (prikupljaju, procjenjuju itd.) američki subjekti obavještajne zajednice njihove podatke i, ako to čine, poštuju li ograničenja propisana u američkom zakonodavstvu. To se u osnovi odnosi na tri područja: zadiranje prema FISA-i; nezakonit, namjerni pristup državnih službenika osobnim podacima i pristup informacijama u skladu sa Zakonom o pravu na pristup informacijama (*Freedom of Information Act*, FOIA) ([157]).

(112) Prvo, u Zakonu o nadzoru stranih obavještajnih službi predviđen je niz mehanizama pravne zaštite koji su dostupni i osobama koje nisu američki državljani za osporavanje nezakonitog elektroničkog nadzora ([158]). To uključuje mogućnost pojedinaca da pokrenu građanski postupak za naknadu štete protiv Sjedinjenih Američkih Država ako su se informacije o njima nezakonito i samovoljno upotrebljavale ili otkrivale ([159]); da osobno tuže američke državne službenike (zbog prekoračenja ovlasti, „*under color of law*") tražeći novčanu odštetu ([160]) i da ospore zakonitost nadzora (i traže uklanjanje informacija) ako američka vlada planira upotrijebiti ili otkriti prikupljene informacije ili podatke dobivene elektroničkim nadzorom osobe u sudskim ili upravnim postupcima u SAD-u ([161]).

(113) Drugo, američka vlada obavijestila je Komisiju o nizu dodatnih sredstava koje osobe iz EU-a čiji se podaci obrađuju mogu upotrijebiti za traženje pravne zaštite od državnih službenika zbog nezakonitog pristupa

([153]) U pravilu 13. (b) Poslovnika FISC-a propisano je da vlada Sudu mora dostaviti pisanu obavijest čim otkrije da se ovlast ili odobrenje koje je Sud dodijelio provodilo na način koji nije u skladu s odobrenjem ili ovlaštenjem Suda, ili u skladu s primjenjivim pravom. U njemu je također propisano da vlada mora pisanim putem obavijestiti Sud o činjenicama i okolnostima koje su relevantne za takvu neusklađenost. Vlada će obično podnijeti završnu obavijest iz pravila 13. (a) kad budu poznate relevantne činjenice i uništeni neovlašteno prikupljeni podaci. Vidjeti Waltonov dopis, str. 10.

([154]) 50 U.S.C. članak 1881. točka 1. Vidjeti i PCLOB, *Sec. 702 Report*, str. 66–76.; NSA CLPO, NSA-ova provedba odjeljka 702. Zakona o nadzoru stranih obavještajnih službi, 16. travnja 2014. Prikupljanje osobnih podataka u obavještajne svrhe u skladu s odjeljkom 702. FISA-e podliježe unutarnjem i vanjskom nadzoru izvršne grane vlasti. Unutarnji nadzor uključuje, među ostalim, programe unutarnjeg usklađivanja za ocjenjivanje i nadzor usklađenosti s postupcima ciljanog prikupljanja i ograničavanja prikupljanja na nužni minimum; izvješćivanje ODNI-ja, Ministarstva pravosuđa, Kongresa i FISC-a o slučajevima unutarnje i vanjske neusklađenosti i godišnja preispitivanja koja se šalju tim tijelima. Kad je riječ o vanjskom nadzoru, on se uglavnom sastoji od preispitivanja odabira cilja i ograničavanja prikupljanja na nužni minimum koje provode ODNI, Ministarstvo pravosuđa i glavni inspektori, koji izvješćuju Kongres i FISC, među ostalim i o slučajevima neusklađenosti. O težim slučajevima neusklađenosti mora se odmah obavijestiti FISC, a ostali u tromjesečnom izvješću. Vidjeti PCLOB, *Sec. 702 Report*, str. 66.-77.

([155]) PCLOB, *Recommendations Assessment Report* (Izvješće o procjeni provedbe preporuka), 29. siječnja 2015., str. 20.

([156]) PCLOB, *Recommendations Assessment Report*, 29. siječnja 2015., str. 16.

([157]) Nadalje, u odjeljku 10. Zakona o postupanju s klasificiranim podacima (*Classified Information Procedures Act*) predviđeno je da u kaznenom postupku u kojem SAD mora utvrditi čini li određeni materijal klasificirane podatke (npr. zato što ga treba zaštiti od neovlaštenog otkrivanja radi nacionalne sigurnosti), SAD obavješćuje tuženika o dijelovima materijala na koji u razumnoj mjeri očekuje da će se osloniti za utvrđivanje elementa klasificiranih podataka u pogledu kaznenog djela.

([158]) Vidjeti i izjave ODNI-ja (Prilog VI.), str. 16.

([159]) 18 U.S.C. članak 2712.

([160]) 50 U.S.C. članak 1810.

([161]) 50 U.S.C. članak 1806.

osobnim podacima ili njihove upotrebe, uključujući u svrhu navodne nacionalne sigurnosti (tj. Zakon o računalnoj prijevari i zloupotrebi, *Computer Fraud and Abuse Act* ([162]); Zakon o zaštiti privatnosti u području elektroničke komunikacije, *Electronic Communications Privacy Act* ([163]) i Zakon o pravu na privatnost financijskih podataka, *Right to Financial Privacy Act* ([164])). Sve te pravne osnove odnose se na posebne podatke, ciljeve i/ili vrste pristupa (npr. daljinski pristup računala internetom) i dostupni su pod određenim uvjetima (npr. namjerno/samovoljno postupanje, postupanje izvan službene dužnosti, pretrpljena šteta) ([165]). Općenitija mogućnost pravne zaštite pruža se u okviru Zakona o upravnom postupku (5 U.S.C. članak 702.), prema kojem „svaka osoba koja je u pravnom smislu oštećena ili ugrožena djelovanjem agencije ili je takvo djelovanje negativno utjecala na nju", ima pravo zatražiti sudsko preispitivanje. To uključuje mogućnost da od suda zatraži da „proglasi nezakonitima i ukine mjere, nalaze i zaključke agencija za koje se smatra da su […] samovoljne, hirovite, zloupotreba diskrecije ili da na drugi način nisu u skladu sa zakonom" ([166]).

(114) Naposljetku, američka vlada spominje FOIA kao sredstvo kojim osobe koje nisu američki državljani mogu tražiti pristup postojećoj evidenciji savezne agencije, uključujući i onoj koja sadržava njihove osobne podatke ([167]). S obzirom na svoju usmjerenost FOIA pojedincima ne osigurava pravnu zaštitu od neovlaštene upotrebe njihovih osobnih podataka, ali bi im načelu mogla omogućiti pristup relevantnim podacima koje čuvaju nacionalne obavještajne agencije. Čini se da su mogućnosti ograničene i u tom pogledu jer agencije nisu dužne otkriti informacije obuhvaćene određenim nabrojenim iznimkama, uključujući pristup klasificiranim podacima iz područja nacionalne sigurnosti i informacijama o istragama u okviru kaznenog progona ([168]). Međutim, osobe koje pokreću upravne i sudske postupke mogu osporiti takve iznimke kojima se koriste nacionalne obavještajne agencije.

(115) Iako prema tome pojedinci, uključujući osobe iz EU-a čiji se podaci obrađuju, imaju na raspolaganju različite oblike pravne zaštite ako su bili predmetom nezakonitog (elektroničkog) nadzora za potrebe nacionalne sigurnosti, očito je i da nisu obuhvaćene barem neke pravne osnove koje američka obavještajna tijela (npr. Izvršni nalog br. 12333) mogu upotrijebiti. Nadalje, čak i ako osobe koje nisu američki državljani u načelu imaju na raspolaganju mogućnosti sudske zaštite, kao u slučaju nadzora u skladu s FISA-om, dostupne pravne osnove ograničene su ([169]) i tužbe koje podnose pojedinci (uključujući američke državljane) proglasit će se neprihvatljivima ako se ne može dokazati „osnovanost" ([170]), kojom se ograničava pristup redovnim sudovima ([171]).

(116) Kako bi osigurala dodatni oblik pravne zaštite dostupan svim osobama iz EU-a čiji se podaci obrađuju, američka vlada odlučila je uspostaviti novi mehanizam u vidu pravobranitelja, kako je navedeno u dopisu američkog ministra vanjskih poslova Komisiji, koji se nalazi u Prilogu III. ovoj Odluci. Taj se mehanizam temelji na imenovanju, u okviru Predsjedničkog ukaza br. 28., višeg koordinatora (na razini zamjenika ministra) u Ministarstvu vanjskih poslova kao kontaktne točke za strane vlade koji će postavljati pitanja u vezi s američkim obavještajnim aktivnostima prikupljanja informacija elektroničkim izviđanjem, ali on uvelike nadilazi taj prvobitni koncept.

([162]) 18 U.S.C. članak 1030.
([163]) 18 U.S.C. članci od 2701. do 2712.
([164]) 12 U.S.C. članak 3417.
([165]) Izjave ODNI-ja (Prilog VI.), str. 17.
([166]) 5 U.S.C. članak 706. stavak 2. točka A.
([167]) 5 U.S.C. članak 552. Slični zakoni postoje na razini saveznih država.
([168]) U tom slučaju osoba će u načelu zaprimiti samo uobičajeni odgovor kojim agencija odbija potvrditi ili poreći postojanje evidencije. Vidjeti *ACLU protiv CIA*, 710 F.3d 422 (D.C. Cir. 2014.).
([169]) Vidjeti izjave ODNI-ja (Prilog VI.), str. 16. Prema dostavljenim objašnjenjima dostupne pravne osnove zahtijevaju postojanje *štete* (18 U.S.C. članak 2712.; 50 U.S.C. članak 1810.) ili dokaz da *vlada planira upotrijebiti ili otkriti informacije* dobivene ili izvedene iz elektroničkog nadzora predmetne osobe protiv te osobe *u sudskim ili upravnim postupcima* u Sjedinjenim Američkim Državama (50 U.S.C. članak 1806.). Međutim, kako je Sud u više navrata naglasio, da bi se moglo utvrditi zadiranje u temeljno pravo na privatnost, nije važno je li predmetna osoba pretrpjela štetne posljedice tog zadiranja. Vidjeti *Schrems*, točka 89. s daljnjim upućivanjima.
([170]) Taj kriterij prihvatljivosti proizlazi iz zahtjeva „*case or controversy*" („predmet ili kontroverzija") američkog Ustava, članak III.
([171]) Vidjeti *Clapper protiv Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013.). U pogledu upotrebe NSL-a, u američkom Zakonu o slobodi (odjeljak 502. točka (f) – 503.) predviđeno je da se zahtjevi neotkrivanja moraju povremeno preispitivati i da *primatelji* NSL-a moraju biti obaviješteni kad činjenice više ne idu u prilog zahtjevu neotkrivanja (vidjeti Izjavu ODNI-ja (Prilog VI.), str. 13.). Međutim, time se ne osigurava da je osoba iz EU-a čiji se podaci obrađuju obaviještena da je predmetom istrage.

(117) U skladu s preuzetim obvezama američke vlade mehanizmom pravobranitelja osigurat će se da se pojedinačne pritužbe na odgovarajući način istraže i riješe i da pojedinci dobiju neovisnu potvrdu poštovanja američkih zakona ili, u slučaju kršenja takvih zakona, da se neusklađenost ispravi ([172]). Taj mehanizam uključuje „Pravobranitelja za sustav zaštite privatnosti", tj. zamjenika ministra i drugo osoblje te ostala nadzorna tijela nadležna za nadzor različitih subjekata obavještajne zajednice na čiju će se suradnju Pravobranitelj za sustav zaštite privatnosti oslanjati pri rješavanju pritužbi. Posebno kad se zahtjev pojedinca odnosi na usklađenost nadzora s pravom SAD-a, Pravobranitelj za sustav zaštite privatnosti moći će se osloniti na neovisna nadzorna tijela s istražnim ovlastima (kao što su glavni inspektori ili PCLOB). U svakom slučaju američki ministar vanjskih poslova (*Secretary of State*) osigurava da Pravobranitelj raspolaže sredstvima kojima može osigurati da se odgovori na pojedinačne zahtjeve temelje na svim potrebnim informacijama.

(118) Putem te „kompozitne strukture" mehanizam pravobranitelja jamči neovisni nadzor i pojedinačne oblike zaštite. Nadalje, suradnja s drugim nadzornim tijelima osigurava pristup nužnom stručnom znanju. Konačno, obvezivanjem Pravobranitelja za sustav zaštite privatnosti da potvrdi usklađenost ili ispravak svih neusklađenosti, taj mehanizam odražava nastojanje vlade SAD-a u cijelosti da reagira na pritužbe pojedinaca iz EU-a i riješi ih.

(119) Prvo, za razliku od običnog međuvladinog mehanizma Pravobranitelj za sustav zaštite privatnosti zaprimat će pojedinačne pritužbe i odgovarati na njih. Takve se pritužbe mogu uputiti nadzornim tijelima u državama članicama nadležnima za nadzor službi nacionalne sigurnosti i/ili obrade osobnih podataka koju provode javna tijela, koja će ih podnijeti centraliziranom tijelu EU-a odakle će se proslijediti Pravobranitelju za sustav zaštite privatnosti ([173]). To će koristiti osobama iz EU-a koje se mogu obratiti svom nacionalnom tijelu i na vlastitom jeziku. To će tijelo pomagati osobi s podnošenjem zahtjeva Pravobranitelju za sustav zaštite privatnosti u kojem će biti navedene osnovne informacije te će se moći smatrati „potpunim". Osoba ne mora dokazivati da je američka vlada stvarno pristupila njezinim podacima u okviru aktivnosti prikupljanja informacija elektroničkim izviđanjem.

(120) Drugo, vlada SAD-a obvezuje se osigurati da će se Pravobranitelj za sustav zaštite privatnosti u obavljanju svojih dužnosti moći osloniti na suradnju s drugim nadzornim mehanizmima i mehanizmima za preispitivanje usklađenosti koji postoje u pravu SAD-a. To će ponekad uključivati nacionalna obavještajna tijela, posebno kad se zahtjev treba tumačiti kao zahtjev za pristup dokumentima u skladu sa Zakonom o pravu na pristup informacijama. U drugim slučajevima, posebno kad se zahtjevi odnose na usklađenost nadzora s pravom SAD-a, takva će suradnja uključivati neovisna nadzorna tijela (npr. glavne inspektore), koja će biti nadležna i ovlaštena za temeljitu istragu (posebno kroz pristup svim relevantnim dokumentima i ovlast da zatraže informacije i izjave) te ispravljanje neusklađenosti ([174]). Nadalje, Pravobranitelj za sustav zaštite privatnosti moći će predmete uputiti PCLOB-u na razmatranje ([175]). Ako neko od tih nadzornih tijela utvrdi neusklađenost, predmetni subjekt obavještajne zajednice (npr. obavještajna agencija) morat će ispraviti neusklađenost jer će Pravobranitelj tek tada

([172]) Ako podnositelj pritužbe traži pristup dokumentima koje čuvaju javna tijela SAD-a, primjenjuju se pravila i postupci iz Zakona o pravu na pristup informacijama. To uključuje mogućnost traženja sudske zaštite (umjesto neovisnog nadzora) ako je zahtjev odbijen, pod uvjetima iz tog zakona.

([173]) U skladu s mehanizmom pravobranitelja (Prilog III.), odjeljak 4. točka (f), Pravobranitelj za sustav zaštite privatnosti izravno će komunicirati s tijelom EU-a za rješavanje pojedinačnih pritužbi, koje će biti nadležno za komunikaciju s osobom koja je podnijela zahtjev. Ako je izravna komunikacija dio „osnovnih postupaka" kojima se može osigurati traženo pravno sredstvo (npr. zahtjev za pristup na temelju FOIA-e, vidjeti odjeljak 5.), ta će se komunikacija odvijati u skladu s primjenjivim postupcima.

([174]) Vidjeti mehanizam pravobranitelja (Prilog III.), odjeljak 2. točka (a). Vidjeti uvodne izjave 0-0.

([175]) Vidjeti mehanizam pravobranitelja (Prilog III.), odjeljak 2. točka (c). Prema objašnjenjima američke vlade PCLOB stalno preispituje politike i postupke, kao i njihovu provedbu, američkih tijela nadležnih za borbu protiv terorizma kako bi mogao utvrditi da li njihove mjere „primjereno štite privatnost i građanske slobode i jesu li u skladu s primjenjivim zakonima, propisima i politikama u pogledu zaštite privatnosti i građanskih sloboda". Osim toga, PCLOB „prima i preispituje izvješća i druge informacije dobivene od službenika za zaštitu privatnosti i građanskih sloboda te im, prema potrebi, daje preporuke u vezi s njihovim aktivnostima."

moći dati „pozitivan" odgovor pojedincu (tj. da je svaka neusklađenost uklonjena) na koji se obvezala američka vlada. Osim toga, u okviru te suradnje Pravobranitelj za sustav zaštite privatnosti bit će obaviješten o ishodu istrage te će raspolagati sredstvima kojima će osigurati da dobije sve informacije potrebne za pripremu odgovora.

(121) Naposljetku, Pravobranitelj za sustav zaštite privatnosti bit će neovisan o američkoj obavještajnoj zajednici te prema tome neće od nje primati upute ([176]). To je vrlo važno jer će Pravobranitelj morati „potvrditi" da je i. pritužba pravilno istražena i da se ii. postupalo u skladu s američkim pravom, uključujući s ograničenjima i zaštitnim mjerama iz Priloga VI. ili da je, u slučaju neusklađenosti, takvo kršenje ispravljeno. Kako bi mogao pružiti takvu neovisnu potvrdu, Pravobranitelj za sustav zaštite privatnosti morat će primiti potrebne informacije o istrazi da bi procijenio točnost odgovora na pritužbu. Osim toga, američki ministar vanjskih poslova obvezao se osigurati da zamjenik ministra obnaša dužnost Pravobranitelja za sustav zaštite privatnosti objektivno i slobodno od mogućeg neprimjerenog utjecaja na odgovor koji treba pružiti.

(122) Općenito gledajući, tim se mehanizmom osigurava da će se pojedinačne pritužbe temeljito istražiti i riješiti te da će to barem u području nadzora uključivati neovisna nadzorna tijela s nužnom stručnosti i istražnim ovlastima te Pravobranitelja koji će moći obavljati svoje dužnosti bez neprimjerenog, posebno političkog utjecaja. Nadalje, pojedinci pri podnošenju pritužbi neće morati dokazivati ni navoditi indikacije o tome da su bili predmet nadzora ([177]). S obzirom na ta obilježja Komisija je zadovoljna što postoje primjerena i djelotvorna jamstva protiv zloupotrebe.

(123) Na temelju svega navedenog Komisija zaključuje da Sjedinjene Američke Države osiguravaju djelotvornu pravnu zaštitu od neovlaštenog zadiranja svojih obavještajnih tijela u temeljna prava osoba čiji se podaci prenose iz Unije u Sjedinjene Američke Države u okviru europsko-američkog sustava zaštite privatnosti.

(124) U tom smislu Komisija prima na znanje presudu Suda EU-a u predmetu *Schrems* prema kojoj se „zakonodavstvom u kojem nije predviđena mogućnost da pojedinac zatraži pravnu zaštitu kako bi dobio pristup osobnim podacima koji se na njega odnose ili pravo na ispravak ili brisanje takvih podataka ne poštuje bit temeljnog prava na djelotvornu sudsku zaštitu prema članku 47. Povelje" ([178]). Komisija je u svojoj procjeni potvrdila da su takve vrste pravne zaštite osigurane u SAD-u, uključujući uvođenjem mehanizma pravobranitelja. Mehanizam pravobranitelja osigurava neovisan nadzor s istražnim ovlastima. U okviru Komisijina stalnog praćenja sustava zaštite privatnosti, uključujući godišnjim zajedničkim preispitivanjem koje uključuje i Pravobranitelja, ponovno će se procjenjivati djelotvornosti tog mehanizma.

3.2. *Pristup američkih javnih tijela podacima i njihova upotreba za potrebe kaznenog progona i javnog interesa*

(125) Kad je riječ o neovlaštenoj upotrebi osobnih podataka koji se prenose u okviru europsko-američkog sustava zaštite privatnosti, američka vlada (posredstvom Ministarstva pravosuđa) dala je jamstva o primjenjivim ograničenjima i zaštitnim mjerama koje su se prema procjenama Komisije pokazale kao dostatna razina zaštite.

([176]) Vidjeti *Roman Zakharov protiv Rusije*, presuda od 4. prosinca 2015. (Veliko vijeće), zahtjev br. 47143/06, točka 275. („iako je u načelu poželjno povjeriti nadzornu kontrolu sucu, može se smatrati da je nadzor koji vrše nepravosudna tijela u skladu s Konvencijom, pod uvjetom da je nadzorno tijelo neovisno o tijelima koja provode nadzor te ima dovoljno djelotvornih nadzornih ovlasti").

([177]) Vidjeti *Kennedy protiv Ujedinjene Kraljevine*, presuda od 18. svibnja 2010., zahtjev 26839/05, točka 167.

([178]) *Schrems*, točka 95. Kako proizlazi iz točaka 91. i 96. presude, točka 95. odnosi se na razinu zaštite zajamčenu u pravnom poretku Unije, kojoj razina zaštite u trećoj zemlji mora biti „u osnovi jednakovrijedna". Prema točkama 73. i 74. presude to ne znači da razina zaštite ili sredstva kojima se služi treća zemlja mora biti jednaka iako se sredstva koja će se primijeniti u praksi moraju pokazati djelotvornima.

(126) Prema tim informacijama, u skladu s Četvrtim amandmanom američkog Ustava ([179]), tijela kaznenog progona u načelu ([180]) mogu vršiti pretrese i zapljene na temelju sudskog naloga koji su ishodila dokazavši da postoji „osnovana sumnja". U nekoliko posebno utvrđenih i iznimnih slučajeva kad se ne primjenjuje zahtjev za nalog ([181]) kazneni progon podliježe provjeri „razumnosti" ([182]). Razumnost pretresa ili zapljene „utvrđuje se procjenom, s jedne strane, mjere do koje se time ugrožava privatnost osobe i, s druge strane, mjere do koje je to potrebno za promicanje legitimnih državnih interesa" ([183]). Općenito, Četvrtim amandmanom jamči se privatnost, dostojanstvo i zaštita od samovoljnih radnji državnih službenika kojima se zadire u privatnost ([184]). Tim je pojmovima obuhvaćena ideja nužnosti i razmjernosti iz prava Unije. Nakon što za kazneni progon više nisu potrebni zaplijenjeni predmeti kao dokaz, moraju biti vraćeni ([185]).

(127) Iako se osobe koje nisu državljani i nemaju sjedište u SAD-u ne mogu pozvati na Četvrti amandman, one ostvaruju posrednu korist od zaštite koju on pruža jer su osobni podaci u posjedu američkih poduzeća i tijela kaznenog progona u svakom slučaju moraju tražiti sudsko odobrenje (ili barem poštovati zahtjev razumnosti) ([186]). Dodatna zaštita osigurava se posebnim zakonskim ovlastima i smjernicama Ministarstva pravosuđa kojima se ograničava pristup tijela kaznenog progona podacima na temelju osnova koje odgovaraju nužnosti i razmjernosti (npr. traženje od FBI-ja da se služi istražnim metodama kojima se najmanje zadire u privatnost, uzimajući u obzir učinak na privatnost i građanske slobode) ([187]). Prema izjavama američke vlade jednaka ili viša zaštita primjenjuje se na istrage tijela kaznenog progona na državnoj razini (u pogledu istraga koje se provode u skladu s državnim zakonima) ([188]).

(128) Iako prethodno sudsko odobrenje suda ili porote (istražnog ogranka suda koji sastavlja sudac ili pomoćni sudac) nije potrebno u svim predmetima ([189]), upravni sudski pozivi ograničeni su na posebne slučajeve i podliježu neovisnom sudskom preispitivanju barem u slučajevima kad vlada traži provedbu sudskim putem ([190]).

([179]) Prema Četvrtom amandmanu „ne smije se kršiti pravo osoba da se osjećaju sigurno te da su njihove kuće, dokumenti i imovina zaštićeni od nerazumnih pretresa i zapljena i nalozi se ne smiju izdavati osim ako postoji opravdana sumnja potkrijepljena zakletvom ili potvrdom te moraju sadržavati točan opis mjesta koje treba pretražiti, osoba koje treba uhititi ili stvari koje treba zaplijeniti." Samo (pomoćni) suci smiju izdavati naloge za pretres. Savezni nalozi za umnožavanje elektronički pohranjenih informacija dodatno su uređeni pravilom 41. saveznih propisa o kaznenom postupku.

([180]) Vrhovni sud je u više navrata pretrese bez naloga nazvao „iznimkom". Vidjeti *Johnson protiv Sjedinjenih Američkih Država*, 333 U.S. 10, 14 (1948.); *McDonald protiv Sjedinjenih Američkih Država*, 335 U.S. 451, 453 (1948.); *Camara protiv Municipal Court*, 387 U.S. 523, 528-29 (1967.); *G.M. Leasing Corp. protiv Sjedinjenih Američkih Država*, 429 U.S. 338, 352-53, 355 (1977.). Isto tako, Vrhovni sud redovito ističe da je osnovno ustavno pravilo u tom području da su pretresi izvan sudskog postupka, bez prethodnog odobrenja suca ili pomoćnog suca, *per se* nerazumni u skladu s Četvrtim amandmanom – uz svega nekoliko točno određenih i jasno ograničenih iznimaka. Vidjeti npr. *Coolidge protiv New Hampshire*, 403 U.S. 443, 454-55 (1971.); *G.M. Leasing Corp. protiv Sjedinjenih Američkih Država*, 429 U.S. 338, 352-53, 358 (1977.).

([181]) *Grad Ontario, Kalifornija protiv Quona*, 130 S. Ct. 2619, 2630 (2010.).

([182]) PCLOB, *Sec. 215 Report*, str. 107., u kojem se upućuje na predmet *Maryland protiv Kinga*, 133 S. Ct. 1958, 1970 (2013.).

([183]) PCLOB, *Sec. 215 Report*, str. 107., u kojem se upućuje na predmet *Samson protiv Kalifornije*, 547 S. Ct. 843, 848 (2006.).

([184]) *Grad Ontario, Kalifornija protiv Quona*, 130 S. Ct. 2619, 2630 (2010.), 2627.

([185]) Vidjeti npr. *Sjedinjene Američke Države protiv Wilsona*, 540 F.2d 1100 (D.C. Cir. 1976.).

([186]) Usp. *Roman Zakharov protiv Rusije*, presuda od 4. prosinca 2015. (Veliko vijeće), zahtjev br. 47143/06, točka 269., prema kojoj „zahtjev da se pružatelju komunikacijskih usluga pokaže odobrenje za presretanje prije dobivanja pristupa komunikaciji osobe jedna je od važnijih zaštitnih mjera protiv zloupotrebe od strane tijela kaznenog progona, čime se osigurava da se svi slučajevi presretanja odvijaju uz pravilna odobrenja."

([187]) Izjave Ministarstva pravosuđa (Prilog VII.), str. 4. s daljnjim upućivanjima.

([188]) Izjave Ministarstva pravosuđa (Prilog VII.), b. 2.

([189]) Prema informacijama koje je zaprimila Komisija te ako se zanemare posebna područja koja nisu relevantna za prijenos podataka u okviru europsko-američkog sustava zaštite privatnosti (npr. istrage prijevare u sustavu zdravstvene skrbi, zlostavljanje djece ili slučajevi povezani s kontroliranim tvarima), to se uglavnom odnosi na određena tijela u skladu sa Zakonom o zaštiti privatnosti u području elektroničke komunikacije (ECPA), odnosno na zahtjeve za osnovne informacije o pretplatniku, sesiji i naplati (18 U.S.C. članak 2703. točka (c) podtočke 1. i 2., npr. adresa, vrsta/trajanje usluge) i za sadržaj poruka e-pošte starijih od 180 dana (18 U.S.C. članak 2703. točke (a) i (b)). Međutim, u potonjem slučaju predmetna osoba mora biti obaviještena te stoga ima priliku osporiti zahtjev na sudu. Vidjeti i pregled u Ministarstvo pravosuđa, Pretres i zapljena računala i pribavljanje elektroničkih dokaza u kaznenim istragama (*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*), Poglavlje 3. Zakon o pohranjenoj komunikaciji (*Stored Communications Act*), str. 115.–138.

([190]) Prema izjavama američke vlade primatelji upravnih sudskih poziva mogu ih osporiti na sudu na osnovi toga da su nerazumni, odnosno pretjerani, opresivni ili opterećujući. Vidjeti izjave Ministarstva pravosuđa (Prilog VII.), str. 2.

(129) Isto vrijedi i za upotrebu upravih sudskih poziva u svrhe javnog interesa. Nadalje, prema izjavama američke vlade, slična materijalna ograničenja primjenjuju se u pogledu toga da agencije mogu tražiti samo pristup podacima koji su relevantni za pitanja u njihovoj nadležnosti te moraju poštovati načelo razumnosti.

(130) Nadalje, u pravu SAD-a predviđa se niz oblika sudske zaštite pojedinaca od javnog tijela ili jednog od njegovih službenika ako ta tijela obrađuju osobne podatke. Ti oblici zaštite, koji napose uključuju Zakon o upravnom postupku (*Administrative Procedure Act*, APA), Zakon o pravu na pristup informacijama (*Freedom of Information Act*, FOIA) i Zakon o zaštiti privatnosti u području elektroničke komunikacije (*Electronic Communications Privacy Act*, ECPA), dostupni su svim osobama bez obzira na državljanstvo, u skladu sa svim primjenjivim uvjetima.

(131) Općenito, prema odredbama Zakona o upravnom postupku koje se odnose na sudsko preispitivanje ([191]), „svaka osoba koja je u pravnom smislu oštećena ili ugrožena aktivnošću agencije ili je takva aktivnost negativno utjecala na nju" ima pravo zatražiti sudsko preispitivanje ([192]). To uključuje mogućnost da od suda zatraži da „proglasi nezakonitima i ukine mjere, nalaze i zaključke agencija za koje se smatra da su […] samovoljne, hirovite, zloupotreba diskrecije ili da na drugi način nisu u skladu sa zakonom" ([193]).

(132) Točnije, u glavi II. Zakona o zaštiti privatnosti u području elektroničke komunikacije ([194]) utvrđuje se sustav propisanih prava na privatnost i uređuje pristup radi kaznenog progona telefonskoj, usmenoj ili elektroničkoj komunikaciji koju pohranjuju pružatelji usluga koji su treća strana ([195]). Njome se kriminalizira nezakonit pristup takvoj komunikaciji (tj. onaj koji nije sudski odobren ili inače dopušten) te se oštećenom pojedincu pruža mogućnost da podnese građansku tužbu američkom Saveznom sudu radi stvarne i kaznene odštete te pravične ili deklarativne naknade protiv vladinog službenika koji je samovoljno počinio takve nezakonite radnje ili protiv Sjedinjenih Američkih Država.

(133) Osim toga, u skladu sa Zakonom o pravu na pristup informacijama (FOIA, 5 U.S.C. članak 552.) svaka osoba ima pravo pristupiti evidenciji saveznih agencija i, nakon što se iscrpe administrativni oblici pravne zaštite, ostvariti takvo pravo na sudu, osim ako je takva evidencija zaštićena od javnog objavljivanja izuzećem ili posebnim isključenjem od kaznenog progona ([196]).

([191]) 5 U.S.C. članak 702.

([192]) Sudskom preispitivanju obično podliježe samo „krajnje", a ne „prethodno, postupovno ili privremeno" djelovanje agencije. Vidjeti 5 U. S.C. članak 704.

([193]) 5 U.S.C. članak 706. stavak 2. točka A.

([194]) 18 U.S.C. članci od 2701. do 2712.

([195]) Zakonom o zaštiti privatnosti u području elektroničke komunikacije (ECPA) štiti se komunikacija na dvije određene vrste pružatelja mrežnih usluga, naime pružateljima: i. usluga elektroničke komunikacije (npr. telefonija ili e-pošta); ii. računalnih usluga na daljinu kao što su usluge računalne pohrane ili obrade.

([196]) Ta su izuzeća, međutim, ograničena. Primjerice, prema 5 U.S.C. članku 552. stavku (b) točki 7., prava zajamčena FOIA-om isključena su za „evidenciju ili informacije prikupljene u svrhu kaznenog progona, ali samo u mjeri u kojoj se za davanje na uvid takve evidencije ili informacija (A) može u razumnoj mjeri očekivati da će omesti provedbeni postupak, (B) njome bi se osobi uskratilo pravo na pošteno suđenje ili nepristrano donošenje presude, (C) može se u razumnoj mjeri očekivati da će predstavljati neopravdano zadiranje u čiju privatnost, (D) moglo bi se u razumnoj mjeri očekivati da će otkriti identitet povjerljivog izvora, uključujući državnu, lokalnu ili stranu agenciju ili tijelo ili bilo koju privatnu ustanovu koja je informacije pribavila na povjerljivoj osnovi te bi se, u slučaju evidencije ili informacija koje je prikupilo tijelo kaznenog progona tijekom kaznene istrage ili agencija pri provedbi zakonite obavještajne istrage radi nacionalne sigurnosti informacijama pribavljenim iz povjerljivih izvora (E) otkrile tehnike i postupci istraga ili kaznenog progona ili bi se otkrile smjernice za njih ako se za takvo otkrivanje može u razumnoj mjeri očekivati da će predstavljati rizik od zaobilaženja zakona ili bi se (F) moglo u razumnoj mjeri očekivati da će ugroziti čiji život ili fizičku sigurnost." Osim toga, „prilikom svakog podnošenja zahtjeva koji uključuje pristup evidenciji [za čije bi se davanje na uvid moglo u razumnoj mjeri očekivati da će omesti provedbeni postupak] – i (A) istraga ili postupak uključuje moguće kršenje kaznenog prava i (B) postoji vjerojatnost da i. predmet istrage ili postupka nije upoznat s tim da su u tijeku te ii. za otkrivanje postojanja evidencije moglo bi se u razumnoj mjeri očekivati da će ometati provedbeni postupak, agencija smije, samo za vrijeme takvih okolnosti, smatrati da se na evidenciju ne primjenjuju zahtjevi iz ovog odjeljka." (5 U.S.C. članak 552. točka (c) podtočka 1.).

(134) Osim toga, nizom drugih zakona pojedincima se pruža pravo da podnesu tužbu protiv američkog javnog tijela ili službenika s obzirom na obradu svojih osobnih podataka, primjerice Zakonom o prisluškivanju (*Wiretap Act*) ([197]), Zakonom o računalnoj prijevari i zloupotrebi (*Computer Fraud and Abuse Act*) ([198]), Saveznim zakonom o tužbi za naknadu građanske štete (*Federal Torts Claim Act*) ([199]), Zakonom o pravu na privatnost financijskih podataka (*Right to Financial Privacy Act*) ([200]) i Zakonom o poštenom izvješćivanju o kreditnoj sposobnosti (*Fair Credit Reporting Act*) ([201]).

(135) Komisija stoga zaključuje da u Sjedinjenim Američkim Državama postoje pravila za ograničavanje zadiranja u temeljna prava za potrebe kaznenog progona ([202]) ili druge potrebe javnog interesa osoba čiji se podaci prenose iz Unije u SAD u okviru europsko-američkog sustava zaštite privatnosti na ono što je nužno za postizanje predmetnog legitimnog cilja i da se tim pravilima osigurava djelotvorna pravna zaštita protiv takvog zadiranja.

4. ODGOVARAJUĆA RAZINA ZAŠTITE U OKVIRU EUROPSKO-AMERIČKOG SUSTAVA ZAŠTITE PRIVATNOSTI

(136) S obzirom na te zaključke Komisija smatra da Sjedinjene Američke Države osiguravaju odgovarajuću razinu zaštite osobnih podataka koji se prenose iz Unije samocertificiranim organizacijama u SAD-u u okviru europsko-američkog sustava zaštite privatnosti.

(137) Komisija posebno smatra da se Načelima koja je izdalo američko Ministarstvo trgovine u cjelini osigurava razina zaštite osobnih podataka koja je u osnovi jednakovrijedna razini zajamčenoj osnovnim načelima iz Direktive 95/46/EZ.

(138) Nadalje, djelotvorna primjena Načela zajamčena je obvezama transparentnosti i upravljanjem sustavom zaštite privatnosti koje provodi Ministarstvo trgovine.

(139) Nadalje, Komisija smatra da se mehanizmima nadzora i pravne zaštite u cjelini, koji se osiguravaju u okviru sustava zaštite privatnosti, organizacijama u sustavu zaštite privatnosti omogućuje otkrivanje i kažnjavanje povreda Načela u praksi te se osobi čiji se podaci obrađuju osiguravaju pravna sredstva za ostvarivanje pristupa njezinim osobnim podacima te za ispravak ili brisanje takvih podataka.

(140) Naposljetku, na temelju dostupnih informacija o pravnom poretku SAD-a, uključujući izjave i jamstva američke vlade, Komisija smatra da će svako zadiranje američkih javnih tijela u temeljna prava osoba čiji se podaci prenose iz Unije u Sjedinjene Američke Države u okviru europsko-američkog sustava zaštite privatnosti radi nacionalne sigurnosti, kaznenog progona ili drugih javnih interesa i povezana ograničenja koja se određuju samocertificiranim organizacijama u pogledu njihovog pridržavanja Načela biti ograničena na ono što je nužno za postizanje predmetnog legitimnog cilja te da postoji djelotvorna pravna zaštita od takvog zadiranja.

([197]) 18 U.S.C. članci 2510. i dalje. U skladu sa Zakonom o prisluškivanju (18 U.S.C. članak 2520.) osoba čija se telefonska, usmena ili elektronička komunikacija presreće, objavljuje ili namjerno koristi može podnijeti građansku tužbu zbog kršenja Zakona o prisluškivanju, u određenim okolnostima i protiv državnog službenika ili Sjedinjenih Američkih Država. Za prikupljanje adresa i drugih informacija koje ne uključuju sadržaj (npr. IP adresa, adresa e-pošte primatelja/pošiljatelja) vidjeti poglavlje Uređaji za bilježenje ulaznih i izlaznih poziva glave 18. (18 U.S.C. poglavlja od 3121. do 3127. te za građansku tužbu članak 2707.).

([198]) 18 U.S.C. članak 1030. U skladu sa Zakonom o računalnoj prijevari i zloupotrebi osoba može podnijeti tužbu protiv svake osobe u pogledu namjernog neovlaštenog pristupa (ili prekoračenja ovlaštenog pristupa) radi prikupljanja informacija od financijske ustanove, računalnog sustava američke vlade ili drugog određenog računala, u određenim okolnostima i protiv državnog službenika.

([199]) 28 U.S.C. članci 2671. i dalje. U skladu sa Saveznim zakonom o tužbi za naknadu građanske štete osoba u određenim okolnostima može podnijeti tužbu protiv Sjedinjenih Američkih Država zbog „nemara, štetne radnje ili propusta svakog zaposlenika vlade dok djeluje u okviru svog mandata ili radnog odnosa."

([200]) 12 U.S.C. članci 3401. i dalje. U skladu sa Zakonom o pravu na privatnost financijskih podataka osoba u određenim okolnostima može podnijeti tužbu protiv Sjedinjenih Američkih Država zbog pribavljanja ili otkrivanja zaštićene financijske evidencije kršenjem tog zakona. Pristup vlade zaštićenoj financijskoj evidenciji općenito je zabranjen osim ako vlada podnese zahtjev koji podliježe zakonitom sudskom pozivu ili nalogu za pretres ili, podložno ograničenjima, službeni pisani zahtjev te pojedinac čije se informacije traže primi obavijest o takvom zahtjevu.

([201]) 15 U.S.C. članci od 1681. do 1681x. U skladu sa Zakonom o poštenom izvješćivanju o kreditnoj sposobnosti osoba može podnijeti tužbu protiv svake osobe koja ne ispunjava zahtjeve (posebno potrebu za zakonitim ovlaštenjem) za prikupljanje, širenje i upotrebu podataka o kreditnoj sposobnosti potrošača ili, pod određenim uvjetima, protiv vladine agencije.

([202]) Sud Europske unije priznao je kazneni progon kao legitiman politički cilj. Vidjeti spojene predmete C-293/12 i C-594/12, *Digital Rights Ireland i dr.*, EU:C:2014:238, točka 42. Vidjeti i članak 8. stavak 2. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda i presudu Europskog suda za ljudska prava u predmetu *Weber i Saravia protiv Njemačke*, zahtjev br. 54934/00, točka 104.

(141) Komisija zaključuje da su time ispunjeni uvjeti iz članka 25. Direktive 95/46/EZ protumačeni s obzirom na Povelju Europske unije o temeljnim pravima, kako je objasnio Sud EU-a posebno u presudi *Schrems*.

5. DJELOVANJE TIJELA ZA ZAŠTITU PODATAKA I OBAVJEŠĆIVANJE KOMISIJE

(142) U presudi *Schrems* Sud EU-a objasnio je da Komisija nije nadležna ograničavati ovlasti tijela za zaštitu podataka na temelju članka 28. Direktive 95/46/EZ (uključujući ovlast za suspenziju prijenosa podataka) ako osoba, podnoseći tužbu u skladu s tom odredbom, dovede u pitanje usklađenost odluke Komisije o primjerenosti sa zaštitom temeljnih prava na privatnost i zaštitu podataka ([203]).

(143) Radi djelotvornog praćenja funkcioniranja sustava zaštite privatnosti države članice trebale bi obavijestiti Komisiju o relevantnim mjerama koje poduzimaju tijela za zaštitu podataka.

(144) Sud EU-a smatrao je i da, u skladu s člankom 25. stavkom 6. drugim podstavkom Direktive 95/46/EZ, države članice i njihova tijela moraju poduzeti potrebne mjere za usklađivanje s aktima institucija Unije jer se ti akti u načelu smatraju zakonitima i proizvode pravne učinke do njihova povlačenja, poništenja u postupku za poništenje ili proglašavanja nevažećima nakon zahtjeva za prethodnu odluku ili tužbenog zahtjeva za proglašenje nezakonitosti. Stoga je odluka Komisije o odgovarajućoj razini zaštite donesena u skladu s člankom 25. stavkom 6. Direktive 95/46/EZ obvezujuća za sva tijela država članica kojima je upućena, uključujući njihova neovisna nadzorna tijela ([204]). Ako je takvo tijelo zaprimilo pritužbu kojom se dovodi u pitanje usklađenost odluke Komisije o odgovarajućoj razini zaštite sa zaštitom temeljnog prava na privatnost i zaštitu podataka i ako smatra da su dostavljeni prigovori utemeljeni, u nacionalnom pravu mora se osigurati mehanizam pravne zaštite za podnošenje tih prigovora nacionalnom sudu, koji u slučaju sumnje mora odgoditi postupak i uputiti Sudu EU-a zahtjev za prethodnu odluku ([205]).

6. POVREMENO PREISPITIVANJE ZAKLJUČKA O ODGOVARAJUĆOJ RAZINI ZAŠTITE

(145) S obzirom na činjenicu da se razina zaštite osigurana pravnim poretkom SAD-a može promijeniti, Komisija će, nakon donošenja ove Odluke, povremeno provjeravati jesu li zaključci u vezi s odgovarajućom razinom zaštite osigurane europsko-američkim sustavom zaštite privatnosti još uvijek činjenično i zakonski opravdani. Takva provjera potrebna je, u svakom slučaju, kad Komisija dobije informacije na temelju kojih može opravdano posumnjati u to ([206]).

(146) Komisija će stoga stalno pratiti opći okvir za prijenos osobnih podataka uspostavljen europsko-američkim sustavom zaštite privatnosti te poštuju li američka tijela izjave i obveze iz dokumenata priloženih ovoj Odluci. Kako bi se taj proces olakšao, SAD se obvezao obavještavati Komisiju o materijalnim razvojima prava SAD-a kad se to odnosi na sustav zaštite privatnosti u području zaštite podataka te ograničenja i zaštitne mjere primjenjive na pristup javnih tijela osobnim podacima. Nadalje, ova Odluka podliježe godišnjem zajedničkom preispitivanju koje će obuhvatiti sve aspekte funkcioniranja europsko-američkog sustava zaštite privatnosti, uključujući primjenu izuzeća od Načela iz razloga nacionalne sigurnosti i za potrebe kaznenog progona. Osim toga, budući da na zaključak o primjerenosti mogu utjecati promjene u pravu Unije, Komisija će procijeniti razinu zaštite koju pruža sustav zaštite privatnosti nakon početka primjene Opće uredbe o zaštiti podataka.

(147) Za potrebe provođenja godišnjeg zajedničkog preispitivanja iz priloga I., II. i VI. Komisija će se sastati s Ministarstvom trgovine i FTC-om i, prema potrebi, i drugim ministarstvima i agencijama uključenima u provedbu dogovora u okviru sustava zaštite privatnosti te, u pogledu pitanja nacionalne sigurnosti, s predstavnicima ODNI-ja, drugim subjektima obavještajne zajednice i Pravobraniteljem. Na tom sastanku mogu sudjelovati tijela za zaštitu podataka EU-a i predstavnici Radne skupine prema članku 29.

([203]) *Schrems*, točke 40. i dalje, od 101. do 103.
([204]) *Schrems*, točke 51., 52. i 62.
([205]) *Schrems*, točka 65.
([206]) *Schrems*, točka 76.

(148) U okviru godišnjeg zajedničkog preispitivanja Komisija će zatražiti od Ministarstva trgovine da dostavi opsežne informacije o svim relevantnim aspektima funkcioniranja europsko-američkog sustava zaštite privatnosti, uključujući slučajeve koje su Ministarstvu trgovine uputila tijela za zaštitu podataka i rezultate preispitivanja usklađenosti po službenoj dužnosti. Komisija će tražiti i objašnjenja u vezi sa svim pitanjima povezanima s europsko-američkim sustavom zaštite privatnosti i njegovim funkcioniranjem iz svih dostupnih izvora informacija, među ostalim iz izvješća o transparentnosti u skladu s američkim Zakonom o slobodi (*USA FREEDOM Act*), javnih izvješća američkih nacionalnih obavještajnih agencija, tijela za zaštitu podataka, skupina za zaštitu privatnosti, medijskih izvješća i drugih mogućih izvora. Nadalje, kako bi Komisiji olakšale obavljanje te zadaće, države članice trebale bi je obavijestiti o slučajevima kad tijela zadužena za osiguranje usklađenosti s Načelima u Sjedinjenim Američkim Državama nisu osigurala usklađenost i o naznakama da se djelovanjem američkih javnih tijela nadležnih za nacionalnu sigurnost ili sprečavanje, istragu, otkrivanje ili kazneni progon kaznenih djela ne osigurava potrebna razina zaštite.

(149) Na temelju zajedničkog godišnjeg preispitivanja Komisija će sastaviti javno izvješće koje se podnosi Europskom parlamentu i Vijeću.

7. SUSPENZIJA ODLUKE O PRIMJERENOSTI

(150) Ako Komisija, na temelju provjera ili drugih dostupnih informacija, zaključi da se razina zaštite pružene u okviru sustava zaštite privatnosti više ne može smatrati u osnovi jednakovrijednom razini zaštite u Uniji ili ako postoje jasne naznake da se više ne može osigurati djelotvorna usklađenost s Načelima u Sjedinjenim Američkim Državama, ili da se djelovanjem američkih javnih tijela nadležnih za nacionalnu sigurnost ili sprečavanje, istragu, otkrivanje ili kazneni progon kaznenih djela ne osigurava potrebna razina zaštite, ona će o tome obavijestiti Ministarstvo trgovine i tražiti poduzimanje odgovarajućih mjera za brzo rješavanje slučajeva moguće neusklađenosti s Načelima u određenom, razumnom roku. Ako po isteku navedenog roka američka tijela ne dokažu na zadovoljavajući način da se europsko-američkim sustavom zaštite privatnosti i dalje jamči djelotvorna usklađenost s Načelima i odgovarajuća razina zaštite, Komisija će pokrenuti postupak za djelomičnu ili potpunu suspenziju ove Odluke ili njezino stavljanje izvan snage ([207]). S druge strane, Komisija može predložiti izmjenu ove Odluke, na primjer ograničavanjem područja primjene zaključka o primjerenosti samo na prijenos podataka na koji se primjenjuju dodatni uvjeti.

(151) Konkretno, Komisija će pokrenuti postupak suspenzije ili stavljanja izvan snage u sljedećim slučajevima:

(a) ako postoje naznake da američka tijela ne poštuju izjave ili obveze iz dokumenata priloženih ovoj Odluci, među ostalim u vezi s uvjetima i ograničenjima pristupa američkih javnih tijela osobnim podacima koji se prenose u okviru sustava zaštite privatnosti u svrhu kaznenog progona, nacionalne sigurnosti i drugih javnih interesa;

(b) ako pritužbe osoba iz EU-a čiji se podaci obrađuju nisu djelotvorno riješene; u tom pogledu Komisija uzima u obzir sve okolnosti koje utječu na mogućnost osoba iz EU-a čiji se podaci obrađuju da ostvare svoja prava, među ostalim, konkretno, dobrovoljno preuzetu obvezu američkih samocertificiranih poduzeća da surađuju s tijelima za zaštitu podataka i postupaju u skladu s njihovim savjetima; ili

(c) ako Pravobranitelj za sustav zaštite privatnosti ne dostavi pravovremene i odgovarajuće odgovore na zahtjeve osoba iz EU-a čiji se podaci obrađuju.

(152) Komisija će razmotriti i pokretanje postupka izmjene, suspenzije ili stavljanja izvan snage ove Odluke ako, u kontekstu zajedničkog godišnjeg preispitivanja funkcioniranja europsko-američkog sustava zaštite privatnosti ili u nekom drugom kontekstu, Ministarstvo trgovine ili druga ministarstva ili agencije koji sudjeluju u provedbi sustava zaštite privatnosti ili, u pogledu pitanja koja se odnose na nacionalnu sigurnost, predstavnici američke obavještajne zajednice ili Pravobranitelj ne dostave informacije ili pojašnjenja nužna za procjenu usklađenosti s

([207]) Od datuma primjene Opće uredbe o zaštiti podataka Komisija će iskoristiti svoje ovlasti da, na osnovi opravdane hitnosti, donese provedbeni akt kojim se suspendira ova Odluka i koji će se primjenjivati odmah, bez prethodnog podnošenja nadležnom komitološkom odboru i koji će ostati na snazi najdulje šest mjeseci.

Načelima, djelotvornosti postupaka rješavanja pritužbi ili snižavanja potrebne razine zaštite zbog djelovanja američkih nacionalnih obavještajnih tijela, posebno zbog prikupljanja osobnih podataka i/ili pristupa tim podacima koji nisu ograničeni na ono što je nužno i razmjerno. U tom pogledu Komisija će uzeti u obzir u kojoj se mjeri relevantne informacije mogu pribaviti iz drugih izvora, među ostalim iz izvješća samocertificiranih američkih poduzeća u skladu s američkim Zakonom o slobodi.

(153) Radna skupina za zaštitu pojedinaca u vezi s obradom osobnih podataka, koja je osnovana u skladu s člankom 29. Direktive 95/46/EZ, objavila je mišljenje o razini zaštite koju pruža europsko-američki sustav zaštite privatnosti ([208]), koje je uzeto u obzir pri pripremi ove Odluke.

(154) Europski parlament donio je rezoluciju o transatlantskom protoku podataka ([209]).

(155) Mjere navedene u ovoj Odluci u skladu su s mišljenjem Odbora osnovanog člankom 31. stavkom 1. Direktive 95/46/EZ,

DONIJELA JE OVU ODLUKU:

Članak 1.

1. Za potrebe članka 25. stavka 2. Direktive 95/46/EZ Sjedinjene Američke Države osiguravaju odgovarajuću razinu zaštite osobnih podataka koji se prenose iz Unije organizacijama u Sjedinjenim Američkim Državama u okviru europsko-američkog sustava zaštite privatnosti.

2. Europsko-američki sustav zaštite privatnosti uspostavljen je u skladu s Načelima koje je 7. srpnja 2016. izdalo američko Ministarstvo trgovine, kako je navedeno u Prilogu II. te u službenim izjavama i obvezama iz dokumenata navedenih u Prilogu I. i prilozima od III. do VII.

3. Za potrebe stavka 1. osobni se podaci u okviru europsko-američkog sustava zaštite privatnosti iz Unije prenose organizacijama u Sjedinjenim Američkim Državama koje se nalaze na „Popisu organizacija u sustavu zaštite privatnosti", koji vodi i objavljuje američko Ministarstvo trgovine u skladu s odjeljcima I. i III. Načela navedenih u Prilogu II.

Članak 2.

Ova Odluka ne utječe na primjenu odredaba Direktive 95/46/EZ, osim članka 25. stavka 1., koje se odnose na obradu osobnih podataka u državama članicama, posebno članka 4.

Članak 3.

Ako nadležna tijela država članica izvršavaju svoje ovlasti u skladu s člankom 28. stavkom 3. Direktive 95/46/EZ čiji je ishod suspenzija ili potpuna zabrana protoka podataka prema organizaciji u Sjedinjenim Američkim Državama koja se nalazi na Popisu organizacija u sustavu zaštite privatnosti u skladu s odjeljcima I. i III. Načela iz Priloga II. radi zaštite osoba u pogledu obrade njihovih osobnih podataka, predmetna država članica bez odgode o tome obavješćuje Komisiju.

Članak 4.

1. Komisija stalno prati funkcioniranje europsko-američkog sustava zaštite privatnosti kako bi mogla procijeniti osiguravaju li Sjedinjene Američke Države i dalje odgovarajuću razinu zaštite osobnih podataka koji se u okviru tog sustava iz Unije prenose organizacijama u Sjedinjenim Američkim Državama.

([208]) Mišljenje 01/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti, doneseno 13. travnja 2016.
([209]) Rezolucija Europskog parlamenta od 26. svibnja 2016. o transatlantskom protoku podataka ((2016/2727 (RSP)).

2. Države članice i Komisija uzajamno se obavješćuju o slučajevima kad se čini da državna tijela u Sjedinjenim Američkim Državama koja imaju zakonske ovlasti za osiguravanje usklađenosti s Načelima iz Priloga II. ne osiguravaju djelotvorne mehanizme za otkrivanje i nadzor koji u praksi omogućuju utvrđivanje povreda Načela i njihovo kažnjavanje.

3. Države članice i Komisija uzajamno se obavješćuju o naznakama da američka javna tijela nadležna za nacionalnu sigurnost, kazneni progon ili druge javne interese zadiru u pravo pojedinaca na zaštitu njihovih osobnih podataka u mjeri koja prelazi ono što je nužno i/ili da ne postoji djelotvorna pravna zaštita protiv takvog zadiranja.

4. Komisija u roku od godine dana od datuma kad su države članice obaviještene o ovoj Odluci, a nakon toga jedanput godišnje, ocjenjuje zaključak iz članka 1. stavka 1. na temelju svih dostupnih informacija, među ostalim na temelju informacija zaprimljenih u okviru zajedničkog godišnjeg preispitivanja iz priloga I., II. i VI.

5. Komisija o svim važnim zaključcima obavješćuje Odbor uspostavljen u skladu s člankom 31. Direktive 95/46/EZ.

6. Komisija podnosi nacrt mjera u skladu s postupkom iz članka 31. stavka 2. Direktive 95/46/EZ radi suspenzije, izmjene ili stavljanja izvan snage ove Odluke ili ograničavanja njezina područja primjene, među ostalim u sljedećim slučajevima:

— ako postoje naznake da američka javna tijela ne poštuju izjave ili obveze iz dokumenata priloženih ovoj Odluci, među ostalim u vezi s uvjetima i ograničenjima pristupa američkih javnih tijela osobnim podacima koji se prenose u okviru europsko-američkog sustava zaštite privatnosti u svrhu kaznenog progona, nacionalne sigurnosti i drugih javnih interesa,

— ako se sustavno ne rješavaju pritužbe osoba iz EU-a čiji se podaci obrađuju, ili

— ako Pravobranitelj za sustav zaštite privatnosti sustavno ne daje pravovremene i odgovarajuće odgovore na zahtjeve osoba iz EU-a čiji se podaci obrađuju u skladu s odjeljkom 4. točkom (e) Priloga III.

Komisija predlaže takve nacrte mjera i ako zbog nedovoljne suradnje tijela odgovornih za osiguravanje funkcioniranja europsko-američkog sustava zaštite privatnosti u Sjedinjenim Američkim Državama ne može utvrditi utječe li to na zaključak iz članka 1. stavka 1.

Članak 5.

Države članice poduzimaju sve mjere potrebne za usklađivanje s ovom Odlukom.

Članak 6.

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 12. srpnja 2016.

Za Komisiju
Věra JOUROVÁ
Članica Komisije

PRILOG I.

Dopis ministrice trgovine SAD-a Penny Pritzker

7. srpnja 2016.

gđa. Věra JOUROVÁ
Povjerenica za pravosuđe, zaštitu potrošača i ravnopravnost spolova
Europska komisija
Rue de la Loi/Westraat 200
1049 Bruxelles
Belgija

Poštovana povjerenice Jourová,

zadovoljstvo mi je u ime Sjedinjenih Američkih Država dostaviti Vam ovim putem paket materijala o europsko-američkom sustavu zaštite privatnosti koji je proizvod dvije godine produktivnih razgovora između naših timova. Ovaj je paket, zajedno s drugim materijalima koji su dostupni Komisiji iz javnih izvora, vrlo čvrsta osnova za novi zaključak Komisije o primjerenosti zaštite ([1]).

Obje bismo trebale biti ponosne na poboljšanja Okvira. Sustav za zaštitu privatnosti temelji se na načelima koja imaju jaku i jednoglasnu potporu s obje strane Atlantika, a mi smo pojačali njihovo djelovanje. Zajedničkim radom doista možemo poboljšati zaštitu privatnosti u cijelom svijetu.

Paket za sustav zaštite privatnosti uključuje načela sustava zaštite privatnosti zajedno s dopisom (Prilog 1.) Uprave za međunarodnu trgovinu (*International Trade Administration,* ITA) Ministarstva trgovine, koja upravlja programom u kojem su opisane obveze našeg Ministarstva u pogledu osiguranja učinkovitog funkcioniranja sustava zaštite privatnosti. Paket uključuje i Prilog 2. koji sadržava ostale obveze Ministarstva trgovine povezane s novim modelom arbitraže koji je dostupan u okviru sustava zaštite privatnosti.

Dala sam uputu svojim zaposlenicima da ulože sve nužne resurse u brzu i potpunu provedbu okvira sustava zaštite privatnosti te da osiguraju pravovremeno ispunjenje obveza iz Priloga 1. i 2.

Paket za sustav zaštite privatnosti uključuje i druge dokumente agencija Sjedinjenih Američkih Država, odnosno sljedeće:

— dopis Savezne trgovinske komisije (*Federal Trade Commission*, FTC) u kojem je opisana njezina provedba sustava zaštite privatnosti,

— dopis Ministarstva prometa u kojem je opisana njegova provedba sustava zaštite privatnosti,

— dva dopisa koja je pripremio Ured direktora Nacionalne obavještajne službe (ODNI) u vezi sa zaštitnim mjerama i ograničenjima koja se primjenjuju na američka tijela za nacionalnu sigurnost,

— dopis Ministarstva vanjskih poslova i prateći memorandum u kojem je opisana opredijeljenost Ministarstva vanjskih poslova za uspostavu novog pravobranitelja sustava zaštite privatnosti za podnošenje upita u vezi s praksom Sjedinjenih Američkih Država povezanom s prikupljanjem obavještajnih podataka elektroničkim izviđanjem i

— dopis Ministarstva pravosuđa u vezi sa zaštitnim mjerama i ograničenjima pristupa američke vlade za potrebe provedbe zakona i radi javnog interesa.

Uvjeravam Vas da Sjedinjene Američke Države te obveze shvaćaju ozbiljno.

([1]) Ako se odluka Komisije o odgovarajućoj razini zaštite koju pruža europsko-američki sustav zaštite privatnosti primjenjuje na Island, Lihtenštajn i Norvešku, paket za sustav zaštite privatnosti obuhvatit će Europsku uniju i te tri navedene zemlje.

U roku od 30 dana od konačnog odobrenja zaključka o odgovarajućoj zaštiti potpuni paket za sustav zaštite privatnosti dostavlja se *Saveznom registru* za objavu.

S nestrpljenjem očekujemo zajedničku suradnju u okviru provedbe sustava zaštite privatnosti dok zajednički ulazimo u sljedeću fazu ovog postupka.

S poštovanjem,

Penny Pritzker

Prilog 1.

Dopis zamjenika ministra za vanjsku trgovinu Kena Hyatta

Poštovana gđa. Věra Jourová
Povjerenica za pravosuđe, zaštitu potrošača i ravnopravnost spolova
Europska komisija
Rue de la Loi/Westraat 200
1049 Bruxelles
Belgija

Poštovana povjerenice Jourová,

u ime Uprave za međunarodnu trgovinu zadovoljstvo mi je opisati pojačanu zaštitu osobnih podataka koja se osigurava europsko-američkim sustavom zaštite podataka (dalje u tekstu: „sustav zaštite podataka" ili „okvir") i obveze koje je preuzelo Ministarstvo trgovine (dalje u tekstu: „Ministarstvo") kako bi osiguralo učinkovito funkcioniranje sustava zaštite privatnosti. Dovršetak ovog povijesnog sporazuma važno je postignuće za privatnost i za poduzeća s obje strane Atlantika. Njime se osobama iz EU-a jamči da će njihovi podaci biti zaštićeni i da će imati na raspolaganju mjere zaštite u slučaju bilo kakvih problema. Time se stvara sigurnost koja će pridonijeti rastu transatlantskog gospodarstva osiguravanjem da tisuće europskih i američkih poduzeća mogu nastaviti ulagati i poslovati preko naših granica. Sustav zaštite privatnosti rezultat je više od dvije godine napornog rada i suradnje s vama, našim kolegama u Europskoj komisiji (dalje u tekstu: „Komisija"). Veselimo se daljnjoj suradnji s Komisijom kako bismo osigurali predviđeno funkcioniranje sustava zaštite privatnosti.

Radili smo s Komisijom na razvoju sustava zaštite privatnosti kako bismo organizacijama s poslovnim nastanom u Sjedinjenim Američkim Državama omogućili da ispune zahtjeve za odgovarajuću zaštitu podataka propisanu zakonodavstvom EU-a. Novi će okvir donijeti nekoliko značajnih prednosti za pojedince i poduzeća. Prvo, on pruža važan skup elemenata zaštite privatnosti podataka pojedinaca iz EU-a. Njime se od američkih organizacija sudionica zahtijeva da razviju usklađenu politiku privatnosti, da se javno obvežu da će poštovati načela sustava zaštite privatnosti kako bi ta obveza postala izvršiva u skladu s američkim zakonodavstvom, da svake godine Ministarstvu ponovno potvrđuju svoje poštovanje načela, da osiguraju besplatno neovisno rješavanje sporova pojedincima iz EU-a i da su u nadležnosti Savezne trgovinske komisije SAD-a (FTC), Ministarstva prometa (DOT) ili druge izvršne agencije. Drugo, sustavom zaštite privatnosti omogućit će se tisućama poduzeća u Sjedinjenim Američkim Državama i tamošnjim podružnicama europskih poduzeća da primaju osobne podatke iz Europske unije kako bi se olakšao protok podataka koji je potpora transatlantskoj trgovini. Transatlantski gospodarski odnos već je sada najveći na svijetu te obuhvaća polovinu svjetske gospodarske proizvodnje i gotovo bilijun dolara u trgovini robom i uslugama čime se podupiru milijuni radnih mjesta s obje strane Atlantika. Poduzeća koja se oslanjaju na prekogranične tokove podataka potječu iz svih sektora industrije i uključuju velika poduzeća Fortune 500 te mnoga mala i srednja poduzeća (MSP-ove). Transatlantski tokovi podataka omogućuju američkim organizacijama da obrađuju podatke koji su potrebni kako bi se Europljanima mogli ponuditi roba, usluge i prilike za zapošljavanje. Sustavom zaštite privatnosti podupiru se zajednička načela privatnosti, premošćuju razlike u našim pravnim pristupima se te potiču trgovina i gospodarski ciljevi Europe i Sjedinjenih Država.

Iako poduzeće dobrovoljno donosi odluku o samostalnom certificiranju u skladu s novim Okvirom, kada se javno obveže poštovati načela sustava zaštite privatnosti, ta je obveza izvršiva u skladu s američkim zakonodavstvom i mogu je izvršiti Savezna trgovinska komisija ili Ministarstvo prometa, ovisno o tome koje je tijelo nadležno za organizaciju u sustavu zaštite privatnosti.

Pojačanja u skladu s načelima sustava zaštite privatnosti

Ostvarenim sustavom zaštite privatnosti jača se zaštita privatnosti na sljedeće načine:

— zahtijevanjem dostavljanja dodatnih informacija osobama u skladu s načelom obavješćivanja, među ostalim izjave o sudjelovanju organizacije u sustavu zaštite privatnosti, izjave o pravu pojedinca na pristup osobnim podacima i naziva relevantnog neovisnog tijela za rješavanje sporova,

— jačanjem zaštite osobnih podataka koji se prenose iz organizacije u sustavu zaštite privatnosti trećoj strani koja djeluje kao voditelj obrade tražeći od stranaka da sklope ugovor kojim se predviđa da se takvi podaci mogu obrađivati samo u ograničene i posebno navedene svrhe u skladu sa suglasnošću pojedinca te da će primatelj osigurati jednaku razinu zaštite kao i načela,

— jačanjem zaštite osobnih podataka koji se prenose iz organizacije u sustavu zaštite privatnosti agentu treće strane, među ostalim tražeći od organizacije u sustavu zaštite privatnosti da učini sljedeće: poduzme razumne i primjerene korake kako bi osigurala da agent učinkovito obradi osobne podatke prenesene u skladu s obvezama organizacije u okviru načela, da na temelju obavijesti poduzme razumne i odgovarajuće korake za zaustavljanje i otklanjanje neovlaštene obrade i da Ministarstvu na zahtjev dostavi sažetak ili reprezentativnu presliku relevantnih odredaba o privatnosti svog ugovora s tim agentom,

— predviđanjem da je organizacija u sustavu zaštite privatnosti odgovorna za obradu osobnih podataka koje zaprima u okviru sustava zaštite privatnosti i koje potom prosljeđuje trećoj strani koja djeluje kao agent u njezino ime te da organizacija u sustavu zaštite privatnosti ostaje odgovorna u skladu s načelima ako njezin agent obrađuje takve osobne podatke na način koji nije u skladu s načelima, osim ako organizacija dokaže da nije odgovorna za događaj zbog kojeg je nastala šteta,

— pojašnjavanjem da organizacije u sustavu zaštite privatnosti moraju ograničiti osobne podatke na podatke koji su relevantni za potrebe obrade,

— traženjem od organizacije da svake godine Ministarstvu potvrdi svoju obvezu primjene načela na informacije koje je zaprimila dok je sudjelovala u sustavu zaštite privatnosti ako napusti taj sustav i odluči zadržati takve podatke,

— zahtijevanjem osiguravanja neovisnih mehanizama pravne zaštite bez troška za pojedinca,

— traženjem od organizacija i odabranih neovisnih mehanizama pravne zaštite da žurno odgovore na upite i zahtjeve Ministarstva trgovine za informacije povezane sa sustavom zaštite privatnosti,

— traženjem od organizacija da hitno odgovore na pritužbe u pogledu poštovanja načela koje su im uputila nadležna tijela država članica posredstvom Ministarstva i

— traženjem od organizacije u sustavu zaštite privatnosti da objavi sve relevantne odjeljke izvješća o poštovanju ili ocjenjivanju povezane sa sustavom zaštite privatnosti koji su podneseni FTC-u ako postane predmetom naloga FTC-a ili sudskog naloga zbog nepoštovanja načela.

Upravljanje programom sustava zaštite privatnosti i nadzor tog programa koje obavlja Ministarstvo trgovine

Ministarstvo ponavlja svoju opredijeljenost za vođenje i objavljivanje obvezujućeg popisa organizacija SAD-a koje su obavile samocertificiranje pred Ministarstvom i izjavile svoju opredijeljenost za poštovanje načela (dalje u tekstu „Popis organizacija u sustavu zaštite privatnosti"). Ministarstvo će ažurirati Popis organizacija u sustavu zaštite privatnosti uklanjanjem organizacija s popisa kada se one dobrovoljno povuku, kada ne ispune obvezu godišnje ponovne certifikacije u skladu s postupcima Ministarstva i ako se utvrdi da uporno ne poštuju načela. Ministarstvo će održavati i objaviti pouzdanu evidenciju američkih organizacija koje su prethodno obavile samocertificiranje Ministarstvu, ali su uklonjene s Popisa organizacija u sustavu zaštite privatnosti, uključujući onih koje su uklonjene zbog trajnog nepoštovanja načela. Ministarstvo će navesti razlog uklanjanja svake organizacije.

Nadalje, Ministarstvo se obvezuje na jačanje upravljanja sustavom zaštite privatnosti i za njegov nadzor. Ministarstvo će posebno činiti sljedeće:

Objaviti dodatne informacije na *web*-mjestu sustava zaštite privatnosti

— održavati Popis organizacija u sustavu zaštite privatnosti i evidenciju o organizacijama koje su prethodno samocertificirale svoje pridržavanje načela, ali koje više ne uživaju koristi sustava zaštite privatnosti,

— uključiti istaknuto objašnjenje da organizacije koje su uklonjene s Popisa organizacija u sustavu zaštite privatnosti više ne uživaju koristi sustava zaštite privatnosti, ali svejedno moraju nastaviti primjenjivati ta načela na osobne podatke koje su zaprimile dok su sudjelovale u sustavu zaštite privatnosti sve dok zadržavaju takve informacije i

— navesti poveznicu na popis slučajeva FTC-a povezanih sa sustavom zaštite privatnosti koji se nalazi na *web*-mjestu FTC-a.

Provjeriti zahtjeve za samocertificiranje

— Prije dovršetka samocertificiranja određene organizacije (ili godišnjeg ponovnog certificiranja) i stavljanja njezina imena na Popis organizacija u sustavu zaštite privatnosti, provjeriti je li organizacija učinila sljedeće:

  — navela potrebne kontaktne podatke za organizaciju,

  — opisala aktivnosti organizacije s obzirom na osobne podatke zaprimljene iz EU-a,

  — navela koji su osobni podaci obuhvaćeni samocertificiranjem,

  — ako organizacija ima javno *web*-mjesto, osigurala da je dostupna web-adresa na kojoj je dostupna politika zaštite privatnosti i da je politika zaštite privatnosti dostupna na tom web-mjestu ili, ako organizacija nema javno *web*-mjesto, osigurala mjesto gdje će politika zaštite privatnosti biti dostupna javnosti za pregled,

  — uključila svoju primjenjivu politiku zaštite privatnosti izjavu da poštuje načela i da je politika zaštite privatnosti dostupna na internetu te poveznicu na *web*-mjesto sustava zaštite privatnosti tog Ministarstva,

  — odredila državno tijelo koje je nadležno rješavati pritužbe protiv organizacije u pogledu mogućih nepoštenih ili prijevarnih praksi i kršenja zakona ili propisa koji uređuju privatnost (i da je to navedeno u načelima ili budućem prilogu načelima),

  — ako organizacija odluči zadovoljiti zahtjeve iz točke (a) podtočke i. i točke (a) podtočke iii. načela pravne zaštite, provedbe i odgovornosti, obvezujući se na suradnju s odgovarajućim nadležnim tijelima EU-a za zaštitu podataka, ako navodi svoju namjeru suradnje s tijelima za zaštitu podataka pri istrazi i rješavanju pritužbi podnesenih u okviru sustava zaštite privatnosti, posebno za odgovaranje na njihove upite kada su osobe iz EU-a čiji se podaci obrađuju podnijele svoje pritužbe izravno svojim nacionalnim tijelima za zaštitu podataka,

  — navela naziv programa za zaštitu privatnosti u kojima organizacija sudjeluje kao član;

  — navela način provjere poštovanja načela (npr. interno, uz pomoć treće strane itd.),

  — navela, u izjavi o samocertificiranju i u svojoj politici za zaštitu privatnosti, neovisni mehanizam pravne zaštite koji je dostupan za istraživanje i rješavanje pritužbi,

  — uključila u svoju politiku zaštite privatnosti, ako je ta politika dostupna na internetu, poveznicu na *web*-mjesto ili obrazac za podnošenje pritužbi neovisnog mehanizma pravne zaštite koji je dostupan za rješavanje neriješenih pritužbi i

  — ako je organizacija navela da planira primati podatke o ljudskim resursima koji se prenose iz EU-a za uporabu u kontekstu radnog odnosa, izjavila svoju obvezu suradnje s nadležnim tijelima zaštitu podataka na rješavanju pritužbi koje se odnose na njezine aktivnosti u vezi s tim podacima, dostavila Ministarstvu presliku svoje politike zaštite ljudskih resursa i navela gdje obuhvaćeni zaposlenici mogu pročitati politiku zaštite privatnosti.

— surađivati s neovisnim mehanizmima pravne zaštite na provjeri da su se organizacije registrriale pri relevantnom mehanizmu navedenom u njihovim potvrdama o samocertificiranju, ako je takva registracija potrebna.

Proširiti napore za praćenje organizacija koje su uklonjene s Popisa organizacija u sustavu zaštite privatnosti

— obavijestiti organizacije koje su uklonjene s Popisa organizacija u sustavu zaštite privatnosti zbog „ustrajnog nepoštovanja načela" da nemaju pravo zadržati podatke prikupljene u okviru sustava zaštite privatnosti i

— slati upitnike organizacijama čija su samocertificiranja istekla ili koje su se dobrovoljno povukle iz europsko-američkog sustava zaštite privatnosti kako bi provjerilo hoće li ta organizacija vratiti ili izbrisati osobne podatke koje je zaprimila tijekom sudjelovanja u europsko-američkom sustavu zaštite privatnosti ili nastaviti primjenjivati načela privatnosti na te podatke i, ako ih zadrži, provjeriti tko će u organizaciji biti stalna kontaktna točka za pitanja povezana sa sustavom zaštite privatnosti.

Tražiti i uklanjati lažne tvrdnje o sudjelovanju

— preispitati politike zaštite privatnosti organizacija koje su prethodno sudjelovale u programu sustava zaštite privatnosti, ali koje su uklonjene s Popisa organizacija u sustavu zaštite privatnosti kako bi mogle utvrditi lažne tvrdnje o sudjelovanju u sustavu zaštite privatnosti,

— redovito kada se organizacija: (a) povukla iz sudjelovanja u sustavu zaštite privatnosti, (b) nije ponovno certificirala svoje pridržavanje načela ili (c) uklonjena je kao sudionik u sustavu zaštite privatnosti zbog „ustrajnog nepoštovanja načela", po službenoj dužnosti obavljati provjere je li organizacija uklonila iz relevantne objavljene politike zaštite privatnosti upućivanje na sustav za zaštitu privatnosti koje bi upućivalo na to da organizacija i dalje aktivno surađuje u sustavu zaštite privatnosti i da ima pravo na njegove koristi. Ako Ministarstvo utvrdi da takva upućivanja nisu uklonjena, Ministarstvo će upozoriti organizaciju da će, ako bude potrebno, uputiti to pitanje relevantnoj agenciji za potrebe mogućeg izvršenja ako nastaviti tvrditi da je certificirana za sudjelovanje u sustavu zaštite privatnosti. Ako organizacija ne ukloni upućivanja i ne obavi ponovnu certifikaciju svog poštovanja načela u okviru sustava zaštite privatnosti, Ministarstvo će po službenoj dužnosti uputiti predmet FTC-u, DOT-u ili drugoj odgovarajućoj izvršnoj agenciji ili, u odgovarajućim slučajevima, poduzeti mjere za ovrhu oznake o certifikaciji sudjelovanja u sustavu zaštite privatnosti,

— poduzeti druge napore za utvrđivanje lažnih tvrdnji o sudjelovanju u sustavu zaštite privatnosti i o neprimjerenoj uporabi oznake o certifikaciji sudjelovanja su sustavu, među ostalim pretraživanjem na internetu radi provjere gdje se prikazuju oznake certifikacije sustava zaštite privatnosti i gdje se u politikama zaštite privatnosti organizacija upućuje na sustav zaštite privatnosti,

— žurno riješiti sva utvrđena pitanja tijekom praćenja lažnih tvrdnji o sudjelovanju i zlouporabe oznake o certifikaciji, među ostalim upozoravanjem organizacija koje lažno tvrde da sudjeluju u programu sustava zaštite privatnosti kako je prethodno opisano,

— poduzeti druge odgovarajuće korektivne mjere, među ostalim primjenom drugih zaštitnih mjera koje je Ministarstvo ovlašteno poduzimati i upućivanjem pitanja FTC-u, DOT-u ili drugoj odgovarajućoj izvršnoj agenciji i

— žurno preispitivati i rješavati zaprimljene pritužbe na lažne tvrdnje o sudjelovanju.

Ministarstvo će provoditi preispitivanje politika zaštite privatnosti organizacija u cilju učinkovitijeg otkrivanja i uklanjanja lažnih tvrdnji o sudjelovanju u sustavu zaštite privatnosti. Ministarstvo će posebno preispitivati politike zaštite privatnosti organizacija čije je samocertificiranje isteklo jer se nisu ponovno potvrdile svoju usklađenost s načelima. Ministarstvo provodi takve vrste preispitivanja kako bi provjerilo da su takve organizacije uklonile iz svojih objavljenih relevantnih politika zaštite privatnosti upućivanja da organizacije aktivno sudjeluju u sustavu zaštite privatnosti. Zbog takvih vrsta preispitivanja, utvrdit ćemo organizacije koje nisu uklonile takva upućivanja i poslat ćemo im dopis iz odjela glavnog pravnog savjetnika Ministarstva s upozorenjem o mogućem provedbenom postupku ako upućivanja ne budu uklonjena. Ministarstvo će dalje naknadno pratiti jesu li organizacije uklonile neodgovarajuća upućivanja ili ponovno potvrdile svoje pridržavanje načela. Nadalje, Ministarstvo će uložiti napore u utvrđivanje lažnih tvrdnji organizacija koje nikada nisu sudjelovale u programu sustava zaštite privatnosti o sudjelovanju u tome sustavu i poduzet će slične korektivne mjere u pogledu takvih organizacija.

Po službenoj dužnosti provoditi povremena preispitivanja usklađenosti i procjene programa

— trajno pratiti usklađenost, među ostalim slanjem detaljnih upitnika organizacijama sudionicama radi utvrđivanja pitanja za koje bi mogle biti opravdane daljnje mjere. Takva preispitivanja usklađenosti posebno se obavljaju u sljedećim slučajevima: (a) Ministarstvo je zaprimilo posebne utemeljene pritužbe da organizacija ne poštuje načela, (b) organizacija ne odgovara na zadovoljavajući način na zahtjeve Ministarstva za informacije u vezi sa sustavom zaštite privatnosti ili (c) postoje uvjerljivi dokazi da organizacija ne izvršava svoje obveze iz sustava zaštite privatnosti. Ministarstvo se, prema potrebi, savjetuje o takvim preispitivanjima usklađenosti s nadležnim tijelom za zaštitu podataka, i

— povremeno ocjenjuje upravljanje programom sustava zaštite privatnosti i nadzire ga kako bi osigurala da je praćenje primjereno za rješavanje novih izazova.

Ministarstvo je povećalo resurse koji će biti posvećeni upravljanju programom sustava zaštite privatnosti i za nadzor tog programa, među ostalim udvostručivanjem broja zaposlenika odgovornih za upravljanje programom i za njegov nadzor. Nastavit ćemo izdvajati odgovarajuće resurse za takve napore u cilju osiguranja učinkovitog praćenja programa i upravljanja njime.

Prilagoditi *web*-mjesto sustava zaštite privatnosti ciljanoj publici

Ministarstvo će prilagoditi *web*-mjesto sustava zaštite privatnosti trima ciljanim publikama: osobama iz EU-a, poduzećima iz EU-a i poduzećima iz SAD-a. Uključivanjem materijala isključivo namijenjenog osobama i poduzećima iz EU-a olakšat će se transparentnost na različite načine. U pogledu fizičkih osoba iz EU-a na njemu će jasno biti objašnjeno sljedeće: 1. prava koja se osobama osiguravaju u okviru sustava zaštite privatnosti; 2. mehanizmi pravne zaštite koji su dostupni osobama iz EU-a kada vjeruju da je organizacija prekršila svoju obvezu poštovanja načela; i 3. kako pronaći informacije povezane sa samocertificiranjem organizacija za sudjelovanje u sustavu zaštite privatnosti. U pogledu poduzeća iz EU-a, olakšat će se provjera sljedećeg: 1. jamče li se organizaciji koristi sustava zaštite privatnosti; 2. vrste informacija povezanih sa samocertificiranjem organizacija za sudjelovanje u sustavu zaštite privatnosti; 3. politike zaštite privatnosti koja se primjenjuje na obuhvaćene informacije i 4. metode koju organizacija upotrebljava za provjeru svojeg pridržavanja načela.

Pojačati suradnju s tijelima za zaštitu podataka

Kako bi povećalo prilike za suradnju s tijelima za zaštitu podataka, Ministarstvo će uspostaviti posebnu kontaktu točku u Ministarstvu koja će djelovati kao veza s tijelima za zaštitu podataka. U slučajevima kada nadležno tijelo za zaštitu podataka vjeruje da organizacija ne poštuje načela, među ostalim na temelju pritužbe osobe iz EU-a, tijelo za zaštitu podataka može se obratiti Ministarstvu da uputi organizaciju na daljnje preispitivanje. Kontaktna točka primat će obavijesti o organizacijama koje lažno tvrde da sudjeluju u sustavu zaštite privatnosti unatoč tome što nikad nisu obavile samocertificiranje svog pridržavanja načela. Kontaktna točka pomagat će tijelima za zaštitu podataka u traženju informacija povezanih sa samocertificiranjem određene organizacije ili s njezinim prethodnim sudjelovanjem u programu i odgovarat će na upite tijela za zaštitu podataka u vezi s provedbom posebnih zahtjeva sustava zaštite privatnosti. Drugo, Ministarstvo će nadležnim tijelima za zaštitu podataka davati materijale u vezi sa sustavom zaštite privatnosti za uključivanje na njihova *web*-mjesta u cilju povećanja transparentnosti za osobe i poduzeća iz EU-a. Podizanjem razine svijesti o sustavu zaštite privatnosti i pravima i odgovornostima koje iz njega proizlaze trebalo bi se olakšati utvrđivanje pitanja kako budu nastajala kako bi se mogla primjereno riješiti.

Olakšati rješavanje pritužbi o neusklađenosti

Ministarstvo će, posredstvom svoje posebne točke za kontakt, primati pritužbe koje je dostavilo tijelo za zaštitu podataka da organizacija u sustavu zaštite privatnosti ne poštuje načela. Ministarstvo će uložiti najbolje napore u rješavanje pritužbe s organizacijom sustava zaštite privatnosti. U roku od 90 dana od primitka pritužbe Ministarstvo će nadležno tijelo za zaštitu podataka obavijestiti o napretku. U cilju olakšavanja podnošenja takvih pritužbi Ministarstvo će izraditi standardni obrazac koji tijela za zaštitu podataka mogu podnositi kontaktnoj točki u Ministarstvu. Posebna kontaktna točka pratit će sve slučajeve koje je tijelo za zaštitu podataka uputilo Ministarstvu i Ministarstvo će u godišnje preispitivanje koje je opisano u nastavku uključiti izvješće s analizom ukupnog broja pritužbi koje zaprima svake godine.

Donijeti arbitražne postupke i odabrati arbitre u dogovoru s Komisijom

Ministarstvo će ispuniti svoje obveze iz Priloga I. i objaviti postupke nakon postignutog dogovora.

Zajednički mehanizam za preispitivanje funkcioniranja sustava zaštite privatnosti

Ministarstvo trgovine, FTC i druge agencije, prema potrebi, održavaju godišnje sastanke s Komisijom, zainteresiranim tijelima za zaštitu podataka i odgovarajućim predstavnicima iz Radne skupine prema članku 29. na kojima ih Ministarstvo obavješćuje o provedbi programa sustava zaštite privatnosti. Godišnji sastanci uključivat će raspravu o aktualnim pitanjima povezanima s funkcioniranjem, provedbom, nadzorom i provedbom sustava zaštite privatnosti, među ostalim o upućenim slučajevima koje je Ministarstvo zaprimilo od tijela za zaštitu podataka, rezultate provjera sukladnosti koje se provode po službenoj dužnosti i mogu uključivati i razgovor o relevantnim izmjenama zakona Prvo godišnje preispitivanje, kao i daljnja preispitivanja, ako za njima bude potrebe, uključit će i dijalog o drugim pitanjima, na primjer u području donošenja automatskih odluka, uključujući aspekte u vezi sa sličnostima i razlikama u pristupima EU-a i SAD-a.

Ažuriranje zakonodavstva

Ministarstvo će uložiti razumne napore kako bi obavijestilo Komisiju o konkretnim mjerama ažuriranja zakona u SAD-u koje su relevantne za sastav zaštite privatnosti u području zaštite privatnosti podataka, ograničenja i zaštitnih mjera koje se primjenjuju na pristup američkih tijela osobnim podacima i njihovu daljnju uporabu.

Izuzeće radi nacionalne sigurnosti

U pogledu ograničenja poštovanja načela sustava zaštite privatnosti iz razloga nacionalne sigurnosti, glavni pravni savjetnik Ureda direktora Nacionalne obavještajne službe, Robert Litt, također je poslao dva dopisa naslovljen na Justina Antonipillaija i Teda Deana iz Ministarstva trgovine i ti su vam dopisi proslijeđeni. U tim se dopisima, među ostalim, opsežno razmatraju politike, zaštitne mjere i ograničenja koja se primjenjuju na aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem koje provodi SAD. Nadalje, u tim se dopisima opisuje transparentnost obavještajne zajednice u pogledu tih pitanja. Dok Komisija ocjenjuje okvir sustava zaštite privatnosti, informacijama u tim dopisima pružaju se jamstva na temelju kojih ona može zaključiti da će sustav za zaštitu privatnosti primjereno funkcionirati, u skladu s utvrđenim načelima. Razumijemo da biste informacije koje je obavještajna zajednica objavila, zajedno s drugim informacijama, mogli upotrijebiti kao temelj za buduće preispitivanje okvira sustava zaštite privatnosti.

Na temelju načela sustava zaštite privatnosti i pratećih dopisa i materijala uključujući obveze koje je Ministarstvo preuzelo u pogledu upravljanja okvirom sustava za zaštitu privatnosti i nadzora nad njim, očekujemo da će Komisija utvrditi da se europsko-američkim sustavom za zaštitu podataka osigurava dovoljna zaštita za potrebe prava EU-a i da će se nastaviti prijenos podataka iz Europske unije organizacijama koje sudjeluju u sustavu zaštite privatnosti.

S poštovanjem,

Ken Hyatt

Prilog 2.

Model arbiraŽe

PRILOG I.

U ovom Prilogu I. navedeni su uvjeti pod kojima su organizacije u sustavu zaštite privatnosti dužne obavljati arbitražu u skladu s načelom pravne zaštite, provedbe i odgovornosti. Mogućnost obvezujuće arbitraže koja je opisana u nastavku primjenjuje se na određena „preostala" potraživanja u vezi s podacima obuhvaćenima europsko-američkim sustavom zaštite privatnosti. Svrha je ove mogućnosti osobama osigurati mogućnost žurnog, neovisnog i poštenog mehanizma za rješavanje navodnih povreda načela koje nisu riješene drugim mehanizmima sustava zaštite privatnosti, ako ih ima.

A. **Područje primjene**

Ova mogućnost arbitraže dostupna je osobama kako bi mogle utvrditi, za preostala potraživanja, je li organizacija u sustavu zaštite privatnosti povrijedila svoju obvezu u skladu s načelima u pogledu pojedinca te je li ta povreda potpuno ili djelomično ispravljena. Ta je mogućnost dostupna samo u navedene svrhe. Ta mogućnost nije dostupna, primjerice, u pogledu izuzeća od načela ([1]) ili u odnosu na navode o primjerenosti sustava zaštite privatnosti.

B. **Dostupna pravna sredstva**

U skladu s ovom mogućnošću arbitraže, Odbor za sustav zaštite privatnosti (koji se sastoji od jednog ili tri arbitra, kako su dogovorile stranke) ima ovlasti odrediti pojedinačnu nenovčanu pravičnu naknadu (poput pristupa, ispravka, brisanja ili vraćanja predmetnih podataka osobe) koji su nužni za ispravak kršenja načela samo u pogledu pojedinca. To su jedine ovlasti arbiražnog odbora u pogledu pravnih sredstava. Kada razmatra pravne lijekove, arbitražni odbor mora uzeti u obzir druge pravne lijekove koji su već određeni drugim mehanizmima u okviru sustava zaštite privatnosti. Nisu dostupne odštete, nadoknade troškova, naknade ili druga pravna sredstva. Svaka stranka snosi vlastite troškove odvjetnika.

C. **Zahtjevi u postupku prije arbitraže**

Osoba koja odluči iskoristiti ovu mogućnost arbitraže mora poduzeti sljedeće korake prije podnošenja zahtjeva za arbitražu: 1. obavijestiti organizaciju o navodnoj povredi i dati joj priliku da riješi pitanje u roku iz odjeljka III. točke 11. podtočke (d) i. Načela; 2. iskoristiti neovisan mehanizam pravne zaštite u skladu s Načelima, koji je besplatan za pojedince; i 3. obratiti se Ministarstvu trgovine posredstvom svog nadležnog tijela za zaštitu podataka i omogućiti Ministarstvu trgovine da uloži najveće napore u besplatno rješavanje pitanja u rokovima iz dopisa Uprave za međunarodnu trgovinu Ministarstva trgovine.

Mogućnost arbitraže ne može se iskoristiti ako je navodna povreda načela (1) prethodno bila predmetom obvezujuće arbitraže; (2) bila predmetom konačne presude donesene u sudskom postupku čiji je ta osoba bila stranka ili (3) stranke su ju prethodno riješile. Nadalje, ta se mogućnost ne može iskoristiti ako tijelo EU-a za zaštitu podataka (1) ima ovlasti u skladu s odjeljkom III. točkom 5 i odjeljkom III. točkom 9. Načela ili (2) ima ovlasti riješiti navodnu povredu izravno s organizacijom. Nadležnost tijela za zaštitu podataka za rješavanje iste pritužbe protiv voditelja obrade podataka EU-a ne isključuje mogućnost uporabe ove mogućnosti arbitraže protiv druge pravne osobe koju ne obvezuje nadležnost tijela za zaštitu podataka.

D. **Obvezujuća priroda odluka**

Odluka o uporabi ove obvezujuće mogućnosti arbitraže u potpunosti je dobrovoljna Arbitražna odluka obvezujuća je za sve stranke u arbitraži. Kada iskoristi mogućnost arbitraže osoba se odriče mogućnosti traženja pravne zaštite za istu navodnu povredu u drugom forumu, osim ako se nenovčanim pravnim lijekom ne ostvaruje potpuna nadoknada za navodnu povredu, iskorištavanje arbitraže ne isključuje zahtjev za odštetu koji se inače može podnijeti sudu.

([1]) Odjeljak I. točka 5. načela.

E. **Preispitivanje i provedba**

Osobe i organizacije u sustavu zaštite privatnosti moći će tražiti sudsko preispitivanje i provedbu arbitražnih odluka u skladu sa zakonodavstvom EU-a, odnosno Saveznim zakonom o arbitraži ([1]). Takvi se postupci mogu pokrenuti pred saveznim okružnim sudom koji je mjesno nadležan za glavno sjedište organizacije su sustavu zaštite privatnosti.

Svrha je ove mogućnosti arbitraže rješavanje pojedinačnih sporova i arbitražne odluke ne moraju služiti kao uvjerljivi ili obvezujući presedan u pitanjima povezanima s drugim strankama, uključujući u budućim arbitražnim postupcima ili na sudovima EU-a ili SAD-a ili u postupcima FTC-a.

F. **Arbitražni odbor**

Stranke biraju arbitre s popisa arbitara o kojem je riječ u nastavku.

U skladu s primjenjivim pravom, američko Ministarstvo trgovine i Europska komisija sastavit će popis od najmanje 20 arbitara koji se biraju na temelju neovisnosti, integriteta i stručnosti. Na taj se postupak primjenjuje sljedeće:

Arbitri:

1. ostaju na popisu 3 godine, osim u iznimnim okolnostima ili iz iznimnih razloga, i to se može obnoviti na dodatno razdoblje od 3 godine;

2. ne primaju upute nijedne stranke ni organizacije u sustavu zaštite privatnosti, ili od EU-a, bilo koje države članice ili drugog državnog tijela, javnog tijela ili izvršnog tijela i nisu s njima povezani i

3. moraju biti odvjetnici u SAD-u i stručnjaci za pravo zaštite privatnosti SAD-a te za pravo EU-a za zaštitu podataka.

G. **Arbitražni postupci**

U skladu s primjenjivim pravom, u roku od 6 mjeseci od donošenja odluke o odgovarajućoj zaštiti, Ministarstvo trgovine i Europska komisija slažu se da će se postupci pred Vijećem sustava za zaštitu privatnosti primjenjivati postojeći, uspostavljeni arbitražni postupci SAD-a (poput AAA-a ili JAMS-a), podložno sljedećim uvjetima:

1. Osoba može pokrenuti obvezujući arbitražni postupak u skladu sa prethodno navedenim zahtjevima u vezi s postupkom prije pokretanja arbitražnog postupka „obavješćivanjem" organizaciji. Obavijest sadržava sažetak koraka poduzetih u skladu s odlomkom C za rješavanje potraživanja, opis navodne povrede i, ako osoba tako želi, prateće dokumente i materijale i/ili raspravu o pravu koje se odnosi na navodno potraživanje.

([1]) U poglavlju 2. Saveznog zakona o arbitraži (dalje u tekstu „FAA") predviđeno je da se na „sporazum o arbitraži ili arbitražnu odluku koji su posljedica pravnog odnosa, neovisno o tome je li riječ o ugovornom odnosu, koji se smatra poslovnim, među ostalim transakciju, ugovor ili sporazum opisan u [odjeljku FAA-a] primjenjuje Konvencija [o priznavanju i izvršenju stranih arbitražnih odluka od 10. lipnja, 1958., 21 U.S.T. 2519, T.I.A.S. br. 6997 (dalje u tekstu ‚Konvencija iz New Yorka')]." 9 U.S.C. članak 202. U FAA-u je dalje predviđeno da „sporazum ili odluka proizašli iz tog odnosa koji su sklopljeni između državljana Sjedinjenih Američkih Država smatraju se obuhvaćenim Konvencijom iz New Yorka osim ako taj odnos uključuje imovinu koja se nalazi u inozemstvu, ako je njime predviđeno obavljanje ili izvršenje u inozemstvu ili ako ima neki drugi razumni odnos s jednom ili više stranih država." *Id.* U skladu s poglavljem 2. „svaka stranka u arbitraži može podnijeti zahtjev bilo kojem sudu koji je nadležan u skladu s ovim poglavljem da donese odluku kojom se potvrđuje odluka protiv druge stranke u arbitraži. Sud potvrđuje odluku osim ako utvrdi jednu od osnova za odbijanje ili odgađanje priznavanja ili izvršenja odluke navedenu u predmetnoj Konvenciji iz [New Yorka]." Id., članak 207. točka (e). U poglavlju 2. dalje je predviđeno da „okružni sudovi Sjedinjenih Država nadležni su za mjeru ili postupak [u skladu s Konvencijom iz New Yorka], neovisno o spornom iznosu." Id., članak 203.
U poglavlju 2. također je propisano da se „poglavlje 1. primjenjuje na mjere i postupke pokrenute u skladu s ovim poglavljem ako to poglavlje nije u suprotnosti s ovim poglavljem ili Konvencijom iz [New Yorka] kako su ju ratificirale Sjedinjene Američke Države." Id., članak 208. S druge strane, u poglavlju 1. predviđeno je da „pisana odredba u ugovoru kao dokaz poslovne transakcije za rješavanje spora arbitražom koja proizlazi iz takvog ugovora ili transakcije ili odbijanja za izvršavanje cijelog ili dijela, ili pisani sporazum o pokretanju arbitraže zbog takvog ugovora, transakcije ili odbijanja, važeća je, neponištiva i izvršiva, osim na osnovama koje postoje u zakonu ili pravnom lijeku za raskid ugovora." Id., članak 2. točka (e). U poglavlju 1. dalje je predviđeno da „svaka stranka u arbitraži može se od navedenog suda tražiti nalog o potvrdi odluke i sud mora potom odobriti takav nalog osim ako je odluka nevažeća, izmijenjena ili ispravljena kako je navedeno u odjeljcima 10. i 11. FAA-a". Id., članak 9.

2. Razvijaju se postupci kojima će se osigurati da osoba ne može primijeniti dvostruku pravnu zaštitu ili provoditi dvostruke postupke za istu navodnu povredu.

3. Postupak FTC-a može se provoditi usporedno s arbitražnim postupkom.

4. U tim arbitražnim postupcima ne može sudjelovati niti jedan predstavnik SAD-a, EU-a ili bilo koje države članice EU-a ili nekog drugog državnog, javnog ili izvršnog tijela osim na zahtjev osobe iz EU-a, tijela za zaštitu podataka iz EU-a mogu pružiti pomoć samo s pripremom obavijesti, ali ta tijela ne smiju imati pristup otkrivanju ili drugim materijalima povezanim s arbitražnim postupkom.

5. Arbitraža se provodi u Sjedinjenim Američkim Državama i osoba može izabrati sudjelovanje videokonferencijom ili telefonom, koje mu se osigurava bez dodatnog troška. Osobna nazočnost neće biti obavezna.

6. Jezik arbitraže bit će engleski, osim ako stranke dogovore drugačije. Na razuman zahtjev i ovisno o tome zastupa li osobu odvjetnik, tumačenje na arbitražnoj raspravi i prijevod materijala za arbitražu osiguravaju se besplatno, osim ako odbor odluči da bi, s obzirom na okolnosti određene arbitraže, time nastali neopravdani ili nerazmjerni troškovi.

7. Materijali dostavljeni arbitrima smatraju se povjerljivima i upotrebljavat će se samo u vezi s arbitražnim postupkom.

8. Podatke je moguće otkriti određenoj osobi, ako je potrebno i stranke to otkrivanje drže u tajnosti i upotrebljavaju samo u vezi s arbitražom.

9. Arbitraže se dovršavaju u roku od 90 dana od obavješćivanja predmetnoj organizaciji, osim ako su stranke dogovorile drugačije.

H. **Troškovi**

Arbitri poduzimaju razumne korake kako bi troškove ili naknade za arbitražu sveli na minimum.

U skladu s primjenjivim pravom, Ministarstvo trgovine pomaže s uspostavom fonda u koji će organizacije sudionice u sustavu zaštite privatnosti svake godine morati uplaćivati godišnji doprinos koji se djelomično temelji na veličini organizacije i kojim će biti obuhvaćeni troškovi arbitraže, među ostalim naknade za arbitre, do najvećeg iznosa („gornje granice”), u dogovoru s Europskom komisijom. Fondom upravlja treća strana koja redovito izvješćuje o radu fonda. U okviru godišnjeg preispitivanja Ministarstvo trgovine i Europska komisija preispituju funkcioniranje fonda, među ostalim potrebu za prilagodbom iznosa doprinosa i uzimaju u obzir, među ostalim, broj provedenih arbitražnih postupaka i troškove i rokove provođenja arbitraže te potvrđuju da se organizacijama u sustavu zaštite privatnosti neće nametati pretjerano financijsko opterećenje. Troškovi odvjetnika nisu obuhvaćeni ovom odredbom ni bilo kojim fondom iz ove odredbe.

PRILOG II.

NAČELA OKVIRA EUROPSKO-AMERIČKOG SUSTAVA ZAŠTITE PRIVATNOSTI KOJA JE IZDALO MINISTARSTVO TRGOVINE SAD-a

I. PREGLED

1. Iako Sjedinjene Američke Države i Europska unija imaju isti cilj povećanja zaštite privatnosti, njihov se pristup privatnosti razlikuje. Sjedinjene Američke Države koriste se sektorskim pristupom koji se oslanja na kombinaciju zakonodavstva, propisa i samoregulacije. S obzirom na te razlike te kako bi se organizacijama u Sjedinjenim Američkim Državama osigurao pouzdan mehanizam za prijenos osobnih podataka iz Europske unije u Sjedinjene Američke Države uz osiguravanje da osobe iz EU-a čiji se podaci obrađuju uživaju učinkovite zaštitne mjere i zaštitu predviđenu u europskom zakonodavstvu u pogledu obrade njihovih osobnih podataka pri prijenosu u države izvan EU-a, Ministarstvo trgovine izdaje ova načela sustava zaštite privatnosti, uključujući Dodatna načela (dalje u tekstu zajedno „načela") u skladu sa svojom zakonskom ovlasti poticanja, promicanja i razvoja međunarodne trgovine (15 U.S.C., članak 1512.). Načela su izrađena u dogovoru s Europskom komisijom, gospodarstvenicima i ostalim dionicima kako bi se olakšala trgovina između Sjedinjenih Američkih Država i Europske unije. Načela su namijenjena isključivo organizacijama SAD-a koje primaju osobne podatke iz Europske unije kako bi se mogle kvalificirati za sudjelovanje u sustavu zaštite privatnosti i iskoristiti odluku Europske komisije o odgovarajućoj zaštiti ([1]). Načela ne utječu na primjenu nacionalnih odredbi o provedbi Direktive 95/46/EZ (dalje u tekstu: Direktiva) koja se primjenjuju na obradu osobnih podataka u državama članicama. Načela ne ograničavaju obveze privatnosti koje se inače primjenjuju u skladu sa zakonodavstvom SAD-a.

2. Da bi mogla sudjelovati u sustavu zaštite privatnosti radi prijenosa osobnih podataka iz EU-a, organizacija mora obaviti samocertificiranje pridržavanja načela pri Ministarstvu trgovine (ili tijelu koje je ono za to odredilo) (dalje u tekstu: Ministarstvo). Iako organizacije mogu dobrovoljno odlučiti hoće li sudjelovati u sustavu zaštite privatnosti, u slučaju sudjelovanja usklađenost je obavezna: organizacije koje obave samoscertificiranje pred Ministarstvom i javno izjave da se obvezuju poštovati načela, moraju ih u potpunosti poštovati. Da bi postala članicom sustava zaštite privatnosti, organizacija se (a) mora podvrgnuti istražnim i provedbenim ovlastima Savezne trgovinske komisije (dalje u tekstu: FTC), Ministarstva prometa ili drugog zakonskog tijela koje će osigurati poštovanje načela *(druga zakonska tijela SAD-a koja je EU priznao mogu se u budućnosti uključiti kao prilog)*; (b) javno izjaviti da se obvezuje poštovati načela; (c) javno izjaviti da su njihove politike zaštite privatnosti u skladu s tim načelima i (d) potpuno ih provesti. Organizacija koja ne poštuje načela može biti kažnjena u skladu s odjeljkom 5. Zakona o Saveznoj trgovinskoj komisiji kojim se zabranjuje takvo nepošteno i prijevarno postupanje u trgovini ili koje utječe na trgovinu (15 U.S.C. članak 45. točka (a)) ili drugim zakonima ili propisima kojima se zabranjuju takva djela.

3. Ministarstvo trgovine vodit će i objavljivati obvezujući popis organizacija SAD-a koje su se samocertificirale pri Ministarstvu i opredijelile se za poštovanje načela (dalje u tekstu: Popis organizacija u sustavu zaštite privatnosti). Pogodnosti u okviru sustava zaštite privatnosti zajamčene su od datuma kada Ministarstvo uvrsti organizaciju na Popis organizacija u sustavu zaštite privatnosti. Ministarstvo uklanja organizaciju s Popisa organizacija u sustavu zaštite privatnosti ako se ona dobrovoljno povuče iz sustava zaštite privatnosti ili ne obavi godišnje ponovno certificiranje pri Ministarstvu. Uklanjanje organizacije s Popisa organizacija u sustavu zaštite privatnosti znači da ona više ne može uživati pogodnosti na temelju odluke Komisije o odgovarajućoj zaštiti za primanje osobnih podataka iz EU-a. Organizacija mora nastaviti primjenjivati načela na osobne podatke koje je zaprimila dok je sudjelovala u sustavu zaštite privatnosti, a Ministarstvu svake godine potvrditi svoju obvezu da će to činiti, sve dok čuva takve podatke; u protivnom organizacija mora vratiti ili izbrisati podatke ili osigurati „odgovarajuću" zaštitu podataka drugim ovlaštenim sredstvima. Ministarstvo će s Popisa organizacija u sustavu zaštite privatnosti ukloniti i one organizacije koje ustrajno ne poštuju načela; te organizacije ne ispunjavaju uvjete za korištenje pogodnostima iz sustava zaštite privatnosti te moraju vratiti ili izbrisati osobne podatke koje su zaprimile u okviru sustava zaštite privatnosti.

4. Ministarstvo će voditi i objavljivati pouzdanu evidenciju američkih organizacija koje su se prethodno samocertificirale pred Ministarstvom, ali su uklonjene s Popisa organizacija u sustavu zaštite privatnosti. Ministarstvo te organizacije jasno upozorava da ne sudjeluju u sustavu zaštite privatnosti; da uklanjanje s Popisa organizacija u sustavu zaštite privatnosti znači da te organizacije ne mogu tvrditi da poštuju načela sustava zaštite privatnosti i da moraju izbjegavati tvrdnje ili prijevarnu praksu koja upućuje na to da sudjeluju u sustavu zaštite privatnosti; i da takve organizacije više nemaju pravo na pogodnosti iz odluke Europske komisije o odgovarajućoj zaštiti na temelju koje bi mogle primati osobne podatke iz EU-a. Organizacija koja nastavi tvrditi da sudjeluje u sustavu zaštite privatnosti ili daje druge lažne izjave povezane sa sustavom zaštite privatnosti nakon što je uklonjena s

([1]) Ako odluka Komisije o primjerenosti zaštite koju pružaju europsko-američki sustav zaštite privatnosti primjenjuje na Island, Lihtenštajn i Norvešku, paket o sustavu zaštite privatnosti obuhvatit će Europsku uniju te tri navedene zemlje. Stoga se smatra da upućivanja na EU i države članice uključuju Island, Lihtenštajn i Norvešku.

Popisa organizacija u sustavu zaštite privatnosti može biti predmetom izvršnih mjera FTC-a, Ministarstva prometa ili drugih izvrših tijela.

5. Pridržavanje tih načela može biti ograničeno: (a) u mjeri potrebnoj da se ispune zahtjevi u pogledu nacionalne sigurnosti, javnog interesa ili kaznenog progona; (b) zakonom, vladinim propisom ili sudskom praksom koji proizvode proturječne obveze ili izričita ovlaštenja, ako pri korištenju takvim ovlaštenjem organizacija može dokazati da je njezino nepoštovanje načela ograničeno u mjeri potrebnoj da se ostvare viši legitimni interesi koje podupire takvo ovlaštenje; ili (c) ako Direktiva ili nacionalno pravo države članice predviđaju iznimke ili odstupanja, uz uvjet da se takve iznimke ili odstupanja primjenjuju u sličnim kontekstima. U skladu s ciljem povećanja zaštite privatnosti organizacije trebaju nastojati u potpunosti i transparentno provoditi ova načela, uključujući i tako da u svojim postupcima zaštite privatnosti navode kada će se redovito primjenjivati iznimke od načela, dopuštene u prethodno opisanom slučaju (b). Iz istog razloga, ako je mogućnost odabira dopuštena prema načelima i/ili zakonodavstvu SAD-a, očekuje se da se organizacije odluče za veću zaštitu tamo gdje je moguće.

6. Kada postanu članice sustava zaštite privatnosti, organizacije imaju obvezu primjenjivati načela na sve osobne podatke prenesene u okviru tog sustava. Organizacija koja želi proširiti koristi sustava zaštite privatnosti na osobne podatke o ljudskim resursima koje se prenose iz EU-a za uporabu u kontekstu radnog odnosa, mora to navesti kada se bude obvezivala Ministarstvu trgovine (ili njegovom ovlaštenom predstavniku) s obzirom na načela, te mora ispuniti zahtjeve iz Dodatnog načela o samocertificiranju.

7. Zakonodavstvo SAD-a primjenjivat će se na pitanja tumačenja i usklađenosti s načelima i relevantne politike zaštite privatnosti organizacija iz sustava zaštite privatnosti, osim ako se organizacije nisu obvezale na suradnju s europskim tijelima za zaštitu podataka. Ako nije navedeno drugačije, sve odredbe načela primjenjuju se tamo gdje su relevantna.

8. Definicije:

   a. „osobni podaci" i „osobne informacije" su podaci o određenom pojedincu ili pojedincu kojeg se može odrediti, obuhvaćeni područjem primjene Direktive, koje je iz Europske unije primila organizacija u SAD-u i pohranila ih u bilo kojem obliku.

   b. „obrada" osobnih podataka znači bilo koja operacija ili skup operacija koje se izvršavaju nad osobnim podacima, neovisno o tome je li automatiziranim sredstvima, poput prikupljanja, evidentiranja, organizacije, pohrane, prilagodbe ili izmjene, povlačenja, savjetovanja, uporabe, otkrivanja ili širenja te brisanja ili uništavanja.

   c. „voditelj obrade" znači osoba ili organizacija koja sama ili s drugima utvrđuje svrhu obrade i sredstva za obradu osobnih podataka.

9. Načela stupaju na snagu na dan konačnog odobrenja zaključka Europske komisije o odgovarajućoj zaštiti.

II. NAČELA

1. **Obavješćivanje**

   a. Organizacija mora obavijestiti osobe o sljedećem:

      i. da sudjeluje u sustavu zaštite privatnosti i i mora navesti poveznicu na Popis organizacija u sustavu zaštite privatnosti i *web*-mjesto na kojem se on nalazi,

      ii. vrstama osobnim podataka koje prikuplja i, prema potrebi, o subjektima ili podružnicama organizacije koje također poštuju načela,

iii. da se obvezala sve osobne podatke zaprimljene od EU-a u okviru sustava zaštite privatnosti obrađivati u skladu s načelima,

iv. svrhama za koje prikuplja njihove osobne podatke i za što ih upotrebljava,

v. kako joj se obratiti s upitima ili pritužbama, uključujući o nadležnom tijelu u EU-u koje može odgovoriti na takve upite ili pritužbe,

vi. o vrsti i identitetu trećih strana kojima otkriva osobne podatke i u koje svrhe to čini,

vii. pravu osoba da pristupe svojim osobnim podacima,

viii. izboru i načinima koji su osobama čiji se podaci obrađuju na raspolaganju za ograničavanje uporabe i otkrivanja njihovih osobnih podataka,

ix. neovisnom tijelu za rješavanje sporova koje je imenovano za rješavanje pritužbi i besplatnom pristupu pravnoj zaštiti osoba i je li riječ o sljedećem: 1. odbor koji su uspostavila tijela za zaštitu podataka, 2. pružatelju usluga alternativnog rješavanja sporova sa sjedištem u EU-u ili 3. pružatelju usluga alternativnog rješavanja sporova sa sjedištem u Sjedinjenim Američkim Državama,

x. da podliježe istražnim i provedbenim ovlastima FTC-a, Ministarstva prometa ili drugog ovlaštenog zakonskog tijela SAD-a,

xi. mogućnosti osobe da u određenim okolnostima zatraži obvezujuću arbitražu,

xii. zahtjevu za otkrivanje osobnih podataka kao odgovorU na zakonite zahtjeve javnih tijela, uključujući za ispunjivanje nacionalnih sigurnosnih zahtjeva ili zahtjeva provedbe zakona i

xiii. svojoj odgovornosti u slučajevima daljnjeg prijenosa trećim stranama.

b. Ova obavijest mora biti sastavljena jasnim i razumljivim jezikom kada se od osoba prvi put zatraži da daju osobne podatke organizaciji ili čim prije nakon toga, ali u svakom slučaju prije nego organizacija upotrijebi takve informacije u neku drugu svrhu osim one za koju ih je prvotno prikupila ili obradila organizacija koja je izvršila prijenos ili prije nego što ih po prvi put otkrije trećoj osobi.

2. **Mogućnost izbora**

a. Organizacija mora osobama ponuditi mogućnost da odaberu (odustanu) hoće li se njihovi osobni podaci moći i. otkriti trećoj osobi ili ii. koristiti u svrhu koja nije u skladu sa svrhom za koju su izvorno prikupljeni ili za koju je pojedinac naknadno dao odobrenje. Osobama moraju biti ponuđeni jasni i očigledni i dostupni mehanizmi odabira.

b. Odstupajući od prethodnog stavka, nije potrebno ponuditi mogućnost odabira kad se podaci otkrivaju trećoj osobi koja kao posrednik izvršava posao (poslove) u ime i prema uputama organizacije. Međutim, organizacija uvijek sklapa ugovor s posrednikom.

c. Kod osjetljivih informacija (tj. osobnih podataka o medicinskom ili zdravstvenom stanju, rasi ili etničkom podrijetlu, političkim stavovima, vjerskim ili filozofskim uvjerenjima, članstvu u sindikatu ili podataka o spolnom životu pojedinca), organizacije moraju pribaviti izričitu suglasnost (pristanak) osoba ako će se te informacije i. otkriti trećoj osobi ili ii. koristiti u neku drugu svrhu osim one za koju su prvotno prikupljene ili za koju je osoba naknadno dala odobrenje koristeći mogućnost odabira. Nadalje, organizacija treba smatrati osjetljivima one informacije koje je primila od treće osobe kada ih treća osoba smatra osjetljivima i odnosi se prema njima kao takvima.

3. **Odgovornost za daljnji prijenos**

a. Da bi mogle prenijeti osobne podatke trećoj strani koja djeluje kao voditelj obrade, organizacije moraju postupiti u skladu s načelima obavješćivanja i izbora. Organizacije moraju isto sklopiti ugovor s trećom stranom koja djeluje kao voditelj obrade u kojem je propisano da se takvi podaci mogu obrađivati samo u ograničene i posebno navedene svrhe u skladu sa suglasnošću osobe te da će primatelj osigurati jednaku razinu zaštite kao i načela te da će obavijestiti organizaciju ako odluči da više ne može ispunjavati svoje obveze. Ugovor omogućuje da ako se to utvrdi, obrada koju provodi treća strana koja djeluje kao voditelj obrade prestaje ili voditelj obrade poduzima druge razumne i odgovarajuće korake za rješavanje te situacije.

b. Da bi mogle prenijeti osobne podatke trećoj stranci koja djeluje kao posrednik, organizacije moraju učiniti sljedeće: i. prenositi takve podatke samo u ograničene i posebne svrhe; ii. provjeriti da posrednik ima obvezu pružiti najmanje istu razinu zaštite kao i načela; iii. poduzeti razumne i primjerene korake kako bi osigurale da posrednik učinkovito obradi osobne podatke prenesene na način koji je u skladu s obvezama koje organizacija ima u skladu s načelima; iv. zahtijevati da posrednik obavijesti organizaciju ako odluči da više ne može ispunjavati svoje obveze pružanja jednake razine zaštite u skladu s načelima; iv. na temelju obavijesti poduzeti razumne i odgovarajuće korake za zaustavljanje i ispravljane neovlaštene obrade; i vi. Ministarstvu na zahtjev dostaviti sažetak ili reprezentativnu presliku relevantnih odredaba o zaštiti privatnosti svog ugovora s tim posrednikom.

4. **Sigurnost**

a. Organizacije koje stvaraju, čuvaju upotrebljavaju ili šire osobne podatke moraju poduzeti razumne i odgovarajuće mjere kako bi zaštitile te podatke o gubitka, zlouporabe i neovlaštenog pristupa, otkrivanja, izmjene i uništenja, uzimajući u obzir rizike povezane s obradom osobnih podataka i njihovom prirodom.

5. **Cjelovitost podataka i ograničenje svrhe**

a. U skladu s načelima, osobni podaci moraju biti ograničeni na podatke koji su relevantni za svrhu obrade ([1]). Organizacija ne može obrađivati osobne podatke na način koji nije u skladu s namjenama za koje su prikupljeni ili za koje je pojedinac naknadno dao odobrenje. U mjeri u kojoj je to potrebno za tu namjenu, organizacija treba poduzeti odgovarajuće korake da podaci budu pouzdani za namjeravano korištenje, točni, potpuni i ažurirani. Organizacija mora poštovati načela sve dok čuva takve podatke.

b. Podaci se mogu zadržati u obliku kojima se ta osoba identificira ili koji omogućuje njezinu identifikaciju ([2]) samo dok služe svrsi obrade u okviru značenja točke 5 podtočke (a). Ta obveza ne sprečava organizaciju od obrade osobnih podataka u duljim razdobljima, ali samo u onoj mjeri u kojoj takva obrada služi svrsi pohranjivanja u javnom interesu, novinarstvu, književnim i umjetničkim svrhama, u svrhe povijesnih i znanstvenih istraživanja te u svrhu statističke analize. U tim slučajevima takva je obrada podložna drugim načelima i odredbama okvira. Organizacije trebaju poduzeti razmne i odgovarajuće mjere kako bi se uskladile s tom odredbom.

6. **Pristup**

a. Osobe moraju imati pristup svojim osobnim podacima koje organizacija čuva, te ih moći ispraviti, promijeniti ili obrisati ako su netočni ili su obrađeni protivno načelima, osim ako teret ili trošak omogućavanja pristupa ne bili razmjeni riziku za privatnost osobe u predmetnom slučaju, ili ako bi bila povrijeđena prava drugih osoba.

([1]) Ovisno o okolnostima, primjeri namjena usklađene obrade mogu uključivati primjere u kojima se u razumnoj mjeri služi odnosima s potrošačima, usklađenosti i pravnim aspektima, reviziji, sigurnosti i sprečavanju prijevare, očuvanja ili obrane zakonskih prava organizacije ili druge namjene u skladu s očekivanjima razumne osobe s obzirom na kontekst prikupljanja podataka.

([2]) Ako u tom kontekstu i s obzirom na sredstva identificiranja koja bi se mogla upotrijebiti (uzimajući u obzir, među ostalim, troškove i vrijeme koje je potrebno za identifikaciju i tehnologiju koja je dostupna u vrijeme obrade) i oblik u kojem se čuvaju podaci, osobu može identificirati organizacija ili treća strana ako ima pristup podacima, tada se osobu može identificirati.

7. **Pravna zaštita, provedba i odgovornost**

a. Učinkovita zaštita privatnosti mora uključivati pouzdane mehanizme kojima se osigurava poštovanje načela, pravna zaštita osoba na koje utječe nepridržavanje načela, te posljedice za organizaciju kad ne poštuje načela. Takvi mehanizmi moraju uključivati barem sljedeće:

i. pristupačne neovisne mehanizme pravne zaštite na temelju kojih se pritužbe i sporovi svake osobe istražuju i brzo rješavaju bez troška za osobu te upućivanjem na načela i odštetu koja se dodjeljuje ako je tako predviđeno privatnim pravom ili inicijativama iz privatnog sektora;

ii. postupke praćenja kojima se provjerava jesu li potvrde i navodi koje poduzeća daju o svojim praksama u pogledu privatnosti istinite i provodi li se praksa zaštite privatnosti kako je navedeno i, posebno, u pogledu slučajeva neusklađenosti s načelima; i

iii. obveze rješevanja problema koji proizlaze iz nepoštovanja načela od strane organizacija koje objavljuju da ih se pridržavaju i posljedice za takve organizacije. Sankcije moraju biti dovoljno stroge da bi ih se organizacije pridržavale.

b. Organizacije i njihovi odabrani neovisni mehanizmi pravne zaštite žurno će odgovarati na upite i zahtjeve Ministarstva za informacije povezane sa sustavom zaštite privatnosti. Sve organizacije moraju spremno odgovarati na pritužbe u pogledu poštovanja načela koje su joj uputila nadležna tijela država članica posredstvom Ministarstva. Organizacije koje su odlučile surađivati s nadležnim tijelima za zaštitu podataka, među ostalim organizacije koje obrađuju podatke o ljudskim resursima moraju izravno odgovoriti takvim tijelima u vezi s istragom i rješavanjem pritužbi.

c. Organizacije su dužne provoditi arbitražu i postupati u skladu s uvjetima iz Priloga I. ako je osoba zatražila obvezujuću arbitražu dostavljanjem obavijesti predmetnoj organizaciji i u skladu s postupcima i podložno uvjetima iz Priloga I.

d. U kontekstu daljnjeg prijenosa, organizacija u okviru sustava zaštite privatnosti odgovorna je za obradu podataka zaprimljenih u okviru sustava zaštite privatnosti koje potom prenosi trećoj strani koja postupa kao posrednik u njezino ime. Organizacija u okviru sustava zaštite privatnosti odgovorna je u skladu s načelima ako njezin posrednik obrađuje takve osobne podatke na način koji nije u skladu s načelima, osim ako organizacija dokaže da nije odgovorna za događaj kojim je uzrokovana šteta.

e. Ako organizacija zbog nepoštovanja načela postane predmetom FTC-a ili sudskog naloga, ona objavljuje sve dijelove svojeg izvješća u poštovanju načela ili izvješća o ocjeni povezana sa sustavom zaštite privatnosti koja su dostavljena FTC-u u mjeri u kojoj je to u skladu sa zahtjevima povjerljivosti. Ministarstvo je uspostavilo posebnu točku za kontakt za nadležna tijela za zaštitu podataka u slučaju problema sa poštovanjem načela organizacija u sustavu zaštite privatnosti. FTC daje prednost slučajevima nepoštovanja načela koje su uputili Ministarstvo i nadležna tijela država članica EU-a i pravovremeno razmjenjuje informacije o upućenim slučajevima s nadležnim tijelima koja su uputila slučaj, podložno postojećim ograničenjima povezanima s povjerljivošću.

III. DODATNA NAČELA

1. **Osjetljivi podaci**

a. Organizacija nije dužna pribaviti izričitu suglasnost (pristanak) u pogledu osjetljivih podataka ako je obrada:

i. od životnog interesa za osobu čiji se podaci obrađuju ili neku drugu osobu;

ii. potrebna za ostvarivanje zakonskih prava ili obrane;

iii. potrebna da bi se pružila medicinska skrb ili dijagnoza;

iv. se vrši tijekom zakonitih aktivnosti zaklade, udruge ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem i uz uvjet da se obrada odnosi isključivo na članove tog tijela ili osobe koje imaju redovne kontakte s istom u te svrhe, te da se podaci ne otkriju trećoj osobi bez privole osoba čiji se podaci obrađuju;

v. potrebna da organizacija ispuni svoje obveze u području radnog prava ili

vi. vezana za podatke koje je očigledno objavio pojedinac.

2. **Novinarska izuzeća**

a. S obzirom na zaštitu slobode tiska u američkom Ustavu i izuzeće iz Direktive koje se odnosi na novinarske materijale, ako se prava na slobodu tiska iz prvog amandmana Ustava SAD-a kose s interesima zaštite privatnosti, mora se uspostaviti ravnoteža tih interesa na temelju prvog amandmana s obzirom na aktivnosti državljana ili organizacija iz SAD-a.

b. Osobni podaci koji se prikupljaju radi objavljivanja, emitiranja ili ostalih oblika javne objave novinarskih materijala, bez obzira koriste li se ili ne, kao i informacije pronađene u prethodno objavljenom materijalu iz medijskih arhiva, ne podliježu zahtjevima načela sustava zaštite privatnosti.

3. **Sekundarna odgovornost**

a. Pružatelji internetskih usluga (ISP), telekomunikacijski operateri ili ostale organizacije ne snose odgovornost u skladu s načelima sustava zaštite privatnosti ako u ime neke druge organizacije samo prenose, usmjeravaju, prespajaju ili privremeno pohranjuju informacije. Kao što je slučaj sa samom Direktivom, sustavom zaštite privatnosti ne uzrokuje se sekundarna odgovornost. U onoj mjeri u kojoj organizacija djeluje samo kao posrednik podataka koje prenose treće osobe i ne određuje svrhu i sredstva obrade tih osobnih podataka, ona nije odgovorna.

4. **Obavljanje dubinske analize i provođenje revizija**

a. Djelatnosti revizora i investicijskih banaka mogu uključivati obradu osobnih podataka bez pristanka ili znanja pojedinca. To je u skladu s načelima obavješćivanja, izbora i pristupa pod uvjetima opisanima u nastavku.

b. Javne korporacije i poduzeća s malim brojem dioničara, uključujući organizacije u sustavu zaštite privatnosti, redovito podliježu reviziji. Takve revizije, posebno one kojima se istražuju moguće povrede, mogle bi se ugroziti u slučaju privremene objave. Slično tomu, organizacija u sustavu zaštite privatnosti koja sudjeluje u mogućem spajanju ili preuzimanju morat će obaviti dubinski pregled ili biti predmetom dubinskog pregleda. To često podrazumijeva prikupljanje i obradu osobnih podataka, na primjer informacija o direktorima i ostalom ključnom osoblju. Preranim otkrivanjem mogla bi se ugroziti transakcija ili se čak prekršiti primjenjivi propisi o vrijednosnim papirima. Investicijski bankari i odvjetnici koji sudjeluju u postupku dubinskog pregleda ili odvjetnici mogu obrađivati informacije bez znanja pojedinca samo u onoj mjeri i u onom razdoblju koje je potrebno da se zadovolje zahtjevi zakonskog ili javnog interesa i u ostalim okolnostima u kojima bi primjena ovih načela naškodila zakonitim interesima organizacije. Ti zakoniti interesi uključuju nadziranje ispunjuje li trgovačko društvo svoje zakonske obveze i zakonite računovodstvene aktivnosti, te potrebu za tajnošću podatka vezanih za moguća preuzimanja, udruživanja, zajedničke pothvate ili ostale slične transakcije investicijskih bankara ili revizora.

5. **Uloga tijela za zaštitu podataka**

a. Organizacije će ispunjavati svoju obvezu suradnje s europskim tijelima za zaštitu podataka na način opisan u nastavku. Prema sustavu zaštite privatnosti, organizacije iz SAD-a koje primaju osobne podatke iz EU-a moraju se obvezati na primjenu učinkovitih mehanizama u skladu s načelima sustava zaštite privatnosti. Kako je posebno propisano načelom pravne zaštite, provedbe i odgovornosti, organizacije sudionice moraju osigurati sljedeće: (a) ii.pravnu zaštitu osobama na koje se odnose podaci; (a) ii. postupke praćenja radi provjere da su njihove tvrdnje i izjave o praksi zaštite privatnosti istinite; i (a) iii. obveze rješavanja problema koji proizlaze iz nepoštovanja načela i posljedica za takve organizacije. Organizacija može zadovoljiti točku (a) podtočke i. i iii. načela pravne zaštite, provedbe i odgovornosti, ako zadovoljava ovdje navedene zahtjeve za suradnju s tijelima za zaštitu podataka.

b. Organizacija se može obvezati na suradnju s nadležnim tijelima za zaštitu podataka izjavljujući u svom podnesku o samocertificiranju za sustav za zaštitu privatnosti upućenom Ministarstvu trgovine SAD-a (vidjeti Dodatno načelo o samocertificiranju) da organizacija:

i. svojevoljno pristaje udovoljiti zahtjevima iz točke (a) podtočaka I. i Ii. načela pravne zaštite, provedbe i odgovornosti sustava za zaštitu podataka, obvezujući se na suradnju s tijelima za zaštitu podataka;

ii. surađivat će s tijelima za zaštitu podataka pri istraživanju i rješavanju pritužbi podnesenih u okviru sustava zaštite privatnosti i

iii. postupit će u skladu s bilo kojim savjetom tijela za zaštitu podataka i ako ta tijela smatraju da organizacija treba izvršiti određenu radnju da bi poštovala načela sustava zaštite privatnosti uključujući mjere za zaštitu prava ili naknadu u korist pojedinaca pogođenih nepoštovanjem načela, te da će dati pisanu potvrdu tijelima za zaštitu podataka da je takva radnja poduzeta.

c. Rad odbora tijela za zaštitu podatka

i. Suradnja nadležnih tijela za zaštitu podataka sastojat će se od pružanja informacija i savjeta na sljedeći način:

1. Savjet nadležnog tijela za zaštitu podataka dostavlja se posredstvom neslužbenog odbora tijela za zaštitu podataka organiziranog na razini Europske unije, kojim će se, među ostalim, pridonijeti osiguranju usklađenog i dosljednog pristupa,

2. Odbor će davati savjete predmetnim organizacijama iz SAD-a o neriješenim pritužbama pojedinaca na postupanje s osobnim podacima koji su preneseni iz EU-a u okviru sustava zaštite privatnosti. Ovim savjetom nastoji se osigurati pravilna primjene načela sustava zaštite privatnosti i uključivat će sva pravna sredstva za predmetnu osobu koja tijela za zaštitu podataka smatraju prikladnima,

3. Odbor će ponuditi takav savjet kao odgovor na smjernice uključenih organizacija i/ili pritužbe primljene izravno od pojedinaca protiv organizacija koje su se obvezale surađivati s tijelima za zaštitu podataka u svrhe „sigurne luke", istodobno potičući i prema potrebi pomažući takvim pojedincima da prvo iskoriste interne načine rješavanja pritužbi koje organizacija može ponuditi.

4. Savjet će biti objavljen tek nakon što su obje stranke u sporu imale razumnu mogućnost dati primjedbe i dostaviti dokaze koje žele. Odbor će pokušati dati savjet brzinom koju omogućuje zahtjev provođenja redovnog postupka. U pravilu, odbor će nastojati dati savjet u roku od 60 dana od primitka pritužbe ili upute, a ako je moguće i brže,

5. Odbor će objaviti rezultate svog razmatranja podnijete mu pritužbe, ako to smatra prikladnim,

6. Davanje savjeta putem odbora ne uključuje bilo kakvu odgovornost za odbor ili pojedino tijelo za zaštitu podataka.

ii. Kako je prethodno navedeno, organizacije koje se odluče za ovu mogućnost rješavanja sukoba moraju se obvezati da će poslušati savjet tijela za zaštitu podataka. Ako ga organizacija ne provede u roku od 25 dana od primitka savjeta i ne ponudi prihvatljivo objašnjenje za kašnjenje, odbor će poslati obavijest o svojoj namjeri da uputi slučaj Saveznog trgovinskoj komisiji ili drugom saveznom ili državnom tijelu SAD-a sa zakonskim ovlastima da poduzme provedbene radnje u slučajevima prijevare ili lažne izjave, ili da zaključi da je sporazum o suradnji ozbiljno prekršen te se stoga mora smatrati ništavim. U potonjem slučaju odbor će obavijestiti Ministarstvo trgovine tako da se Popis organizacija u sustavu zaštite privatnosti može prikladno ispraviti. Svako neispunjenje obveze o suradnji s tijelima za zaštitu podataka, kao i nepoštovanje načela sustava zaštite privatnosti bit će kažnjivo kao prijevarno postupanje u skladu s odjeljkom 5. Zakona o FTC-u ili nekom drugom sličnom propisu.

e. Organizacija koja želi da njezinim povlasticama u okviru sustava zaštite privatnosti budu obuhvaćeni podaci o ljudskim resursimama preneseni iz EU-a u kontekstu radnog odnosa mora se u vezi s tim podacima obvezati na suradnju s nadležnim tijelima za zaštitu podataka (vidjeti Dodatno načelo o podacima o ljudskim resursimama).

e. Organizacije koje odaberu ovu mogućnost morat će platiti godišnju naknadu koja će biti namijenjena za pokrivanje operativnih troškova odbora, od njih se može dodatno zatražiti da podmire potrebne troškove prevođenja koji nastaju kada članovi odbora razmatraju upućene slučajeve ili pritužbe protiv njih. Godišnja naknada neće premašivati 500 USD i iznosit će manje za manja trgovačka društva.

6. **Samocertificiranje**

a. Povlastice sustava zaštite privatnosti osiguravaju se od datuma kada je Ministarstvo uvrstilo izjavu organizacije o samocertificiranju na Popis organizacija u sustavu zaštite privatnosti nakon što je utvrdilo da je podnesak potpun.

b. Da bi se mogla samocertificirati u pogledu poštovanja načela sustava zaštite privatnosti, organizacija mora dostaviti Ministarstvu izjavu o samocertificiranju koju je potpisao nadležni službenik u ime organizacije koja se pridružuje sustavu zaštite privatnosti koja sadržava najmanje sljedeće podatke:

i. ime organizacije, adresu, internetsku adresu, broj telefona i telefaksa;

ii. opis aktivnosti organizacije s obzirom na osobne podatke primljene iz EU-a; i

iii. opis politike organizacije u pogledu zaštite privatnosti takvih osobnih podataka, uključujući:

1. ima li organizacija ima javno *web*-mjesto na kojem je dostupna politika zaštite privatnosti ili, ako organizacija nema javno *web*-mjesto, gdje se može pogledati politika za zaštitu privatnosti;

2. datum od kojega se provodi;

3. kontaktni ured za rješavanje pritužbi, zahtjeva za pristup i svih ostalih pitanja povezanih sa sustavom zaštite privatnosti;

4. posebno državno tijelo koje je nadležno rješavati pritužbe protiv organizacije u pogledu mogućih nepoštenih ili prijevarnih praksi i kršenja zakona ili propisa koji uređuju privatnost (i da je to navedeno u načelima ili budućem prilogu načelima),

5. ime programa za zaštitu privatnosti u kojima organizacija sudjeluje kao član;

6. metodu provjere (npr. u kući, treća stranka) (vidjeti Dodatno načelo o provjeri; i

7. neovisni mehanizam pravne zaštite koji je dostupan za istraživanje neriješenih pritužbi.

c. Ako organizacija želi upotrijebiti svoje povlastice u okviru sustava zaštite privatnosti na podatke o ljudskim resursima prenesene iz EU-a za uporabu u kontekstu radnog odnosa, ona to može učiniti ako je zakonsko tijelo navedeno u načelima ili budućem prilogu načelima nadležno za rješavanje pritužbi protiv organizacije koje proizlaze iz obrade podataka o ljudskim resursima. Osim toga, organizacija to mora navesti u svojoj izjavi o samocertificiranju i izjasniti se o svojoj obvezi suradnje s nadležnim tijelom ili tijelima EU-a u skladu s Dodatnim načelima o podacima o ljudskim resursima i ulozi tijela za zaštitu podataka, ako je primjenjivo, te da će postupiti u skladu sa savjetom takvih nadležnih tijela. Organizacija mora dostaviti Ministarstvu preslik svoje politike zaštite privatnosti u pogledu podataka o ljudskim resursima te navesti gdje uključeni zaposlenici mogu pogledati politiku zaštite privatnosti.

d. Ministarstvo vodi Popis organizacija u sustavu zaštite privatnosti koje su podnijele potpune izjave o samocertificiranju čime se osigurava dostupnost pogodnosti sustava zaštite privatnosti i ažurira taj popis na temelju godišnjih izjava o samocertificiranju i obavijestima zaprimljenima u skladu s Dodatnim načelom o rješavanju sporova i izvršenju odluka. Takve izjave o samocertificiranju dostavljaju se najmanje jednom godišnje. U suprotnom se organizacija uklanja s Popisa organizacija u sustavu zaštite privatnosti i više joj nisu zajamčene povlastice sustava zaštite privatnosti. Popis organizacija u sustavu zaštite privatnosti i izjave organizacija o samocertificiranju javno su dostupni. Sve organizacije koje je Ministarstvo uvrstilo Popis organizacija u sustavu zaštite privatnosti moraju također navesti u svojim relevantnim objavljenim izjavama o politici zaštite privatnosti da poštuju načela sustava zaštite privatnosti. Nadalje, ako je dostupna na internetu, politika zaštite

privatnosti određene organizacije mora uključivati poveznicu na *web*-mjesto sustava zaštite privatnosti te poveznicu na *web*-mjesto ili obrazac za podnošenje pritužbi neovisnog mehanizma za pravnu zaštitu koji je dostupan za rješavanje neriješenih pritužbi.

e. Načela zaštite privatnosti primjenjuju se odmah nakon certificiranja. Svjesne da će načela utjecati na njihove poslovne odnose s trećim strankama, organizacije koje su se certificirale za okvir sustava zaštite privatnosti tijekom prva dva mjeseca nakon stupanja okvira na snagu usklađuju postojeći poslovni odnos s trećim strankama s načelom odgovornosti za daljnji prijenos što je prije moguće, a u svakom slučaju najkasnije devet mjeseci od datuma kada su se certificirale za sudjelovanje u sustavu zaštite privatnosti. U tom prijelaznom razdoblju, kada organizacije prenose podatke trećoj stranci, one i. primjenjuju načela obavješćivanja i izbora i ii. ako se osobni podaci prenose trećoj stranci koja djeluje kao agent, osigurati da agent mora pružiti razinu zaštite koja je najmanje jednaka razini propisanoj načelima.

f. Organizacija mora obrađivati sve sobne podatke zaprimljene od EU-a u okviru sustava zaštite privatnosti obrađivati u skladu s načelima sustava zaštite privatnosti. Preuzeta obveza poštovanja načela sustava zaštite privatnosti nije vremenski ograničena u odnosu na podatke zaprimljene tijekom razdoblja u kojem organizacija uživa pogodnosti sustava zaštite privatnosti. Njezina obveza znači da će nastaviti primjenjivati načela na takve podatke sve dok ih organizacija pohranjuje, koristi ili otkriva, čak i ako kasnije napusti sustav za zaštitu privatnosti iz bilo kojeg razloga. Organizacija koja se povlači iz sustava zaštite privatnosti, ali želi zadržati te podatke mora svake godine potvrditi Ministarstvu trgovine da se obvezuje dalje primjenjivati načela ili osigurati „odgovarajuću" zaštitu osobnih podataka drugim odobrenim sredstvima (na primjer, uporabom ugovora koji se temelji na zahtjevima relevantnih standardnih ugovornih odredaba koje je odobrila Komisija). U protivnom organizacija mora te podatke vratiti ili ihizbrisati. Organizacija koja se povlači iz sustava zaštite privatnosti mora ukloniti iz relevantnih politika zaštite privatnosti sva upućivanja na sustav za zaštitu privatnosti u kojima je navedeno da organizacija aktivno sudjeluje u sustavu zaštite privatnosti i da ima pravo na njegove pogodnosti.

g. Organizacija koja prestane postojati kao zasebna pravna osoba zbog spajanja ili preuzimanja, mora unaprijed o tome obavijestiti Ministarstvo. U obavijesti treba također navesti hoće li društvo koje je steklo organizaciju ili ono koje je rezultat udruživanja: i. nastavit poštovati načela sustava zaštite privatnosti u skladu sa zakonom kojim se uređuje preuzimanje ili spajanje; ili ii. odlučit će obaviti samocertificiranje pridržavanja načela sustava zaštite privatnosti ili uspostaviti druge zaštitne mjere, poput pisanog sporazuma kojim će se osigurati poštovanje načela sustava zaštite privatnosti. Ako se ne primjenjuju ni i. niti ii., svi osobni podaci koji su prikupljeni u okviru sustava zaštite privatnosti moraju se odmah izbrisati.

h. Ako organizacija napusti sustav zaštite privatnosti iz bilo kojeg razloga, ona mora ukloniti sve izjave da sudjeluje u sustavu zaštite privatnosti ili da ima pravo na pogodnosti sustava zaštite privatnosti. Ako se upotrebljava certifikacijska oznaka europsko-američkog sustava zaštite privatnosti, ona se također mora ukloniti. FTC ili drugo relevantno nadležno tijelo može pokrenuti sudski postupak u slučaju lažne izjave da se organizacija pridržava načela sustava zaštite privatnosti. Lažno prikazivanje Ministarstvu kažnjivo je u skladu sa Zakonom o lažnim izjavama (18 U.S.C. članak 1001.).

7. **Provjera**

a. Organizacije moraju osigurati postupke praćenja za provjeru istinitosti potvrda i navoda koje su dale o svojim praksama zaštite privatnosti u okviru sustava zaštite privatnosti i te se prakse moraju provoditi kako je navedeno i u skladu s načelima sustava zaštite privatnosti.

b. Kako bi mogla zadovoljiti zahtjeve provjere iz načela pravne zaštite, provedbe i odgovornosti, organizacija može provjeriti takve potvrde i navode samoprocjenom ili vanjskim preispitivanjima njihova poštovanja.

c. U okviru pristupa samoprocjene, takva bi provjera trebala pokazati da je objavljena politika zaštite privatnosti neke organizacije u pogledu osobnih podataka primljenih iz EU-a točna, sveobuhvatna, jasno prikazana, u potpunosti provedena i dostupna. Također bi trebala pokazati da je njezina politika zaštite privatnosti u skladu s načelima sustava zaštite privatnosti; da su pojedinci obaviješteni o unutarnjim mehanizmima za rješavanje pritužbi i o neovisnim mehanizmima putem kojih mogu podnositi pritužbe; da ima uvedene postupke za osposobljavanje zaposlenika o njegovoj primjeni i za kažnjavanje za neprovođenje; te da ima uvedene unutarnje postupke za periodično provođenje objektivnih provjera poštuje li se gore navedeno. Izjavu kojom se potvrđuje

samoproocjena treba potpisati rukovoditelj poduzeća ili neki drugi ovlašteni predstavnik organizacije barem jednom godišnje i staviti je na raspolaganje pojedincima na njihov zahtjev ili u kontekstu istrage ili pritužbe o neusklađenosti.

d. Ako organizacija odabere vanjsku provjeru poštovanja privatnosti, takva provjera treba pokazati da je njezina politika zaštite privatnosti s obzirom na osobne podatke primljene iz EU-a usklađena s načelima sustava zaštite privatnosti, da se poštuje i da su pojedinci obaviješteni o mehanizmima putem kojih mogu podnositi pritužbe. Metode provjere mogu bez ograničenja uključivati reviziju, nasumične provjere, korištenje „mamaca" ili, prema potrebi, uporabu tehnoloških sredstava. Izjavu kojom se potvrđuje da je vanjska provjera poštovanja načela uspješno završena treba potpisati voditelj provjere, ili rukovoditelj poduzeća ili neki drugi ovlašteni predstavnik organizacije najmanje jednom godišnje i staviti je na raspolaganje pojedincima na njihov zahtjev, ili u kontekstu istrage ili pritužbe u vezi s poštovanjem načela.

e. Organizacije moraju čuvati svoje evidencije o provedbi svoje prakse privatnosti u okviru sustava zaštite privatnosti i na zahtjev ih učiniti dostupnima u kontekstu istrage ili pritužbe o nepoštovanju neovisnom tijelu odgovornom za istraživanje pritužbi ili agenciji koja je nadležna za nepoštena i prijevarna postupanja. Organizacije moraju bez odlaganja odgovoriti na upite i druge zahtjeve Ministarstva za informacije koje se odnose na to pridržava li se organizacija načela.

8. **Pristup**

a. Načelo pristupa u praksi

i. U skladu s načelima sustava zaštite privatnosti, pravo pristupa od temeljne je važnosti za zaštitu privatnosti. Njime se osobito omogućuje pojedincima da provjere točnost informacija koje se čuvaju o njima. Načelo pristupa znači da osobe imaju pravo na sljedeće:

1. od organizacije dobiti potvrdu o tome obrađuje li ona podatke koji se odnose na njih ([1]);

2. da im se ti podaci priopće kako bi mogle provjeriti njihovu točnost i zakonitost obrade i

3. na ispravljanje, mijenjanje ili brisanje netočnih podataka ili podataka koji se obrađuju protivno načelima.

ii. Osobe ne moraju obrazlagati zahtjeve za pristup vlastitim podacima. Kada odgovaraju na zahtjeve osoba za pristup, organizacije bi se trebale voditi pitanjima zbog kojih su zahtjevi izvorno postavljeni. Na primjer, ako je zahtjev za pristup nejasan ili preširok, organizacija može razgovarati s pojedincem kako bi bolje shvatila motive za zahtjev i dala povratnu informaciju. Organizacija se može raspitati s kojim je dijelom (dijelovima) organizacije pojedinac kontaktirao i/ili o vrsti informacija ili njihovom korištenju za koje se zahtjeva pristup.

iii. U skladu s osnovnom prirodom pristupa, organizacije uvijek trebaju poduzeti napore u dobroj vjeri da omoguće pristup. Na primjer, ako određenu informaciju treba zaštititi, a moguće ju je lako izdvojiti od ostalih informacija za koje se traži pristup, organizacija treba redigirati zaštićenu informaciju i učiniti dostupnima ostale informacije. Ako organizacija odluči da treba uskratiti pristup u nekom određenom slučaju, treba objasniti podnositelju zahtjeva za pristup zašto je donijela takvu odluku i uputiti ga na kontaktno mjesto za sve daljnje upite.

b. Teret ili trošak pružanja pristupa

i. Pravo pristupa osobnim podacima može biti ograničeno u iznimnim okolnostima ako bi bilo povrijeđeno zakonito pravo osoba koje nisu ta osoba ili ako bi teret ili trošak pružanja pristupa bio nerazmjeran rizicima za privatnost osobe u predmetnom slučaju. Trošak i teret važni su čimbenici i trebaju se uzeti u obzir, ali oni nisu presudni u odlučivanju je li omogućivanje pristupa razumno.

([1]) Organizacija bi trebala odgovoriti na zahtjeve osoba u vezi sa svrhom obrade, kategorijama predmetnih osobnih podataka i primateljima ili kategorijama primatelja kojima se otkrivaju osobni podaci.

ii. Na primjer, ako se osobni podaci upotrebljavaju za odluke koje će značajno utjecati na pojedinca (npr. uskraćenje ili odobrenje bitnih pogodnosti, kao što je osiguranje, hipoteka ili posao), tada bi u skladu s ostalim odredbama ovih Dodatnih načela organizacija morala otkriti informacije čak i ako je to relativno teško ili skupo pružiti. Ako traženi osobni podaci nisu osjetljivi ili se ne upotrebljavaju za odluke koje će znatno utjecati na osobu već su lako dostupni i nije ih skupo pružati, organizacija će morati osigurati pristup takvim podacima.

c. Povjerljivi tržišni podaci

i. Povjerljivi osobni podaci jesu podaci koje je organizacija zaštitila od otkrivanja, ako bi se njihovim otkrivanjem pomoglo konkurentu na tržištu. Organizacije mogu uskratiti ili ograničiti pristup u onoj mjeri u kojoj bi se njegovim omogućivanjem razotkrilo vlastitu povjerljivu poslovnu informaciju koje je ranije definirana, kao što su zaključci vezani za tržište ili razvrstavanje koje je napravila organizacija ili povjerljiva poslovna informacija treće osobe ako takva informacija podliježe ugovornoj obvezi o povjerljivosti.

ii. Ako se povjerljivi poslovni podatak može lako izdvojiti od ostalih podatka za koje se traži pristup, organizacija treba redigirati povjerljivi poslovni podatak i učiniti dostupnima nepovjerljive podatke.

e. Organizacija baza podataka

i. Pristup se može omogućiti i na način da organizacija otkrije pojedincu relevantne osobne podatke pri čem se ne zahtijeva pristup pojedinca bazi podataka organizacije.

ii. Pristup treba omogućiti samo ako organizacija pohranjuje osobne podatke. Načelom pristupa samim po sebi ne stvara se obveza zadržavanja, održavanja, reorganiziranja ili restrukturiranja datoteke s osobnim podacima.

e. Kada pristup može biti ograničen

i. Budući da organizacije moraju uvijek ulagati napore u dobroj vjeri kako bi osobama osigurale pristup njihovim osobnim podacima, okolnosti u kojima organizacije mogu ograničiti takav pristup ograničene su i razlog za ograničavanje pristupa mora biti posebno naveden. Kao u skladu s Direktivom, organizacija može ograničiti pristup informacijama u onoj mjeri u kojoj bi se otkrivanje moglo kositi sa zaštitom bitnih prevladavajućih javnih interesa, kao što su nacionalna sigurnost, obrana; ili javna sigurnost. Osim toga, ako se osobni podaci obrađuju isključivo u istraživačke ili statističke svrhe, pristup se može uskratiti. Ostali razlozi za uskraćivanje ili ograničavanje pristupa jesu:

1. ometanje izvršenja ili provedbe zakona li privatni uzroci djelovanja, među ostalim sprečavanje, istraživanje ili otkrivanje kaznenih djela ili prava na pošteno suđenje;

2. otkrivanje ako bi bila narušena zakonita prava ili važni interesi ostalih,

3. kršenje obveze čuvanja pravnih ili profesionalnih tajni ili obveza;

4. ugrožavanje sigurnosnih istraga zaposlenika ili žalbenih postupaka ili u vezi s planiranjem osobe koja će naslijediti zaposlenika ili reorganizacije poduzeća, ili

5. dovođenje u pitanje povjerljivosti koja je nužna za praćenje, inspekciju ili regulatorne zadaće povezane s dobrim upravljanjem ili u budućim ili tekućim pregovorima u kojima organizacija sudjeluje.

ii. Organizacija koja zahtijeva izuzeće snosi teret dokazivanja njegove nužnosti i osobe bi trebalo obavijestiti o razlozima za ograničavanje pristupa te o kontaktnoj točki za daljnje upite.

f. Pravo na pribavljanje potvrde i naplaćivanje naknade za pokrivanje troškova pružanja pristupa

i. Osoba ima pravo dobiti potvrdu posjeduje li ta organizacija osobne podatke koji se odnose na nju. Osoba također ima pravo da mu se priopće osobni podaci koji se odnose na nju. Organizacija smije naplaćivati naknadu koja nije pretjerana.

ii. Naplaćivanje naknade može biti opravdano, na primjer, ako su zahtjevi za pristup očito pretjerani, posebno jer se ponavljaju.

iii. Pristup se ne može uskratiti radi troška ako osoba ponudi da će platiti troškove.

g. Višestruki ili naporni zahtjevi za pristup

Organizacija može odrediti razumne granice u pogledu toga koliko puta se može ispuniti zahtjev određene osobe za pristupom. Pri određivanju takvih ograničenja organizacija bi trebala uzeti u obzir čimbenike kao što su učestalost ažuriranja informacija, svrha uporabe podataka i priroda informacija.

h. Prijevarni zahtjevi za pristup

Organizacija ne mora omogućiti pristup ako joj se ne da dovoljno informacija koje joj omogućavaju da provjeri identitet osobe koja podnosi zahtjev.

i. Rokovi za odgovore

Organizacije bi trebale odgovoriti na zahtjeve za pristup u razumnom roku, na razuman način i u obliku koji osoba razumije. Organizacija koja redovito pruža podatke osobama čiji se podaci obrađuju može zadovoljiti pojedinačni zahtjev za pristup redovitim otkrivanjem podataka, ako to ne bi bio prekasno.

9. **Podaci o ljudskim resursima**

a. Pokrivenost sustavom za zaštitu podataka

i. Ako organizacija u EU-u prenosi osobne podatke o svojim zaposlenicima (bivšim ili sadašnjim) prikupljene u kontekstu radnog odnosa, matičnom, povezanom ili nepovezanom pružatelju usluga u Sjedinjenim Američkim Državama koji sudjeluje u sustavu zaštite privatnosti, na prijenos se primjenjuju pogodnosti sustava zaštite privatnosti. U takvim slučajevima prikupljanje podataka i njihova obrada prije prijenosa podliježu nacionalnom pravu države EU-a u kojoj su prikupljeni i moraju se poštovati svi uvjeti ili ograničenja njihova prijenosa u skladu s tim pravom.

ii. Načela sustava zaštite privatnosti bitna su samo ako se prenosi pojedinačno utvrđena evidencija ili ako joj se pristupa. Statističkim izvješćivanje koje se temelji na ukupnim podacima o zaposlenosti i ne sadržava osobne podatke ili na uporabi anonimiziranih podataka ne ugrožava povjerljivost.

b. Primjena načela obavješćivanja izbora

i. Organizacija iz SAD-a koja je primila informacije o zaposlenicima iz EU-a u skladu sa sustavom zaštite privatnosti može ih otkriti trećih stranama i/ili upotrijebiti u različite svrhe samo u skladu s načelima obavješćivanja i izbora. Na primjer, ako organizacija namjerava koristiti osobne podatke prikupljene tijekom radnog odnosa u svrhe koje nisu vezane uz radni odnos, kao što su tržišne obavijesti, organizacija iz SAD-a mora osobama na koje se podaci odnose ponuditi izbor prije nego što tako učini, osim ako su oni već odobrili uporabu podataka u takve svrhe. Takvo korištenje ne smiju biti u suprotnosti s svrhe u koje su podaci prikupljeni ili za koje je pojedinac naknadno dao odobrenje. Štoviše, takve se mogućnosti izbora ne smiju upotrebljavati za ograničavanje prilika za zapošljavanje ili poduzimanje kaznenih mjera protiv takvih zaposlenika.

ii. Treba napomenuti da određeni opće važeći uvjeti za prijenos iz nekih država članica mogu isključivati druge vrste uporabe takvih informacija čak i nakon prijenosa izvan EU-a, i takve uvjete se mora poštovati.

iii. Osim toga, poslodavci trebaju uložiti razumne napore da bi udovoljili zaposlenikovom izboru u odnosu na privatnost. To može, na primjer, uključivati ograničivanje pristupa osobnim podacima, anonimizaciju određenih podataka ili korištenje šifri ili pseudonima kad stvarna imena nisu potrebna za postojeću svrhu upravljanja.

iv. U onoj mjeri i onom razdoblju koje je nužno kako bi se izbjeglo ugrožavanje zakonitih interesa organizacije pri unapređivanju, imenovanjima ili ostalim sličnim odlukama o zaposlenju, organizacija ne mora nuditi obavješćivanje i mogućnost izbora.

c. Primjena načela pristupa

Dodatnim načelom o pristupu osiguravaju se smjernice o razlozima zbog kojih je opravdano uskratiti ili ograničiti zahtjev za pristup u kontekstu ljudskih potencijala. Naravno, poslodavci u Europskoj uniji moraju poštovati lokalne propise i osigurati da zaposlenici Europske unije imaju pristup takvim informacijama u skladu sa zakonodavstvom njihove domovine, neovisno o mjestu obrade i pohrane podataka. Sustavom zaštite privatnosti zahtijeva se da organizacija koja obrađuje takve podatke u Sjedinjenim Američkim Državama surađuje u omogućivanju takvog pristupa bilo izravno ili posredstvom poslodavca iz EU-a.

d. Provedba

i. Ako se osobni podaci upotrebljavaju samo u kontekstu radnog odnosa, glavnu odgovornost za podatke u pogledu zaposlenika snosi organizacija u EU-u. Iz toga proizlazi da europske zaposlenike koji se žale na kršenje njihovih prava na zaštitu podataka i nisu zadovoljni s rezultatima internih postupaka provjere, pritužbi i žalbi (ili nekog žalbenog postupka koji se primjenjuje u skladu s ugovoru sa sindikatom) treba uputiti državnom ili nacionalnom tijelu za zaštitu podataka ili za radno pravo u području u kojem zaposlenik radi. To uključuje slučajeve kada je za navodno krivo postupanje s njihovim osobnim podacima odgovorna organizacija SAD-a koja je primila informacije od poslodavca i stoga je riječ o navodnoj povredi načela sustava za zaštitu privatnosti. To će biti najučinkovitiji način rješavanja preklapanja prava i obveza propisanih lokalnim radnim pravom i kolektivnim ugovorima te pravom o zaštiti podataka.

ii. Organizacija iz SAD-a, sudionica u sustavu zaštite privatnosti koja se koristi podacima o ljudskim resursima koji su preneseni iz Europske unije u kontekstu radnog odnosa i koja želi da takvi prijenosi budu obuhvaćeni sustavom zaštite privatnosti mora se iz tog razloga obvezati na suradnju u istragama i poštovanje savjeta nadležnih tijela EU-a u takvim slučajevima.

e. Primjena načela odgovornosti za daljnji prijenos

U slučaju povremenih operativnih potreba organizacije u sustavu zaštite privatnosti za osobnim podacima prenesenima u kontekstu zapošljavanja u skladu sa sustavom za zaštitu privatnosti, na primjer rezervacije zrakoplovne karte, hotelske sobe ili osiguranja, mogu se izvršiti prijenosi osobnih podataka malog broja zaposlenika voditeljima obrade bez primjene načela pristupa ili sklapanja ugovora s trećom stranom koja djeluje kao voditelj obrade, kako je propisano u skladu s načelom odgovornosti za daljnji prijenos, pod uvjetom da je organizacija u sustavu zaštite privatnosti postupila u skladu s načelima obavješćivanja i izbora.

10. **Obavezni ugovori za daljni prijenos**

a. Ugovori o obradi podataka

i. Kada se osobni podaci iz EU-a prenose u Sjedinjene Američke Države samo za potrebe obrade, bit će potreban ugovor, bez obzira na sudjelovanje izvršitelja obrade u sustavu zaštite privatnosti.

ii. Voditelji obrade podataka u Europskoj uniji uvijek su obvezni sklopiti ugovor kada se prijenos izvršava radi same obrade, bez obzira hoće li se radnje obrade izvršiti unutar ili izvan EU-a i neovisno o tome sudjeluje li izvršitelj obrade u sustavu zaštite privatnosti. Svrha je ugovora osigurati da izvršitelj obrade:

1. djeluje samo prema uputama voditelja obrade;

2. osigurava odgovarajuće tehničke i ustrojstvene mjere za zaštitu osobnih podataka od slučajnog ili nezakonitog uništenja ili slučajnog gubitka, izmjene, neovlaštenog otkrivanja ili pristupa i razumije zašto je dopušten daljnji prijenos i

3. uzimajući u obzir prirodu obrade, pomaže voditelju obrade da odgovori osobama koje ostvaruju svoja prava u skladu s načelima.

iii. Budući da sudionici u sustavu zaštite privatnosti pružaju primjerenu zaštitu, za ugovore sa sudionicima sustava zaštite privatnosti radi same obrade nije potrebno prethodno odobrenje (ili će takvo ovlaštenje automatski davati države članice EU-a), kao što bi bilo potrebno za ugovore s primateljima koji ne sudjeluju u sustavu zaštite privatnosti ili ne pružaju primjerenu zaštitu na neki drugi način.

b. Prijenos unutar kontrolirane skupine poduzeća ili subjekata

Ako se osobni podaci prenose između dvaju voditelja obrade u kontroliranoj skupini poduzeća ili subjekata, nije uvijek potreban ugovor u skladu s načelom odgovornosti za daljnji prijenos. Voditelji obrade podataka u kontroliranoj skupini poduzeća ili subjekata mogu takve prijenose temeljiti na drugim instrumentima, poput obvezujućih korporativnih pravila EU-a ili drugih instrumenata unutar skupine (npr. programi usklađenosti i kontrole) osiguravajući kontinuitet zaštite osobnih podataka u skladu s Načelima. U slučaju takvih prijenosa, organizacija u sustavu zaštite privatnosti odgovorna je za poštovanje načela zaštite privatnosti.

c. Prijenosi između voditelja obrade

U slučaju prijenosa između voditelj obrade, voditelj primatelj ne mora biti organizacija u sustavu zaštite privatnosti ni imati neovisan mehanizam pravne zaštite. Organizacija u sustavu zaštite privatnosti mora sklopiti ugovor s trećom stranom koja djeluje kao voditelj obrade koji je primatelj, a kojim se osigurava ista razina zaštite koja je dostupna u okviru sustava za zaštitu privatnosti. Pritom ne postoji zahtjev da treća strana koja djeluje kao voditelj obrade mora biti organizacija sustava za zaštitu privatnosti ili imati neovisan sustav pravne zaštite, ako je dostupan jednakovrijedni mehanizam.

11. **Rješavanje sporova i provedba**

a. Načelom pravne zaštite, provedbe i odgovornosti utvrđuju se zahtjevi za provedbu sustava zaštite privatnosti. Načini ispunjenja zahtjeva iz točke (a) podtočke iii. Načela utvrđeni su u Dodatnom načelu o provjeri. Dodatno načelo odnosi se na točku (a) podtočke i. i iii. za koje su potrebni neovisni mehanizmi pravne zaštite. Ti mehanizmi mogu imati različite oblike, ali moraju ispunjavati zahtjeve načela pravne zaštite, provedbe i odgovornosti. Organizacije udovoljavaju zahtjevima na sljedeće načine: i. poštovanjem programa privatnosti koje je razvio privatni sektor koji je u svoja pravila ugradio načela sustava zaštite privatnosti i koji uključuju učinkovite mehanizme izvršenja opisane u načelu pravne zaštite, provedbe i odgovornosti; ii. poštovanjem zakonskih ili regulatornih nadzornih tijela koja rješavaju pojedinačne pritužbe i sporove; ili iii. preuzimanjem obveze suradnje s tijelima za zaštitu podataka smještenima u Europskoj uniji ili s njihovim ovlaštenim predstavnicima.

b. Ovaj popis trebao bi biti ilustrativan, a ne ograničavajući. Privatni sektor može osmisliti druge mehanizme provedbe ako oni zadovoljavaju zahtjeve načela pravne zaštite, provedbe i odgovornosti i dodatna načela. Imajte na umu da su zahtjevi pravne zaštite, provedbe i odgovornosti dodatni uz zahtjev da se samoregulacija mora

provesti u skladu s odjeljkom 5. Zakona o Saveznoj trgovinskoj komisiji kojim se zabranjuje nepoštene i prijevarne radnje ili drugim zakonom ili uredbom kojim se zabranjuje takvo djelovanje.

c. Kako bi se omogućilo poštovanje obveza iz njihova sustava zaštite privatnosti i radi podupiranja upravljanja programom, organizacija i njezini neovisni mehanizmi pravne zaštite moraju pružiti informacije o sustavu zaštite privatnosti na zahtjev Ministarstva. Nadalje, organizacije moraju žurno odgovoriti na pritužbe u vezi sa svojim poštovanjem načela koje su nadležna tijela za zaštitu podataka proslijedila Ministarstvu. U odgovoru bi trebalo biti navedeno je li pritužba osnovana te kako će organizacija ispraviti problem. Ministarstvo će zaštititi povjerljivost informacija zaprimljenih u skladu sa zakonodavstvom EU-a.

d. Mehanizmi pravne zaštite

i. Potrošače treba poticati da podnose pritužbe protiv određene organizacije prije nego što upotrijebe neovisni mehanizam pravne zaštite. Organizacije moraju odgovoriti potrošaču u roku od 45 dana od primitka pritužbe. Neovisnost mehanizma pravne zaštite činjenično je pitanje na koje se može odgovoriti nepristranošću, transparentnom strukturom i financiranjem ili dokazima o poslovanju. U skladu s načelom pravne zaštite, provedbe i odgovornosti, pravna zaštita koja je na raspolaganju mora biti lako dostupna i prihvatljiva. Tijela za rješavanje sporova trebaju razmotriti svaku pritužbu koju prime od pojedinaca osim ako je očigledno neutemeljena ili neozbiljna. Time se ne sprečava organizacija koja upravlja mehanizmom pravne zaštite da utvrdi zahtjeve prihvatljivosti, ali takvi zahtjevi trebaju biti transparentni i opravdani (na primjer, da isključuju pritužbe koje nisu obuhvaćene područjem primjene programa ili koje treba razmotriti na drugom forumu) i ne smiju umanjivati obvezu razmatranja opravdanih pritužbi. Osim toga, mehanizmima pravne zaštite osobama se trebaju osigurati potpune i lako dostupne informacije o funkcioniranju postupka rješavanja sporova kada ulažu žalbu. Takve informacije trebaju obuhvatiti obavijest o odnosu mehanizma prema praksama u vezi s privatnosti, u skladu s načelima sustava zaštite privatnosti. Također trebaju surađivati u izradi alata kao što su standardni obrasci žalbi kojima će se olakšati postupak rješavanja pritužbi.

ii. Neovisni mehanizmi pravne zaštite moraju uključivati na svojim javnim *web*-mjestima informacije o načelima sustava zaštite privatnosti i uslugama koje pružaju u okviru sustava zaštite privatnosti. Te informacija moraju uključivati sljedeće: 1. informacije o zahtjevima načela sustava zaštite privatnosti u pogledu neovisnih mehanizama pravne zaštite ili poveznicu na te zahtjeve; 2. poveznicu na *web*-mjesto sustava zaštite privatnosti Ministarstva; 3. objašnjenje da su njihove usluge rješavanja sporova u okviru sustava zaštite privatnosti besplatne za sve osobe; 4. opis kako je moguće podnijeti pritužbu povezanu sa sustavom zaštite privatnosti; 5. vremensko razdoblje obrade pritužbi sustava zaštite privatnosti; i 6. opis raspona mogućih pravnih sredstavaa.

iii. Neovisni mehanizmi pravne zaštite moraju objaviti godišnje izvješće sa ukupnim statističkim podacima o njihovim uslugama rješavanja sporova. Godišnje izvješće mora sadržavati informacije o sljedećem: 1. ukupnom broju pritužbi povezanih sa sustavom zaštite privatnosti zaprimljenih tijekom izvještajne godine; 2. vrstama zaprimljenih pritužbi; 3. mjerama kvalitete rješavanja sporova poput trajanja obrade zahtjeva; i 4. rezultatima zaprimljenih pritužbi, posebno o broju i vrstama pravnih sredstava ili određenih sankcija.

iv. Kako je navedeno u Prilogu I., osobi je dostupna mogućnost arbitraže kojom se može utvrditi, za preostala potraživanja, je li organizacija u sustavu zaštite privatnosti povrijedila svoju obvezu u skladu s načelima u pogledu pojedinca te je li ta povreda potpuno ili djelomično ispravljena. Ta je mogućnost dostupna samo u navedene svrhe. Ta mogućnost nije dostupna, primjerice, u pogledu izuzeća od načela ([1]) ili u odnosu na navode o primjerenosti sustava zaštite privatnosti. U skladu s ovom mogućnošću arbitraže, Odbor za sustav zaštite privatnosti (koji se sastoji od jednog ili tri arbitra, kako su dogovorile stranke) ima ovlasti odrediti pojedinačnu nenovčanu pravičnu naknadu (poput pristupa, ispravka, brisanja ili vraćanja predmetnih podataka osobe) koji su nužni za ispravak kršenja načela samo u pogledu pojedinca. Osobe i organizacije u sustavu zaštite privatnosti moći će tražiti sudsko preispitivanje i izvršenje arbitražnih odluka u skladu sa zakonodavstvom EU-a, odnosno Saveznim zakonom o arbitraži

([1]) Odjeljak I. točka 5. Načela.

e. Pravna sredstva i sankcije

Rezultat bilo kojeg pravnog lijeka koji nudi tijelo za rješavanje sporova treba biti takav da organizacija poništi ili ispravi učinke neusklađenosti, koliko god je to izvedivo i da ubuduće obrada organizacije bude u skladu s načelima i ako je primjereno, da se prestanu obrađivati osobni podaci pojedinca koji je podnio žalbu. Sankcije trebaju biti dovoljno stroge da se njima osigura da organizacija poštuje načela. Nizom sankcija različite težine omogućuje se tijelima za rješavanje sporova da na odgovarajući način reagiraju na različite stupnjeve neusklađenosti. Sankcije trebaju uključivati i javno objavljivanje otkrivenih slučajeva neusklađenosti i zahtjev da se u određenim okolnostima obrišu ([1]). Ostale sankcije mogu uključivati privremeno ukidanje i oduzimanje pečata, nadoknadu gubitaka pojedincima koje su pretrpjeli kao posljedicu neusklađenosti i sudske zabrane. Tijela za rješavanje sporova iz privatnog sektora i samoregulatorna tijela moraju obavijestiti nadležno tijelo ili sud, prema potrebi, i Ministarstvo, o tome da organizacija u sustavu zaštite privatnosti ne pridržava njihovog rješenja.

f. Djelovanje Savezne trgovinske komisije

FTC se obvezao davati prednost preispitivanju upućenih slučajeva navodnog nepoštovanja načela koje mu podnose: i. samoregulatorne organizacije za zaštitu privatnosti i druga neovisna tijela za rješavanje sporova; ii. države članice EU-a i iii. Ministarstvo, kako bi utvrdio je li povrijeđen odjeljak 5. Zakona o FTC-u kojim se zabranjuju nepoštene ili prijevarne radnje ili trgovačka praksa. Ako FTC zaključi da je opravdano vjerovati da je prekršen odjeljak 5., može riješiti stvar traženjem administrativne zabrane spornih radnji, ili ulaganjem tužbe saveznom okružnom sudu koja, ako bude uspješno riješena, može dovesti do saveznog sudskog naloga s istim učinkom. To uključuje lažne tvrdnje o poštovanju načela sustava zaštite privatnosti ili o sudjelovanju u sustavu zaštite privatnosti organizacija koje više nisu na Popisu organizacija u sustavu zaštite privatnosti ili se nikada nisu samocertificirale Ministarstvu. FTC može ishoditi građanskopravnu kaznu za povrede administrativne zabrane i može pokrenuti građansku parnicu ili kazneni postupak zbog povrede naloga saveznog suda. FTC će obavijestiti Ministarstvo o poduzimanju takvih mjera. Ministarstvo potiče ostala državna tijela da ga obavješćuju o konačnoj presudi o takvim prosljeđenim slučajevima ili o drugim odlukama kojima se odlučuje o pridržavanju načela sustava zaštite privatnosti.

g. Ustrajno nepoštovanje načela

i. Ako organizacija ustrajno ne poštuje načela, ona više nema pravo na pogodnosti iz sustava zaštite privatnosti. Organizacije koje ustrajno ne poštuju načela zaštite privatnosti Ministarstvo će ukloniti s Popisa organizacija u sustavu zaštite privatnosti i one moraju vratiti ili obrisati osobne podatke zaprimljene u okviru europsko-američkog sustava zaštite privatnosti.

ii. Ustrajno nepoštovanje načela nastaje kada organizacija koja je obavila samocertificiranje Ministarstvu odbije postupiti u skladu s odlukom samoregulatornog tijela za zaštitu privatnosti, tijela za neovisno rješavanje sporova ili državnog tijela ili ako takvo tijelo utvrdi da organizacija ustrajno ne poštuje načela do mjere u kojoj njezin zahtjev za izvršenje više nije vjerodostojan. U tim slučajevima organizacija mora bez odlaganja obavijestiti Ministarstvo o tim činjenicama. Ako to ne učini može biti kažnjena u skladu sa Zakonom o lažnim izjavama (18 U.S.C. članak 1001.). Povlačenjem iz samoregulatornog programa zaštite privatnosti privatnog sektora ili neovisnog mehanizma za rješavanje sporova organizacija se ne oslobađa obveze postupanja u skladu s načelima i to čini ustrajno nepoštovanje načela.

iii. Ministarstvo briše organizaciju s Popisa organizacija u sustavu zaštite privatnosti na temelju bilo kakve zaprimljene obavijesti o ustrajnom nepoštovanju načela bez obzira je li ju zaprimila od same organizacije, od samoregulatornog tijela za zaštitu privatnosti, od drugog neovisnog tijela za rješavanje sporova ili od državnog tijela, ali tek nakon što je organizaciji koja nije poštovala načela dostavila obavijesti 30 dana

([1]) Tijela za rješavanje sporova imaju slobodu odlučivanja o okolnostima u kojima primjenjuju te sankcije. Osjetljivost predmetnih podataka jedan je od čimbenika koje treba uzeti u obzir pri odlučivanju hoće li biti potrebno brisati podatke, kao što je i činjenica je li organizacija prikupila, koristila ili otkrila informacije u očitoj suprotnosti s načelima sustava zaštite privatnosti.

unaprijed i dala joj priliku za odgovor. U skladu s time na Popisu organizacija u sustavu zaštite privatnosti koji vodi Ministarstvo mora biti jasno navedeno kojim su organizacijama zajamčene pogodnosti sustava zaštite privatnosti, a kojima više nisu.

iv. Organizacija koja se prijavi za sudjelovanje u samoregulatornom tijelu kako bi ponovno stekla uvjete za članstvo u sustavu zaštite privatnosti mora tom tijelu dostaviti sve informacije o svom prijašnjem sudjelovanju u sustavu zaštite privatnosti.

12. **Izbor – Rokovi za traženje izuzeća**

a. Općenito je svrha načela mogućnosti izbora osigurati korištenje i otkrivanje osobnih podataka na načine koji su u skladu s očekivanjima i željama pojedinca. Stoga, pojedincu treba biti omogućeno da iskoristi mogućnost da bilo kada „zatraži izuzeće" od toga da se njihovi podaci upotrebljavaju za izravni marketing u razumnim rokovima koje je odredila organizacija kako bi se organizaciji dalo vremena da provede izuzeće. Organizacija može također tražiti dovoljno informacija da potvrdi identitet pojedinca koji zahtijeva „izuzeće". U Sjedinjenim Američkim Državama osobe se mogu koristiti ovom mogućnošću u okviru središnjeg programa „izuzeća" kao što je usluga željene pošte organizacije Direct Marketing Association. Organizacije koje koriste uslugu željene pošte organizacije Direct Marketing Association trebaju promicati njezinu dostupnost potrošačima koji ne žele primati marketinške informacije. U svakom slučaju, pojedincu treba ponuditi lako dostupan i pristupačan mehanizam za uporabu ove mogućnosti.

b. Slično tome, organizacija se može koristiti informacijama u određene svrhe izravnog marketinga kada nije praktično ponuditi pojedincu mogućnost „izuzeća" prije uporabe informacija, ako organizacija toj osobi bez odgađanja ponudi mogućnost istodobnog (i na zahtjev bilo kada) odbijanja (bez troška za pojedinca) primanja izravnih marketinških obavijesti i postupi u skladu s njegovim željama.

13. **Putničke informacije**

a. Podaci o rezervaciji zrakoplovne karte i ostale putničke informacije, kao što su informacije o učestalim putnicima ili hotelskim rezervacijama i posebnim potrebama, kao što su obroci koji ispunjavaju vjerske zahtjeve ili fizička pomoć, mogu se prenositi organizacijama izvan EU-a u nekoliko različitih slučajeva: U skladu s člankom 26. Direktive, osobni podaci mogu se prenositi „u treću zemlju koja ne osigurava odgovarajuću razinu zaštite u smislu članka 25. stavka 2." ako je: i. to potrebno da bi se pružile usluge koje traži potrošač ili radi izvršenja ugovora, na primjer ugovora o „programu nagrađivanja putnika"; ili ii. ako je potrošač dao za to svoju nedvojbenu suglasnost. Organizacije iz SAD-a koje sudjeluju u sustavu zaštite privatnosti osiguravaju odgovarajuću zaštitu osobnih podataka i stoga mogu primati podatke prenesene iz EU-a bez ispunjivanja ovih uvjeta ili ostalih uvjeta iz članka 26. Direktive. Budući da sustav zaštite privatnosti uključuje posebna pravila za osjetljive podatke, takvi podaci (koji možda moraju biti prikupljeni, na primjer, vezano za potrebe korisnika za fizičkom pomoći) mogu biti uključeni u prijenose sudionicima u sustavu zaštite privatnosti. Međutim, u svim slučajevima organizacija koja prenosi informacije mora poštovati pravo države članice EU-a u kojoj djeluje, kojim se mogu, među ostalim, odrediti posebni uvjeti za postupanje s osjetljivim podacima.

14. **Farmaceutski i medicinski proizvodi**

a. Primjena prava država članica EU-a ili načela sustava zaštite privatnosti

Pravo države članice primjenjuje se na prikupljanje osobnih podataka i na obradu koja se obavlja prije prijenosa u Sjedinjene Američke Države. Načela sustava zaštite privatnosti primjenjuju se na podatke nakon njihova prijenosa u Sjedinjene Američke Države. Podatke koji se koriste za farmaceutsko istraživanje i ostale svrhe treba učiniti anonimnima kada je to prikladno.

b. Buduće znanstveno istraživanje

i. Osobni podaci razvijeni u određenim studijama medicinskih ili farmaceutskih istraživanja često imaju vrijednu ulogu u budućem znanstvenom istraživanju. Ako se osobni podaci prikupljeni za jednu istraživačku studiju prenose američkoj organizaciji u okviru sustava zaštite privatnosti, ta organizacija može se koristiti podacima za nove aktivnosti znanstvenog istraživanja podložno odgovarajućem obavješćivanju i mogućnosti izbora u prvom stupnju. Takva obavijesti treba sadržavati informacije o svim budućim posebnim korištenjima podataka, kao što je povremeno praćenje, povezano istraživanje ili marketing.

ii. Podrazumijeva se da ne mogu biti točno navedene sve buduće uporabe podataka budući da novo korištenje pri istraživanju može proizaći iz novih saznanja o izvornim podacima, novih medicinskih otkrića i napretka, te promjena u javnom zdravstvu i regulatornh promjena. Obavijest stoga treba uključivati, prema potrebi, objašnjenje da je moguće da će se osobni podaci koristiti u budućim medicinskim i farmaceutskim istraživanjima koja nisu predviđena. Ako uporaba nije u skladu s općom istraživačkom svrhom (svrhama) za koju su osobni podaci prvotno prikupljeni ili na koju je pojedinac pristao, mora se ishoditi novi pristanak.

c. Povlačenje iz kliničkog ispitivanja

Sudionici se mogu u bilo kojem trenutku odlučiti povući iz kliničkog ispitivanja ili se to od njih može tražiti. Svi podaci prikupljeni prije povlačenja ipak se mogu obraditi zajedno s ostalim podacima prikupljenima kao dio kliničkog ispitivanja, ako je to bilo pojašnjeno sudioniku u obavijesti u trenutku kada je pristao sudjelovati.

d. Prijenosi u regulatorne ili nadzorne svrhe

Poduzeća koja proizvode lijekove i medicinske proizvode smiju davati osobne podatke iz kliničkih ispitivanja provedenih u EU-u regulatornim tijelima u Sjedinjenim Američkim Državama za regulatorne i nadzorne potrebe. Slični prijenosi dopušteni su drugim strankama, kao što u su podružnice poduzeća i ostali istraživači, u skladu s načelima obavješćivanja i izbora.

e. „Slijepe” studije

i. Kako bi se zajamčila objektivnost kliničkih ispitivanja njihovi sudionici, a često i istraživači, ne mogu dobiti pristup informacijama koju terapiju dobiva koji sudionik. Otkrivanjem tih informacija ugrozila bi se valjanost istraživanja i rezultata. Sudionicima o takvim kliničkim ispitivanjima (koja se nazivaju „slijepe”) studije ne mora se osigurati pristup podacima o njihovom liječenju tijekom ispitivanja ako je to ograničenje objašnjeno kada je sudionik pristao sudjelovati u studiji i ako bi se otkrivanjem takvih informacija ugrozila cjelovitost istraživanja.

ii. Pristanak na sudjelovanje u ispitivanju pod tim uvjetima razuman je razlog za odricanje od prava pristupa. Nakon zaključenja ispitivanja i analize rezultata sudionici trebaju imati pristup svojim podacima ako to zatraže. Trebaju ga prvenstveno tražiti od liječnika ili drugih zdravstvenih djelatnika koji su ih liječili u sklopu kliničkog ispitivanja ili od poduzeća koje je sponzor.

f. Sigurnost proizvoda i praćenje učinkovitosti

Poduzeće koje proizvodi farmaceutske i medicinske proizvode ne mora primjenjivati načela sustava zaštite privatnosti u pogledu obavješćivanja, izbora, odgovornosti za daljnji prijenos i pristup u svojim aktivnostima praćenja sigurnosti i učinkovitosti proizvoda, uključujući izvješćivanje o neželjenim učincima i praćenju pacijenata/osoba koje uzimaju određene lijekove ili medicinske proizvode ako je poštovanje načela u suprotnosti sa zadovoljavanjem regulatornih zahtjeva. To se odnosi i na izvješća, na primjer, davatelja zdravstvene skrbi

poduzećima koja proizvode lijekove i medicinske proizvode i na izvješća poduzeća koja proizvode lijekove i medicinske proizvode državnim agencijama, poput Agencije za hranu i lijekove.

g. Šifrirani podaci

Podatke o istraživanju glavni istraživač redovito zaštićuje jedinstvenom šifrom na njihovom izvoru kako se ne bi mogao otkriti identitet pojedinih osoba čiji se podaci obrađuju. Farmaceutska poduzeća koja sponzoriraju takva istraživanja ne dobivaju šifru. Jedinstvenu šifru ima samo istraživač kako bi mogao identificirati sudionika istraživanja u posebnim okolnostima (npr. ako je potrebno praćenje liječenja). Prijenos tako šifriranih podataka iz EU-a u Sjedinjene Američke Države ne čini prijenos osobnih podataka na kojih se primjenjuju načela sustava zaštite privatnosti.

15. **Javna evidencija i javno dostupne informacije**

a. Organizacija mora primjenjivati načela sustava zaštite privatnosti u pogledu sigurnosti, cjelovitosti podataka i ograničenja svrhe, pravne zaštite, provedbe i odgovornosti na osobne podatke iz javno dostupnih izvora. Ta načela primjenjuju se i na osobne podatke prikupljene iz javne evidencije, odnosno iz evidencije koju vode državne agencije ili tijela na bilo kojoj razini i koji su na raspolaganju općoj javnosti.

b. Načela obavješćivanja, izbora ili odgovornosti za daljnji prijenos a ne moraju se primjenjivati na podatke iz javne evidencije ako oni nisu pomiješani s podacima iz evidencije koja nije javna i ako se poštuju uvjeti za savjetovanje koje je utvrdilo nadležno tijelo. Općenito nije nužno primjenjivati načela obavješćivanja, izbora i odgovornosti za daljnji prijenos na javno dostupne podatke osim ako europski prenositelj navede da takvi podaci podliježu ograničenjima zbog kojih organizacija mora primjenjivati ta načela za namjeravane uporabe. Organizacije neće biti odgovorne za to kako takve podatke koriste oni koji ih dobiju iz objavljenih materijala.

c. Ako se utvrdi da je organizacija namjerno objavila osobne podatke suprotno načelima kako bi ona ili ostali izvukli koristi od tih iznimaka, više neće imati pravo na pogodnosti sustava zaštite privatnosti.

d. Nije nužno primjenjivati načelo pristupa na podatke iz javne evidencije ako nisu povezani s ostalim osobnim podacima (osim malih količina podataka koji se upotrebljavaju za indeksaciju ili organizaciju informacija iz javne evidencije). Međutim, moraju se poštovati svi uvjeti za uvid koje je utvrdilo nadležno tijelo. Međutim, ako su podaci iz javne evidencije povezani s ostalim informacijama iz evidencije koja nije javna (osim kako je prethodno navedeno), organizacija mora omogućiti pristup svim takvim informacijama, uz pretpostavku da ne podliježe drugim dopuštenim iznimkama.

e. Kao što je slučaj s informacijama iz javne evidencije, nije potrebno omogućiti pristup informacijama koje su već javno dostupne široj javnosti, osim ako nisu povezane s informacijama koje nisu javno dostupne. Organizacije koje se bave prodajom javno dostupnih informacija mogu naplatiti uobičajenu naknadu organizacije kada odgovaraju na zahtjev za pristup. S druge strane, pojedinci mogu tražiti pristup svojim informacijama od organizacije koja je prvotno prikupila podatke.

16. **Zahtjevi javnih tijela za pristup**

a. Kako bi osigurale transparentnost u pogledu zakonitih zahtjeva javnih tijela za pristup osobnim podacima, organizacije u sustavu zaštite privatnosti mogu dobrovoljno objavljivati povremena izvješća o transparentnosti o broju zahtjeva za osobne podatke koje su zaprimile od javnih tijela za provedbu zakona ili iz razloga nacionalne sigurnosti, ako je takvo otkrivanje dopušteno u skladu s primjenjivim pravom.

b. Podaci koje su navele organizacije sustava zaštite privatnosti u tim izvješćima zajedno s podacima koje je objavila obavještajna zajednica, i ostali podaci, mogu se upotrebljavati za godišnje preispitivanje funkcioniranja sustava zaštite privatnosti u skladu s načelima.

c. Nepostojanjem obavijesti u skladu s točkom (a) podtočkom xiii. načela obavješćivanja ne sprječava se i ne ugrožava sposobnost organizacije da odgovori na bilo koji zakoniti zahtjev.

Prilog I.

Model arbiraže

U ovom Prilogu I. navedeni su uvjeti pod kojima su organizacije u sustavu zaštite privatnosti dužne obavljati arbitražu u skladu s načelom pravne zaštite, provedbe i odgovornosti. Mogućnost obvezujuće arbitraže koja je opisana u nastavku primjenjuje se na određena „preostala" potraživanja u vezi s podacima obuhvaćenima europsko-američkim sustavom zaštite privatnosti. Svrha je ove mogućnosti osobama osigurati mogućnost žurnog, neovisnog i poštenog mehanizma za rješavanje navodnih povreda načela koje nisu riješene drugim mehanizmima sustava za zaštitu privatnosti, ako ih ima.

A. **Područje primjene**

Ova mogućnost arbitraže dostupna je osobama kako bi mogle utvrditi, za preostala potraživanja, je li organizacija u sustavu zaštite privatnosti povrijedila svoju obvezu u skladu s načelima u pogledu pojedinca te je li ta povreda potpuno ili djelomično ispravljena. Ta je mogućnost dostupna samo u navedene svrhe. Ta mogućnost nije dostupna, primjerice, u pogledu izuzeća od načela ([1]) ili u odnosu na navode o primjerenosti sustava zaštite privatnosti.

B. **Dostupna pravna sredstva**

U skladu s ovom mogućnošću arbitraže, Odbor za sustav zaštite privatnosti (koji se sastoji od jednog ili tri arbitra, kako su dogovorile stranke) ima ovlasti odrediti pojedinačnu nenovčanu pravičnu naknadu (poput pristupa, ispravka, brisanja ili vraćanja predmetnih podataka osobe) koji su nužni za ispravak kršenja načela samo u pogledu pojedinca. To su jedine ovlasti arbiražnog odbora u pogledu pravnih sredstava. Kada razmatra pravne lijekove, arbitražni odbor mora uzeti u obzir druge pravne lijekove koji su već određeni drugim mehanizmima u okviru sustava zaštite privatnosti. Nisu dostupne odštete, nadoknade troškova, naknade ili druga pravna sredstva. Svaka stranka snosi vlastite troškove odvjetnika.

C. **Zahtjevi u postupku prije arbitraže**

Osoba koja odluči iskoristiti ovu mogućnost arbitraže mora poduzeti sljedeće korake prije podnošenja zahtjeva za arbitražu: 1. obavijestiti organizaciju o navodnoj povredi i dati joj priliku da riješi pitanje u roku iz odjeljka III.11točke (d) podtočke i. Načela; 2. iskoristiti neovisan mehanizam pravne zaštite u skladu s Načelima, koji je besplatan za pojedince; i 3. obratiti se Ministarstvu trgovine posredstvom svog nadležnog tijela za zaštitu podataka i omogućiti Ministarstvu trgovine da uloži najveće napore u besplatno rješavanje pitanja u rokovima iz dopisa Uprave za međunarodnu trgovinu Ministarstva trgovine.

Mogućnost arbitraže ne može se iskoristiti ako je navodna povreda načela (1) prethodno bila predmetom obvezujuće arbitraže; (2) bila predmetom konačne presude donesene u sudskom postupku čiji je ta osoba bila stranka ili (3) stranke su ju prethodno riješile. Nadalje, ta se mogućnost ne može iskoristiti ako nadležno tijelo EU-a za zaštitu podataka (1) ima ovlasti u skladu s odjeljcima III. 5 i III. 9 Načela ili (2) ima ovlasti riješiti navodnu povredu izravno s organizacijom. Nadležnost tijela za zaštitu podataka za rješavanje iste pritužbe protiv voditelja obrade podataka EU-a ne isključuje mogućnost uporabe ove mogućnosti arbitraže protiv druge pravne osobe koju ne obvezuje nadležnosti tijela za zaštitu podataka.

D. **Obvezujuća priroda odluka**

Odluka o uporabi ove obvezujuće mogućnosti arbitraže u potpunosti je dobrovoljna Arbitražna odluka obvezujuća je za sve stranke u arbitraži. Kada iskoristi mogućnost arbitraže osoba se odriče mogućnosti traženja pravne zaštite za istu navodnu povredu u drugom forumu, osim ako se nenovčanim pravnim lijekom ne ostvaruje potpuna nadoknada za navodnu povredu, iskorištavanje arbitraže ne isključuje zahtjev za odštetu koji se inače može podnijeti sudu.

([1]) Odjeljak 1.5. načela.

E. **Preispitivanje i provedba**

Osobe i organizacije u sustavu zaštite privatnosti moći će tražiti sudsko preispitivanje i izvršenje arbitražnih odluka u skladu sa zakonodavstvom EU-a, odnosno Saveznim zakonom o arbitraži ([1]). Takvi se postupci mogu pokrenuti pred saveznim okružnim sudom koji je mjesno nadležan za glavno sjedište organizacije su sustavu zaštite privatnosti.

Svrha je ove mogućnosti arbitraže rješavanje pojedinačnih sporova i arbitražne odluke ne moraju služiti kao uvjerljivi ili obvezujući presedan u pitanjima povezanima s drugim strankama, uključujući u budućim arbitražnim postupcima ili na sudovima EU-a ili SAD-a ili u postupcima FTC-a.

F. **Arbitražno vijeće**

Stranke biraju arbitre s popisa arbitara o kojem je riječ u nastavku.

U skladu s primjenjivim pravom, američko Ministarstvo trgovine i Europska komisija sastavit će popis od najmanje 20 arbitara koji se biraju na temelju neovisnosti, integriteta i stručnosti. Na taj se postupak primjenjuje sljedeće:

Arbitri:

1. ostaju na popisu 3 godine, osim u iznimnim okolnostima ili iz iznimnih razloga, i to se može obnoviti na dodatno razdoblje od 3 godine;

2. na primaju upute nijedne strane ni organizacije u sustavu zaštite privatnosti, ili od EU-a, bilo koje države članice ili drugog državnog tijela, javnog tijela ili izvršnog tijela i nisu s njima povezani i

3. moraju biti odvjetnici u SAD-u i stručnjaci za pravo zaštite privatnosti SAD-a te za pravo EU-a za zaštitu podataka.

G. **Arbitražni postupci**

U skladu s primjenjivim pravom, u roku od 6 mjeseci od donošenja odluke o odgovarajućoj zaštiti, Ministarstvo trgovine i Europska komisija slažu se da će se postupci pred Vijećem sustava za zaštitu privatnosti primjenjivati postojeći, uspostavljeni arbitražni postupci SAD-a (poput AAA-a ili JAMS-a), podložno sljedećim uvjetima:

1. Osoba može pokrenuti obvezujući arbitražni postupak u skladu sa prethodno navedenim zahtjevima u vezi s postupkom prije pokretanja arbitražnog postupka dostavljanjem „obavijesti" organizaciji. Obavijest sadržava sažetak koraka poduzetih u skladu s odlomkom C za rješavanje potraživanja, opis navedene potvrde i, ako osoba tako želi, prateće dokumente i materijale i/ili raspravu o pravu koje se odnosi na navodno potraživanje.

([1]) U poglavlju 2. Saveznog zakona o arbitraži (dalje u tekstu „FAA") predviđeno je da se na sporazum o arbitraži ili arbitražna odluka koji su posljedica pravnog odnosa, neovisno o tome je li riječ o ugovornom odnosu, koji se smatra poslovnim, među ostalim transakcija, ugovor ili sporazum opisan u [odjeljku 2. FAA-a] primjenjuje Konvencija [o priznavanju i izvršenju stranih arbitražnih odluka iz lipnja 10., 1958., 21 U.S.T. 2519, T.I.A.S. br. 6997 (dalje u tekstu „Konvencija iz New Yorka")]. 9 U.S.C. članak 202. U FAA-u je dalje predviđeno da „sporazum ili odluka proizašli iz tog odnosa koji su sklopljeni između državljana Sjedinjenih Američkih Država smatraju se obuhvaćenim Konvencijom iz New Yorka osim ako taj odnos uključuje imovinu koja se nalazi u inozemstvu, ako je njime predviđeno obavljanje ili izvršenje u inozemstvu ili ako ima neki drugi razumni odnos s jednom ili više stranih država." *Id.* U skladu s poglavljem 2. „svaka stranka u arbitraži može podnijeti zahtjev bilo kojem sudu koji je nadležan u skladu s ovim poglavljem da donese odluku kojom se potvrđuje odluka protiv druge stranke u arbitraži. Sud potvrđuje odluku osim ako utvrdi jednu od osnova za odbijanje ili odgađanje priznavanja ili izvršenja odluke navedenu u predmetnoj Konvenciji iz [New Yorka]." Id., članak 207. U poglavlju 2. dalje je predviđeno da „okružni sudovi Sjedinjenih Država. nadležni su za. mjeru ili postupak [u skladu s Konvencijom iz New Yorka], neovisno o spornom iznosu." Id., članak 203.
U poglavlju 2. također je propisano da se „poglavlje 1. primjenjuje na mjere i postupke pokrenute u skladu s ovim poglavljem ako to poglavlje nije u suprotnosti s ovim poglavljem ili Konvencijom iz [New Yorka] kako su ju ratificirale Sjedinjene Američke Države." Id., članak 208. S druge strane, u poglavlju 1. predviđeno je da „pisana odredba u ugovoru kao dokaz poslovne transakcije za rješavanje spora arbitražom koja proizlazi iz takvog ugovora ili transakcije ili odbijanja za izvršavanje cijelog ili dijela, ili pisani sporazum o pokretanju arbitraže zbog takvog ugovora, transakcije ili odbijanja, važeća je, neponištiva i izvršiva, osim na osnovama koje postoje u zakonu ili pravnom lijeku za raskid ugovora." Id., članak 2. točka (e). U poglavlju 1. dalje je predviđeno da „svaka stranka u arbitraži može se od navedenog suda tražiti nalog o potvrdi odluke i sud mora potom odobriti takav nalog osim ako je odluka nevažeća, izmijenjena ili ispravljena kako je navedeno u odjeljcima 10. i 11. FAA-a". Id., članak 9.

2. Razvijaju se postupci kojima će se osigurati da osoba ne može primijeniti dvostruku pravnu zaštitu ili provoditi dvostruke postupke za istu navodnu povredu.

3. Postupak FTC-a može se provoditi usporedno s arbitražnim postupkom.

4. U tim arbitražnim postupcima niti može sudjelovati niti jedan predstavnik SAD-a, EU-a ili bilo koje države članice EU-a ili nekog drugog državnog, javnog ili izvršnog tijela osim na zahtjev osobe iz EU-a, nadležna tijela za zaštitu podataka iz EU-a mogu pružiti pomoć samo s pripremom obavijesti, ali ta nadležna tijela za zaštitu podataka iz EU-a ne smiju imati pristup otkrivanju ili drugim materijalima povezanim s arbitražnim postupkom.

5. Arbitraža se provodi u Sjedinjenim Američkim Državama i osoba može izabrati sudjelovanje videokonferencijom ili telefonom, koje mu se osigurava bez dodatnog troška. Osobna nazočnost neće biti obavezna.

6. Jezik arbitraže bit će engleski, osim ako stranke dogovore drugačije. Na razuman zahtjev i ovisno o tome zastupa li osobu odvjetnik, tumačenje na arbitražnoj raspravi i prijevod materijala za arbitražu osiguravaju se besplatnu, osim ako odbor odluči da bi, s obzirom na okolnosti određene arbitraže, time nastali neopravdani ili nerazmjerni troškovi.

7. Materijali dostavljeni arbitrima smatraju se povjerljivima i upotrebljavat će se samo u vezi s arbitražnim postupkom.

8. Podatke je moguće otkriti određenoj osobi, ako je potrebno i stranke to otkrivanje drže u tajnosti i upotrebljavaju samo u vezi s arbitražom.

9. Arbitraže se dovršavaju u roku od 90 dana od dostavljanja obavijesti predmetnoj organizaciji, osim ako su stranke dogovorile drugačije.

H. **Troškovi**

Arbitri poduzimaju razumne korake kako bi troškove ili naknade za arbitražu sveli na najveću moguću razinu.

U skladu s primjenjivim pravom, Ministarstvo trgovine pomaže s uspostavom fonda u koji će organizacije sudionice u sustavu zaštite privatnosti svake godine morati uplaćivati godišnji doprinos koji se djelomično temelji na veličini organizacije i kojim će biti obuhvaćeni troškovi arbitraže, među ostalim naknade za arbitre, do najvećeg iznosa („gornje granice”), u dogovoru s Europskom komisijom. Fondom upravlja treća stranka koja redovito izvješćuje o radu fonda. U okviru godišnjeg preispitivanja Ministarstvo trgovine i Europska komisija preispituju funkcioniranje fonda, među ostalim potrebu za prilagodbom iznosa doprinosa i uzimaju u obzir, među ostalim, broj provedenih arbitražnih postupaka i troškove i rokove provođenja arbitraže te potvrđuju da se organizacijama u sustavu zaštite privatnosti neće nametati pretjerano financijsko opterećenje. Troškovi odvjetnika nisu obuhvaćeni ovom odredbom ili kao ni bilo kojim fondom iz ove odredbe.

PRILOG III.

Dopis Državnog tajnika SAD-a, Johna Kerryja

7. srpnja 2016.

Poštovana povjerenice Jourová,

Zadovoljan sam da smo uspjeli postići dogovor o europsko-američkom sustavu zaštite privatnosti koji će uključivati mehanizam pravobranitelja posredstvom kojeg će nadležna tijela EU-a moći podnositi zahtjeve u ime osoba iz EU-a u vezi s praksom SAD-a koja se sastoji od prikupljanja obavještajnih podataka elektroničkim izviđanjem.

Predsjednik Barack Obama najavio je 17. siječnja 2014. važne reforme obavještajnog sustava koje su navedene u Predsjedničkom ukazu br. 28 (PPD-28). U skladu s ukazom PPD-28 imenovao sam zamjenicu Državnog tajnika, Catherine A. Novelli, koja također obavlja dužnost višeg koordinatora međunarodne diplomacije u području informacijske tehnologije, kao kontaktnu točku za strane vlade koje žele izraziti svoju zabrinutost u vezi s aktivnostima SAD-a u vezi s prikupljanjem obavještajnih podataka elektroničkim izviđanjem. Na temelju te uloge uspostavio sam mehanizam pravobranitelja za sustav zaštite privatnosti u skladu s uvjetima iz Priloga A, koji su ažurirani nakon mog dopisa od 22. veljače 2016. Tu sam dužnost povjerio zamjenici Državnog tajnika, gđi. Novelli. Zamjenica Državnog tajnika, gđa. Novelli, neovisna je od američke obavještajne zajednice i odgovara izravno meni.

Dao sam upute svom osoblju da izdvoje nužne resurse za provedbu ovog novog mehanizma pravobranitelja i uvjeren sam da će on biti učinkovito sredstvo za rješavanje pitanja osoba iz EU-a.

S poštovanjem,

John F. Kerry

Prilog A

Mehanizam pravobranitelja za europsko-američki sustav za zaštitu privatnosti u vezi prikupljanja obavještajnih podataka elektroničkim izviđanjem

Kao priznanje važnosti okvira europsko-američkog sustava zaštite privatnosti, u ovoj Memorandumu utvrđuje se postupak za provedbu ovog novog mehanizma u skladu s Predsjedničkim ukazom br. 28 (PPD-28) u vezi s prikupljanjem obavještajnih podataka elektroničkim izviđanjem ([1]).

Predsjednik Obama održao je 17. siječnja 2014. govor u kojem je najavio važne reforme obavještajnog sustava. U tom govoru on je istaknuo da „naša nastojanja da pomognemo zaštititi ne samo naš narod već i naše prijatelje i saveznike. Naši napori bit će učinkoviti samo ako obični građani iz drugih zemalja budu uvjereni da Sjedinjene Američke Države poštuju i njihovu privatnost." Predsjednik Obama najavio je donošenje novog predsjedničkog ukaza – PPD-28 – u kojem će „biti jasno propisano što smijemo, a što ne smijemo raditi, u slučaju prekomorskog nadzora."

U odjeljku 4. točki (d) PPD-28 ministru vanjskih poslova određuje se zadaća da imenuje „Višeg koordinatora međunarodne diplomacije u području informacijske tehnologije" (Viši koordinator) „koji će … biti kontaktna točka za strane vlade koje žele izraziti zabrinutost u vezi s aktivnostima prikupljanja obavještajnih podataka elektroničkim izviđanjem koje obavljaju Sjedinjene Američke Države." Zamjenica ministra vanjskih poslova, gđa. C. Novelli, obavlja dužnost Više koordinatorice od siječnja 2015.

U ovom memorandumu opisan je novi mehanizam kojim će se omogućiti Višoj koordinatorici da lakše obrađuje zahtjeve povezane s pristupom podacima prenesenima iz EU-a u Sjedinjene Američke Države u okviru sustava zaštite privatnosti za potrebe nacionalne sigurnosti, sa standardnim ugovornim odredbama, obvezujućim korporativnim pravilima (BRC), „odstupanjima" ([2]) ili „mogućim budućim odstupanjima" ([3]) sredstvima utvrđenima u primjenjivim zakonima i politikama Sjedinjenih Američkih Država te da odgovara na te zahtjeve.

1. **Pravobranitelj za sustav zaštite podataka** Viši koordinator obavlja dužnost pravobranitelja za sustav zaštite privatnosti i imenuje dodatne službenike Ministarstva vanjskih poslova da mu pomognu u obavljaju dužnosti navedenih u memorandumu. (dalje u tekstu, koordinator i svi službenici koji obavljaju takve dužnosti nazivaju se „pravobraniteljem za sustav zaštite privatnosti"). Pravobranitelj za sustav zaštite privatnosti blisko će surađivati s odgovarajućim dužnosnicima iz drugih odjela i agencija koji su odgovorni za obradu zahtjeva u skladu s primjenjivim američkim zakonodavstvom i politikom. Pravobranitelj djeluje neovisno od obavještajne zajednice. Pravobranitelj izravno izvješćuje ministra vanjskih poslova koji će pravobranitelju osigurati objektivno obavljanje dužnosti, neovisno od bilo kakvog neprimjerenog utjecaja koje bi moglo imati učinka na odgovor koji treba pružiti.

2. **Učinkovita koordinacija.** Pravobranitelj za sustav zaštite privatnosti može se učinkovito naslanjati na rad nadzornih tijela, opisanih u nastavku, i koordinirati njima u cilju osiguranja odgovarajućeg odgovora na dopise tijela koje rješava

([1]) Ako odluka Komisije o primjerenosti zaštite koju pružaju europsko-američki sustav zaštite privatnosti primjenjuje na Island, Lihtenštajn i Norvešku, paket o sustavu zaštite privatnosti obuhvatit će Europsku uniju te tri navedene zemlje. Stoga se smatra da upućivanja na EU i države članice uključuju Island, Lihtenštajn i Norvešku.

([2]) „Odstupanja" u ovom kontekstu znače komercijalni prijenos ili prijenose koji se odvijaju pod sljedećim uvjetima: (a) osoba čiji se podaci obrađuju dala je svoju nedvosmislenu suglasnost predloženom prijenosu; ili (b) prijenos je potreban radi izvršenja ugovora između osobe čiji se podaci obrađuju i voditelja obrade ili provedbe predugovornih mjera poduzetih na zahtjev osobe čiji se podaci obrađuju ili (c) prijenos je potreban za sklapanje ili izvršenje ugovora sklopljenog između voditelja osobe i treće strane u interesu osobe čiji se podaci obrađuju ili (d) prijenos je potreban ili propisan zakonom radi važnog javnog interesa ili uspostave, izvršenja ili obrane prava na pravne zahtjeve ili (e) prijenos je potreban kako bi se zaštitili vitalni interesi osobe čiji se podaci obrađuju ili (f) prijenos se obavlja iz evidencije koja u skladu sa zakonima ili propisima treba javnosti pružiti podatke i koja je na raspolaganju javnosti općenito ili svakoj osobi koja može dokazati svoj zakoniti interes u mjeri u kojoj su u određenom slučaju ispunjeni uvjeti u vezi dostupnosti propisani zakonom.

([3]) „Moguća buduća odstupanja" u ovom kontekstu znače komercijalni prijenos ili prijenose koji se odvijaju pod jednim od sljedećih uvjeta u mjeri u kojoj uvjet predstavlja zakonitu osnovu za prijenose osobnih podataka iz EU-a u SAD: (a) osoba čiji se podaci obrađuju izričito je pristala na predloženi prijenos nakon što je bila obaviještena o mogućim rizicima takvih prijenosa za ispitanika zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera; ili (b) prijenos je nužan za zaštitu životno važnih interesa osoba čiji se podaci obrađuju ili drugih osoba ako osoba čiji se podaci obrađuju fizički ili pravno ne može dati suglasnost ili (c) ako se prijenos u treću zemlju ili međunarodnu organizaciju može izvršiti samo ako se ne ponavlja, a ne primjenjuju se druga odstupanja ili eventualna buduća odstupanja ako se odnosi na ograničen broj osoba čiji se podaci obrađuju, ako je nužan iz obveznih zakonitih interesa koje ostvaruje voditelj obrade, a nad kojima ne prevladavaju interesi, prava ili slobode osobe čiji se podaci obrađuju, ako je voditelj obrade ocijenio sve okolnosti povezane s prijenosom podataka i na temelju te procjene donio je odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka.

prigovor osoba iz EU-a. Kad se zahtjeva odnosi na usklađenost nadzora sa zakonima SAD-a, pravobranitelj za sustav zaštite privatnosti može surađivati s jednim od neovisnih nadzornih tijela koje ima istražne ovlasti.

a. Pravobranitelj za sustav zaštite privatnosti blisko surađuje s drugim državnim službenicima Sjedinjenih Država, među ostalim s odgovarajućim neovisnim nadzornim tijelima, kako bi osigurao obradu i rješavanje popunjenih zahtjeva u skladu s primjenjivim zakonima i politikama. Pravobranitelj za sustav zaštite privatnosti posebno može blisko surađivati s Uredom direktora Nacionalne obavještajne službe, Ministarstvom pravosuđa i ostalim ministarstvima i agencijama koje sudjeluju u sustavu nacionalne sigurnosti Sjedinjenih Američkih Država, prema potrebi, i s glavnim inspektorima, službenicima koji provode Zakon o pravu na pristup informacijama i službenicima za zaštitu građanskih sloboda i privatnosti.

b. Vlada Sjedinjenih Američkih država oslanja se na mehanizme koordinacije i nadzora pitanja nacionalne sigurnosti u različitim ministarstvima i agencijama kako bi osigurala da pravobranitelj za sustav zaštite privatnosti može odgovoriti u smislu članka 4. točke (e) na popunjene zahtjeve iz odjeljka 3. točke (b).

c. Pravobranitelj za sustav zaštite privatnosti može pitanja uputiti na razmatranje Nadzornom odboru za zaštitu privatnosti i građanskih sloboda.

3. **Podnošenje zahtjeva.**

a. Zahtjev se u početku podnosi nadzornim tijelima u državama članicama koja su nadležna za nadzor službi za nacionalne sigurnosne usluge i/ili obradu osobnih podataka koju provode tijela javne vlasti. Zahtjev će pravobranitelju podnijeti središnje tijelo EU-a (dalje u tekstu: „tijelo EU-a za rješavanje pojedinačnih pritužbi").

b. Tijelo EU-a za rješavanje pojedinačnih pritužbi sljedećim postupcima provjerava potpunost zahtjeva:

i. provjerom identiteta osobe te da ta osoba djeluje u vlastito ime, a ne kao predstavim vladine ili međuvladine organizacije;

ii. provjerom da je zahtjev podnesen u pisanom obliku i da sadržava sljedeće osnovne podatke:

— sve podatke koji čine osnovu zahtjeva,

— prirodu informacija ili tražene pravne zaštite,

— državna tijela Sjedinjenih Američkih Država za koje se vjeruje da su uključena, ako ih ima, i

— druge mjere kojima se nastoje prikupiti informacije ili traženi pravni lijek te odgovor zaprimljen uporabom tih mjera;

iii. provjerom da se zahtjev odnosi na podatke za koje se razumno vjeruje da su preneseni iz EU-a u Sjedinjene Američke Države u skladu sa sustavom zaštite privatnosti, SCC-om, BCR-om, odstupanjima ili budućim mogućim odstupanjima;

iv. početnom provjerom da zahtjev nije neozbiljan, neugodan ili podnesen u lošoj vjeri.

c. Da bi se smatrao potpunim za potrebe daljnje obrade pravobranitelja za sustav zaštite privatnosti u skladu s ovim memorandumom, zahtjevom nije potrebno dokazati da je vlada Sjedinjenih Američkih država pristupila podacima tražitelja s pomoću aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem.

4. **Obveze komunikacije s tijelom EU-a za rješavanje pojedinačnih pritužbi koje je podnijelo zahtjev.**

a. Pravobranitelj za sustav zaštite privatnosti potvrdit će primitak zahtjeva tijelu EU-a za rješavanje pojedinačnih pritužbi koje je podnijelo zahtjev.

b. Pravobranitelj za sustav zaštite privatnosti prvo će preispitati je li zahtjev popunjen u skladu s odjeljkom 3. (b). Ako pravobranitelj za sustav zaštite privatnosti uoči nedostatke ili ima pitanja u vezi s popunjavanjem zahtjeva, pravobranitelj za sustav zaštite privatnosti nastoji to riješiti s nadležnim tijelom EU-a za rješavanje pojedinačnih zahtjeva koje je podnijelo zahtjev.

c. Ako, kako bi se olakšala primjerena obrada zahtjeva, pravobranitelj za sustav zaštite privatnosti treba više informacija o zahtjevu ili ako osoba koja je izvorno podnijela zahtjev mora poduzeti posebne mjere, pravobranitelj za sustav zaštite privatnosti o tome obavješćuje tijelo EU-a za rješavanje pojedinačnih pritužbi koje je podnijelo zahtjev.

d. Pravobranitelj za sustav zaštite privatnosti pratit će stanje zahtjeva i obavješćivati tijelo EU-a za rješavanje pojedinačnih zahtjeva koje je podnijelo zahtjev.

e. Kada je zahtjev popunjen kako je opisano u odjeljku 3. ovog memoranduma, pravobranitelj za sustav zaštite privatnosti pravovremeno daje odgovarajući odgovor tijelu EU-a za rješavanje pojedinačnih zahtjeva koje je podnijelo zahtjev podložno trajnoj obvezi zaštite informacija u skladu s primjenjivim zakonima i politikama. Pravobranitelj za sustav zaštite privatnosti daje odgovor nadležnom tijelu EU-a za rješavanje pojedinačnih pritužbi koje je podnijelo zahtjev potvrđujući i. da je obavljena pravila istraga navoda iz pritužbe i ii. da se postupilo u skladu sa zakonom, propisima, izvršnim nalozima, predsjedničkim ukazima i politikama agencije kojima se osiguravaju ograničenja i zaštitne mjere opisane u dopisu ODNI-ja ili, u slučaju neusklađenosti, da je takva neusklađenost ispravljena. Pravobranitelj za sustav zaštite privatnosti neće potvrditi ni poreći je li osoba bila predmetom nadzora i neće potvrditi je li poduzeta određena pravna zaštita. Kako je dalje objašnjeno u odjeljku 5. zahtjevi FOIA obrađivat će se u skladu s tim zakonom i primjenjivim propisima.

f. Pravobranitelj za sustav zaštite privatnosti izravno će komunicirati s tijelom EU-a za rješavanje pojedinačnih pritužbi koje će biti odgovorno za komunikaciju s osobom koja je podnijela zahtjev. Ako je izravna komunikacija dio jednog od postupaka opisanih u nastavku, te će se komunikacija odvijati u skladu s postojećim postupcima.

g. Obveze iz ovog memoranduma ne primjenjuju se na opće tvrdnje da je europsko-američki sustav zaštite privatnosti nije u skladu sa zahtjevima Europske unije za zaštitu podataka. Obveze iz ovog memoranduma temelje se na dogovoru Europske komisije i vlade SAD-a da, s obzirom na opseg obveza iz mehanizma, mogu nastati ograničenja povezana s resursima, među ostalim u pogledu zahtjeva iz Zakona o pravu na pristup informacijama (FOIA). Ako izvršavanje funkcija pravobranitelja za zaštitu podataka u okviru sustava zaštite privatnosti prekoračuje razumna ograničena resursa i sprječava ispunjenje tih obveza, vlada EU-a razmotrit će se Europskom komisijom sve prilagodbe koje su primjerene za rješavanje situacije.

5. **Zahtjevi za pristup informacijama** Zahtjevi za pristup evidenciji Sjedinjenih Američkih Država podnose se i obrađuju u skladu sa Zakonom o pravu na pristup informacijama (FOIA).

a. FOIA-om su svakoj osobi osigurana sredstva za traženje pristupa postojećoj evidenciji savezne agencije, neovisno o državljanstvu tražitelja. Taj zakon dio je Zakonika Sjedinjenih Američkih država pod brojem 5. U.S.C., članak 552. Zakon i dodatne informacije o njemu dostupni su na www.FOIA.gov i http://www.justice.gov/oip/foia-resources. Svaka agencija ima glavnog službenika za FOIA i na svom web-mjestu navodi kako se agenciji podnosi zahtjev za pristup informacijama. Agencije su uspostavile postupke za uzajamno savjetovanje u vezi sa zahtjevima u skladu sa FOIA-om koji se odnose na evidenciju druge agencije.

b. Na primjer:

i. Ured direktora Nacionalne obavještajne službe (ODNI) uspostavio je portal za FOIA za ODNI: http://www.dni.gov/index.php/about-this-site/foia. Na tom portalu navedene su informacije o podnošenju zahtjeva, provjeri statusa postojećeg zahtjeva i pristupu informacijama koje je ODNI objavio u skladu s FOIA. Portal ODNI-ja za FOI-a sadržava poveznice na druga web-mjesta FOIA-e za subjekte obavještajne zajednice: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii. Ured za politiku informiranja Ministarstva pravosuđa daje opsežne informacije o FOIA-u. http://www.justice.gov/oip. Te informacije uključuju ne samo informacije o podnošenju zahtjeva u skladu s FOIA-om Ministarstvu pravosuđa već i smjernice američkoj vladi o tumačenju i primjeni zahtjeva FOIA.

c. U skladu sa FOIA-om, na pristup državnoj evidenciji primjenjuju se određene navedene iznimke: One uključuju ograničenja pristupa klasificiranim podacima povezanima s nacionalnom sigurnošću, osobnim podacima trećih osoba i podacima o istragama tijela za provedbu zakona i mogu se usporediti s ograničenjima koja je odredila svaka država članica EU-a vlastitim zakonom o pristupu podacima. Ta se ograničenja jednako primjenjuju na američke državljane i osobe koje nisu američki državljani.

d. Protiv odluka u sporovima o puštanju evidencije zatraženom u skladu s FOIA-om moguće je podnijeti upravu žalbu ili žalbu saveznom sudu. Sud je dužan ponovno utvrditi je li neotkrivanje podataka u skladu sa zakonom, 5. U.S.C. članak 552. točka (a) podtočka 4. (B) i može obvezati vladu da osigura pristup evidenciji. U nekim slučajevima sudovi su odbacili tvrdnje vlade da se podaci ne bi trebali otkriti jer su klasificirani. Iako nije moguće tražiti naknadu novčane štete, sudovi mogu dodijeliti nadoknadu odvjetničkih troškova.

6. **Razlozi za daljnje djelovanje.** Zahtjev u kojem se tvrdi da je došlo do povrede zakona ili drugog prekršaja upućuju se odgovarajućem nadležnom tijelu američke vlade, među ostalim neovisnim nadzornim tijelima, koje ima ovlasti istražiti predmetni zahtjev i riješiti prethodno opisano pitanje neusklađenosti.

a. Glavni inspektori zakonski su neovisni, imaju široke ovlasti provoditi istrage, revizije i preispitivanja programa, među ostalim prijevare i zlouporabe ili povrede zakona i mogu preporučiti korektivne mjere.

i. U Zakonu o glavnom inspektoru iz 1978, kako je izmijenjen, propisano je da su glavni inspektori neovisne i objektivne jedinice u većini agencija čije dužnosti obuhvaćaju suzbijanje otpada, prijevare i zlouporabe u programima i operacijama njihovih agencija. U tu svrhu svaki je glavni inspektor odgovoran provoditi revizije i istrage povezane s programima i operacijama svoje agencije. Nadalje, glavni inspektori osiguravaju vodstvo i koordinaciju i preporučuju politike za djelovanja kojima se promiče ekonomičnost, djelotvornost i učinkovitost i otkrivaju prijevaru i zlouporabu u programima i operacijama agencije.

ii. Svaki subjekt obavještajne zajednice ima vlastiti Ured glavnog inspektora koji je odgovoran za nadzor stranih obavještajnih aktivnosti i drugih pitanja. Brojna su izvješća glavnog inspektora o obavještajnim programima javno objavljena.

iii. Na primjer:

— Ured glavnog inspektora obavještajne zajednice (IC IG) osnovan je u skladu s odjeljkom 405. Zakona o odobrenju prikupljanja obavještajnih podataka za fiskalnu godinu 2010. http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf Glavni inspektor obavještajne zajednice odgovoran je za provođenje revizije, istraga, inspekcija i preispitivanja u cijeloj obavještajnoj zajednici i za uklanjanje sustavnih rizika, osjetljivosti i nedostataka, koji se javljaju u svim misijama agencija obavještajne zajednice, kako bi se ostvario pozitivan učinak na gospodarstva i učinkovitosti u cijeloj obavještajnoj zajednici. Ured glavnog inspektora obavještajne zajednice ovlašten je za istrage pritužbi ili informacija o navodnim povredama zakona, pravila, propisa, otpadu, zlouporabi ovlasti ili znatnoj i posebnoj opasnosti za javno zdravlje i sigurnost u vezi s ODNI-jem i/ili obavještajnim programima ili aktivnostima obavještajne zajednice. Ured glavnog inspektora obavještajne zajednice daje informacije o tome kako mu se izravno obratit radi podnošenja izvješća: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Ured glavnog inspektora u američkom Ministarstvu pravosuđa (DOJ) https://www.justice.gov zakonom je osnovano neovisno tijelo čija je misija otkrivati i sprječavati otpad, prijevaru, zlouporabu i neispravno provođenje programa Ministarstva pravosuđa i osoblja te promicanje ekonomičnosti i učinkovitosti tih programa. Ured glavnog inspektora istražuje navodne povrede kaznenih i građanskih zakona koje su počinili zaposlenici Ministarstva pravosuđa te obavlja revizije i preglede programa Ministarstva pravosuđa. Ured glavnog inspektora nadležan je za sve pritužbe na neprimjereno postupanje zaposlenika Ministarstva pravosuđa, među ostalim Saveznog istražnog ureda; Uprave za droge; Savezne uprave za zatvore; Službe U. S. Marshals; Ureda za alkohol, duhan, oružje i eksplozive; urede državnih odvjetnika Sjedinjenih Američkih država i zaposlenika koji rade u drugim odjelima ili uredima Ministarstva pravosuđa. (Jedina je iznimka da je za navode neprimjerenom postupanju odvjetnika odjela ili osoblja za provedbu zakona koje se odnosi

na izvršavanje ovlasti odvjetnika odjela za istrage, vođenje postupka ili davanje pravnih savjeta odgovoran Ured za profesionalnu odgovornost.) Nadalje, u odjeljku 1001. američkog Zakona o borbi protiv terorizma, koji je stupio na snagu 26. listopada 2001., pripisano je da glavni inspektor preispituje informacije i zaprima pritužbe o navodnim povredama građanskih prava i sloboda koje su počinili zaposlenici Ministarstva pravosuđa. Ured glavnog inspektora održava javno web-mjesto– https://www.oig.justice.gov – na kojem se nalazi i poveznica za podnošenje pritužbi – https://www.oig.justice.gov/hotline/index.htm.

b. Uredi i subjekti za zaštitu privatnosti i građanske slobode vlade Sjedinjenih Američkih Država također imaju relevantne odgovornosti. Na primjer:

i. Odjeljkom 803. Provedbenih preporuka Akta Komisije 9/11 iz 2007., koja je kodificirana u Zakonik Sjedinjenih Američkih Država pod br. 42 U.S.C. članak 2000.-ee1, uspostavljaju se uredi za zaštitu privatnosti i građanske slobode u određenim ministarstvima i agencijama (među ostalim u Ministarstvu vanjskih poslova, Ministarstvu pravosuđa i ODNI-ju.). U odjeljku 803. navedeno je da će ti službenici za privatnost i građanske slobode biti glavni savjetnici, kako bi se osiguralo, među ostalim, da to ministarstvo, agencija ili subjekt imaju uspostavljene primjerene postupke za rješavanje pritužbi osoba koje tvrde da je to ministarstvo, agencija ili subjekt prekršilo njihovu privatnost ili građanske slobode.

ii. Na čelu Ureda ODNI-ja za građanske slobode i privatnost (ODNI CLPO) nalazi se službenik ODNI-ja za zaštitu građanskih sloboda. To je mjesto uspostavljeno Zakonom o nacionalnoj sigurnosti iz 1948., kako je izmijenjen. Dužnosti Ureda ODNI-ja za građanske slobode i privatnost uključuju osiguravanje da politike i postupci subjekata obavještajne zajednice uključuju odgovarajuće zaštite privatnosti i građanskih sloboda i preispitivanje i istrage pritužbi o navodnoj zlouporabi ili povredi građanskih sloboda i privatnosti u programima i aktivnostima ODNI-ja. Ured ODNI-ja za građanske slobode i privatnost objavljuje informacije javnosti na svom *web*-mjestu, uključujući upute o tome kako podnijeti pritužbu: www.dni.gov/clpo. Ako Ured ODNI-ja za građanske slobode i privatnost zaprimi pritužbu povezanu s privatnošću i građanskim slobodama u vezi s programima i aktivnostima obavještajne zajednice, on će surađivati s drugim subjektima obavještajne zajednice na tome kako dalje rješavati tu pritužbu u obavještajnoj zajednici. Imajte na umu da Nacionalna sigurnosna agencija (NSA) također ima Ured za građanske slobode i privatnost čije su odgovornosti navedene na njezinim internetskim stranicama – https://www.nsa.gov/civil_liberties/. Ako informacije upućuju na to ta neka agencija ne ispunjuje zahtjeve privatnosti (*npr.*, zahtjev iz odjeljka 4.PPD-28), tada agencije imaju mehanizme usklađenosti za preispitivanje i ispravljanje incidenta. Agencije su dužne DNI-ju prijaviti incidente povezane sa poštovanjem načela u skladu s PPD-28.

iii. Ured za privatnost i građanske slobode (OPCL) pri Ministarstvu pravosuđa pomaže glavnom službeniku Ministarstva za privatnost i građanske slobode u izvršavanju dužnosti i odgovornosti (CPCLO). Glavna je misija OPCL-a zaštititi privatnost i građanske slobode američkih državljana preispitivanjem, nadzorom i koordinacijom operacija Ministarstva povezanih s privatnošću. Ured za privatnost i građanske slobode daje pravne savjete i smjernice dijelovima Ministarstva; osigurava da Ministarstvo poštuje zahtjeve privatnosti, među ostalim Zakon o privatnosti iz 1974., odredbe o privatnosti Zakona o e-vladi iz 2002. i Saveznog zakona o upravljanju sigurnošću informacija te državne političke smjernice izdane u skladu s tim zakonima; razvija i pruža osposobljavanje Odjela o pitanjima privatnosti; pomaže CPCLO-u s razvojem politike privatnosti Ministarstva; priprema izvješća povezana s privatnošću za Predsjednika i Kongres; i preispituje prakse postupanja s informacijama u Ministarstvu kako bi osiguralo da su te prakse u skladu sa zaštitom privatnosti i građanskih sloboda. OPCL daje javnosti informacije o svojim odgovornostima na http://www.justice.gov/opcl.

iv. U skladu s 42. U.S.C. članak 2000.ee *i dalje*, Odbor za nadzor privatnosti i građanskih sloboda trajno preispituje politike i postupke ministarstava, agencija i subjekata izvršne vlasti koji se odnose na napore usmjerene na zaštitu države od terorizma kako bi se osigurala zaštita privatnosti i građanskih sloboda te njihovu provedbu i ii. druge mjere izvršne vlasti povezane s tim naporima kako bi utvrdio jesu li te mjere primjerene za zaštitu privatnosti i građanskih sloboda i jesu li u skladu s primjenjivim zakonima, propisima i politikama u području privatnosti i građanskih sloboda. On će također primati i preispitivati izvješća i druge informacije od službenika za zaštitu privatnosti i građanske slobode i, prema potrebi, davati im preporuke u vezi s njihovim aktivnostima. Odjeljkom 803. Provedbenih preporuka Akta Komisije 9/11 iz 2007., koja je kodificirana pod br. 42 U.S.C. članak 2000.-ee1, usmjeravaju se službenici za privatnost i građanske slobode iz osam saveznih agencija (među ostalim, Ministarstva vanjskih poslova, Ministarstva domovinske sigurnosti, direktora Nacionalne obavještajne službe i direktora Središnje obavještajne agencije (CIA)) i svih dodatnih

agencija koje odredi Odbor, da podnose povremena izvješća PCLOB-u, među ostalim o broju, prirodi i rješenju pritužbi koje je predmetna agencija zaprimila zbog navodnih povreda. Prema statutu PCLOB-a, Odbor može zaprimati ta izvješća i, prema potrebi, davati preporuke službenicima za privatnost i građanske slobode u vezi s njihovim aktivnostima.

PRILOG IV.

Dopis predsjednice Savezne trgovinske komisije Edith Ramirez

7. srpnja 2016.

Zaprimljen E-poštom

Věra Jourová
Povjerenica za pravosuđe, zaštitu potrošača i ravnopravnost spolova
Europska komisija
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgija

Poštovana povjerenice Jourová,

Savezna trgovinska komisija Sjedinjenih Američkih Država (dalje u tekstu „FTC") zahvaljuje na prilici da opiše svoju provedbu novog europsko-američkog okvira za zaštitu privatnosti („Okvir za zaštitu privatnosti" ili „Okvir"). Vjerujemo da će Okvir imati ključnu ulogu u olakšavanju poslovnih transakcija kojima se štiti privatnost u svijetu koji je sve više međusobno povezan. Time će se omogućiti poduzećima da obavljaju važne operacije u globalnom gospodarstvu i istodobno osiguraju da potrošači iz EU-a zadrže važnu zaštitu privatnosti. FTC je opredijeljen za prekograničnu zaštitu privatnosti i provedba novog okvira bit će mu prioritet. Nadalje objašnjavamo objašnjavamo protekla opća nastojanja FTC-a da osigura zaštitu privatnosti, među ostalim provedbu izvornog programa „sigurne luke" te prikazujemo pristup FTC-a provedbi novog Okvira.

FTC je prvi puta javno izjavio svoju opredijeljenost za provođenje programa „sigurne luke" iz 2000. Tada je predsjednik FTC-a, Robert Pitofsky, poslao Europskoj komisiji dopis u kojem je naveo da se FTC obvezuje strogo provoditi načela zaštite privatnosti programa „sigurne luke". FTC je nastavio izvršavati tu obvezu s pomoću gotovo 40 mjera provedbe, brojnih dodatnih istraga i suradnje s europskim tijelima za zaštitu podataka (dalje u tekstu: nadležna tijela za zaštitu podataka iz EU-a) na pitanjima od uzajamnog interesa.

Kada je Europska komisija u studenome 2013. izrazila zabrinutost u pogledu upravljanja programom „sigurne luke" i njegove provedbe, zajedno s Ministarstvom trgovine SAD-a započeli smo savjetovanje sa službenicima Europske komisije kako bismo istražili moguće načine njegovog jačanja. Dok je to savjetovanje još bilo u tijeku, Sud EU-a donio je 6. listopada 2015. odluku u predmetu*Schrems* kojom je, među ostalim, poništena odluka Europske komisije o primjerenosti programa „sigurne luke". Nakon te odluke nastavili smo blisko surađivati s Ministarstvom trgovine i Europskom komisijom kako bismo zajedno ojačali zaštitu privatnosti koja se pruža pojedincima iz EU-a. Okvir sustava za zaštitu privatnosti rezultat je tih trajnih savjetovanja. Kao i u slučaju programa „sigurne luke", FTC se obvezuje na odlučnu provedbu novog Okvira. Ovim dopisom obilježava se ta obveza.

Posebno potvrđujemo svoju opredijeljenost u četiri ključna područja: 1. određivanje prioriteta za upućivanje i istrage; 2. suzbijanje lažnih ili prijevarnih tvrdnji o sudjelovanju u sustavu zaštite privatnosti 3. trajno praćene reda i i 4. pojačano sudjelovanje i suradnja u provedbi s nadležnim tijelima za zaštitu podataka u EU-u. U nastavku detaljno opisujemo svaku od tih obveza i podatke o ulozi FTC-a u zaštiti privatnosti potrošača i provođenju programa „sigurne luke" te u širem okviru zaštite privatnosti u Sjedinjenim Američkim Državama. ([1])

I. KONTEKST

A. **Rad FTC-a u području provedbe zaštite privatnosti i u području politike**

FTC ima široke građanske ovlasti promicati zaštitu potrošača i tržišno natjecanje u području trgovine. U okviru svog mandata zaštite potrošača, FTC provodi širok raspon zakona za zaštitu privatnosti i sigurnosti podataka o potrošačima.

([1]) Dodatne informacije o saveznim i državnim zakonima SAD-a o privatnosti navodimo u Prilogu A i sažetak nedavnih mjera za osiguranje privatnosti i sigurnosti na stranici: https://www.ftc.gov/reports/privacy-data-security-update-2015.

Glavnim zakonom koji provodi FTC, Zakonom o FTC-u, zabranjuju se „nepoštene" ili „prijevarne" radnje ili prakse u trgovini ili koje utječu na trgovinu ([1]). Pisana izjava, propust ili praksa prijevarni su ako su materijalni i mogli bi zavarati potrošače koji postupaju razumno s obzirom na okolnosti ([2]). Radnja ili praksa smatraju ne nepoštenima ako uzrokuju, ili bi mogle uzrokovati, znatnu štetu koju potrošači ne mogu razumno izbjeći ili prevladati kompenzacijskim koristima za potrošače ili tržišno natjecanje ([3]). FTC također provodi ciljane zakone kojima se štite podaci o zdravlju, kreditnim i ostalim pitanjima te podaci o djeci na internetu te je donio provedbene propise za svaki od tih zakona.

Nadležnost FTC-a u skladu sa Zakonom o FTC-u primjenjuje se na pitanja „u trgovini ili koja utječu na trgovinu". FTC nije nadležan za provedbu kaznenog prava ili za pitanja nacionalne sigurnosti. FTC ne može utjecati ni na većinu državnih mjera. Nadalje, postoje iznimke od nadležnosti FTC-a nad tržišnim aktivnostima, među ostalim u odnosu na banke, zrakoplovne tvrtke, osiguravateljske tvrtke i zajedničke operaterske aktivnosti pružatelja telekomunikacijskih usluga. FTC nije nadležan za većinu neprofitnih organizacija, ali nadležan je za lažne dobrotvorne tvrtke ili druge neprofitne organizacije koje zapravo zarađuju dobit. FTC ima nadležnost nad neprofitnim organizacijama koje posluju kako bi njihovi neprofitni članovi ostvarivali dobit, među ostalim osiguravanjem znatnih gospodarskih koristi tim članovima ([4]). U nekim slučajevima FTC je nadležan zajedno s drugim agencijama za provedbu zakona.

Razvili smo dobar radni odnos sa saveznim i državnim tijelima i blisko s njima surađujemo na koordinaciji istraga ili na upućivanju predmeta prema potrebi.

Provedba je od ključne važnosti za pristup FTC-a zaštiti privatnosti. FTC je do danas pokrenuo više od 500 predmeta zaštite privatnosti i sigurnosti podataka o potrošačima. Zbirkom predmeta obuhvaćeni su podaci na internetu i izvan njega i ona uključuje mjere izvršenja protiv velikih i malih poduzeća za koja se tvrdi da nisu pravilno obrisala osjetljive podatke o potrošačima, da nisu osigurala osobne podatke potrošača, da su na prijevaru pratila potrošače na internetu, da su im slala neželjenu poštu, da su postavila softver za prisluškivanje ili drugi zloćudni softver na računala potrošača, da su prekršila pravila o ne zvanju ili druga pravila telemarketinga i da su na neprimjereni način prikupljanja i dijelila podatke o potrošačima na mobilnim uređajima. Provedbenim mjerama FTC-a – u fizičkom i digitalnom svijetu – šalje se važna poruka poduzećima o potrebi za zaštitom privatnosti potrošača.

FTC je također provodio brojne inicijative politike s ciljem zaštite privatnosti potrošača na kojima se temelje njegove aktivnosti izvršenja. FTC je organizirao radionice i objavljivao izvješća s preporukama o najboljoj praksi usmjerenima na poboljšanje privatnosti u mobilnom ekosustavu; povećanje transparentnosti u industriji posrednika podataka; ostvarivanje najvećih mogućih koristi velikih podatka uz ublažavanje rizika, posebno za potrošače s niskim prihodima i potrošače koji to nisu zaslužili; i isticanje utjecaja prepoznavanja lica i Interneta stvari na pitana sigurnosti i privatnosti, među ostalim.

FTC također organizira obrazovanje potrošača i poduzeća u cilju jačanja svojih inicijativa izvršenja i razvoja politika. FTC je upotrijebio različite alate – publikacije, resurse na internetu, radionice i društvene medije – za pružanje obrazovnih materijala na različite teme, uključujući mobilne aplikacije, privatnost djece i sigurnost podataka. Komisija je nedavno pokrenula svoju inicijativu „Početak sa sigurnošću" koja uključuje nove smjernice za poduzeća utemeljene na poukama naučenima iz slučajeva agencije povezanih sa sigurnošću podatka te brojne radionice diljem zemlje. Nadalje, FTC je dugo imao vodeće mjesto u obrazovanju potrošača o osnovama računalne sigurnosti. Prošle je godine *web*-mjesto OnGuard online i njego pandan na španjolskom jeziku, Alerta en Línea, posjetilo više od 5 milijuna posjetitelja.

B. **Pravne zaštite SAD-a koje koriste potrošačima iz EU-a**

Okvir će se provoditi u kontekstu opsežnijeg okoliša privatnosti SAD-a kojim se potrošači EU-a štite na brojne načine.

([1]) 15 U.S.C. članak 45. točka (a)
([2]) Vidjeti Izjava politike FTC-a o prijevari, priložena Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
([3]) Vidjeti 15 U.S.C. članak 45. točka (n); Izjava politike FTC-a o nepoštenju, priložena Int'l Harvester Co., 104. F.T.C. 949, 1070 (1984), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
([4]) Vidjeti *California Dental Ass'n* protiv FTC-a, 526 U.S. 756 (1999).

Zabrana nepoštenih ili prijevarnih radnih ili praksi iz Zakona o FTC-u nije ograničena na zaštitu potrošača SAD-a od američkih poduzeća jer uključuje one prakse kojima 1. se uzrokuje ili bi se mogla uzrokovati razumno predvidljiva šteta Sjedinjenim Američkim Državama ili 2. koje uključuju materijalno postupanje u Sjedinjenim Američkim Državama. Nadalje, FTC može upotrijebiti sve pravne lijekove, uključujući nadoknadu štete, koji su dostupni za zaštitu domaćih potrošača kada se štite strani potrošači.

Rad FTC-a na izvršenju znatno koristi potrošačima iz SAD-a i stranim potrošačima. Na primjer, u našim predmetima u kojima se provodio odjeljak 5. Zakona o FTC-u zaštitila se privatnost američkih i stranih potrošača. U predmetu protiv posrednika informacijama, Accusearch, FTC je tvrdio da je prodaja povjerljivih podataka iz telefonskih imenika trećim stranama bez znanja ili suglasnosti potrošača nepoštena praksa kojom se krši odjeljak 5. Zakona o FTC-u. Accusearch je prodao podatke o američkim i stranim potrošačima ([1]). Sud je odobrio privremenu mjeru protiv poduzeća Accusesearch kojim mu je zabranjen, među ostalim, marketing ili prodaja osobnih podataka potrošača bez pisane suglasnosti, osim ako su ti podaci zakonito pribavljeni iz javno dostupnih informacija i naredio je odštetu od gotovo 200 000 USD ([2]).

Drugi je primjer nagodba FTC-a s poduzećem TRUSTe. Time se osigurava da se potrošači, među ostalim i oni u Europskoj uniji, mogu osloniti na izjave globalne samoregulatorne organizacije o svom preispitivanju i certifikaciji domaćih i stranih internetskih službi ([3]). Što je još važnije, našim djelovanjem protiv TRUSTe jača se samoregulacijski sustav privatnosti osiguravanjem odgovornosti subjekata koji imaju važnu ulogu u programima samoregulacije, među ostalim u prekograničnim okvirima zaštite privatnosti.

FTC provodi i druge ciljane zakone kojima se štite i potrošači izvan EU-a, poput Zakona o zaštiti privatnosti djece na internetu (dalje u tekstu „COPPA"). Zakonom o zaštiti privatnosti djece na internetu propisano je, među ostalim, da operateri *web*-mjesta ili internetskih usluga usmjerenih na djecu ili mjesta za opću publiku koji svjesno prikupljaju osobne podatke od djece mlađe od 13 godine, moraju obavijestiti roditelje i zatražiti provjerljivu suglasnost roditelja. Američka *web*-mjesta i usluge na koje se primjenjuje CPPA i koja prikupljaju osobne podatke od strane djece moraju se uskladiti s COPPA-om. Strana *web*-mjesta i internetske usluge također moraju postupati u skladu s COPPA-om ako su usmjereni na djecu u Sjedinjenim Američkim Državama ili ako svjesno prikupljaju osobne podatke od djece u Sjedinjenim Američkim Državama. Osim američkih saveznih zakona koje FTC provodi, dodatne pogodnosti potrošačima iz EU-a mogu se osigurati i određenim drugim saveznim i državnim zakonima o zaštiti potrošača i privatnosti.

C. **Provedba „sigurne luke"**

U okviru svog programa osiguranja zaštite privatnosti i sigurnosti, FTC je također nastojao zaštititi potrošače EU-a pokretanjem izvršnih mjera u slučaju povreda načela „sigurne luke". FTC je pokrenuo 39 provedbenih mjera u okviru „sigurne luke": njih 36 pokrenuto je zbog navoda o lažnoj certifikaciji, a tri predmeta —protiv Googlea, Facebooka i Myspacea— zbog navodnih povreda načela zaštite privatnosti iz programa „sigurne luke" ([4]). Ti predmeti primjer su izvršnosti certifikacija i posljedica neusklađenosti. Dvadesetogodišnjim nalozima za suglasnost zahtijeva se od Googlea, Facebooka i MySpacea da provode sveobuhvatne programe zaštite privatnosti koji moraju biti prikladno osmišljeni da bi se njima mogli ukloniti rizici za privatnost povezani s razvojem novih programa i upravljanjem novim i postojećim proizvodima i uslugama te da bi se zaštitile privatnost i povjerljivost osobnih podataka. U sveobuhvatnim programima zaštite privatnosti koji su im određeni tim nalozima moraju se moći utvrditi predvidljivi materijalni rizici i moraju postojati kontrole za uklanjanje tih rizika. Poduzeća se moraju podvrgnuti trajnom, neovisnom ocjenjivanju njihovih programa zaštite privatnosti, koje se moraju dostaviti FTC-u. Nalozima se zabranjuje tim trgovačkim društvima da krivo prikazuju svoje prakse privatnosti i svoje sudjelovanje u bilo kojem programu privatnosti ili sigurnosti. Ta zabrana

([1]) Vidjeti Ured kanadskog Povjerenika za zaštitu privatnosti, Pritužba u skladu s PIPEDA-om protiv Accusearch, Inc., koji posluje kao Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp.Ured kanadskog povjerenika za zaštitu privatnosti podnio je sažetak *amicus curiae* u okviru žalbe protiv mjere FTC-a i proveo je vlastitu istragu u kojoj je utvrđeno da se praksama Accusearcha također povrijedilo pravo EU-a.

([2]) Vidjeti *FTC protiv Accusearcha, Inc.*, br. 06CV015D (D. Wyo. 20. prosinca 2007.), *aff'd* 570 F.3d 1187 (10. Cir. 2009.).

([3]) Vidjeti *In the Matter of True Ultimate Standards Everywhere, Inc.*, br. C-4512 (F.T.C. 12. ožujka 2015.) (odluka i nalog), *dostupno na* https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Vidjeti *U predmetu u vezi s Googleom, Inc.*, br. C-4336 (F.T.C. 13. listopada 2011.) (odluka i nalog), *dostupno na* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *U predmetu u vezi s Google, Inc.*, br. C-4365 (F.T.C. 27. srpnja 2012.) (odluka i nalog), *dostupno na* https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *U predmetu Myspace LLC*, br. C-4369 (F.T.C. 30. kolovoza 2012.) (odluka i nalog), *dostupno na* https://www.ftc.gov/news- events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

primjenjivala bi se i na postupke i praksu poduzeća u skladu s novim okvirom sustava za zaštitu privatnosti. FTC može izvršavati te naloge tražeći građanske kazne. Google je 2012 platio rekordnih 22,5 milijuna USD kazne zbog navoda da je prekršio svoj nalog. Navedenim nalozima FTC-a pridonosi se zaštiti više od milijardu potrošača u cijelom svijetu, od kojih stotine milijuna žive u Europi.

FTC se suočio i sa slučajevima lažnih, prijevarnih ili zavaravajućih tvrdnji o sudjelovanju u programu „sigurne luke". FTC te tvrdnje ozbiljno shvaća. Na primjer, u predmetu *FTC protiv Karnanija*, FTC je 2011. pokrenu postupak protiv poduzeća koje obavlja marketing na Internetu tvrdeći da su ono i njegov partner prevarili britanske potrošače da vjeruju da do poduzeće ima sjedište u Ujedinjenoj Kraljevini uporabom internetske domene.uk web i upućivanjem na britansku valutu i poštanski sustav UK-a. ([1]) Međutim, kada potrošači dobili proizvode otkrili su neočekivane carine, jamstva koja ne vrijede u Ujedinjenoj Kraljevini i naknade povezane s traženjem povrata novca. TC je također tvrdio da su tuženici prevarili potrošače u pogledu njihova sudjelovanja u programu„sigurne luke". Svi potrošači koji su bili žrtve nalazili su se u Ujedinjenoj Kraljevini.

Mnogi od naših drugih predmetna izvršenja u vezi s programom „sigurne luke" uključivali su organizacije koje su se pridružile programu „sigurne luke", ali nisu obnovili godišnji certifikat, a nastavili su se predstavljati kao aktualni članovi. Kako je dalje navedeno u nastavku, FTC također rješava lažne tvrdnje o sudjelovanju u okviru sustava zaštite privatnosti. Ovom strateškom aktivnošću izvršenja nadopunit će se pojačane mjere Ministarstva trgovine usmjerene na provjeru poštovanja zahtjeva iz programa za certifikaciju i ponovnu certifikaciju, praćenje učinkovitog poštovanja načela, uključujući uporabom upitnika za sudionike u Okviru i pojačane napore za utvrđivanje lažnih tvrdnji o članstvu u Okviru i zlouporabu oznake članstva u Okviru sustava zaštite privatnosti ([2]).

II. PREDNOST PRI UPUĆIVANJU I ISTRAGE

Kao što smo učinili u slučaju programa „sigurne luke", FTC se obvezuje dati prednost upućenim predmetima iz država članica EU-a u vezi sa sustavom zaštite privatnosti. On će također davati prednost predmetima povezanima s nepoštovanjem samoregulatornih smjernica povezanih s okvirom zaštite privatnosti koje su uputile samoregulatorne organizacije i ostala neovisna tijela za rješavanje sporova.

Kako bi olakšao upućivanja predmeta iz država članica EU-a unutar Okvira, FTC stvara standardizirani postupak upućivanja i davanja smjernica državama članicama EU-a o vrsti informacija kojima bi se na najbolji način pomoglo FTC-u s istragom upućenog predmeta. Kao dio tih napora, FTC će imenovati točku za kontakt za upućivanje predmeta iz država članica. Najkorisnije je kada tijelo koje upućuje predmet obavilo prethodnu istragu navodne povrede i može surađivati s FTC-om u istrazi.

Po primitku upućenog predmeta od države članice EU-a ili samoregulatorne organizacije, FTC može poduzeti niz mjera za rješavanje navedenih problema. Na primjer, možemo preispitati politike zaštite privatnosti poduzeća, pribaviti dodatne informacije izravno od poduzeća ili od trećih stranaka, tražiti informacije od tijela koje je uputilo predmet, ocijeniti postoji li uzorak povreda ili je pogođen velik broj potrošača, utvrdili odnose se upućeni predmeti na pitanja u nadležnosti Ministarstva trgovine, ocijeniti hoće li koristiti obrazovanje potrošača i poduzeća i, prema potrebi, pokrenuti ovršni postupak.

FTC se također obvezuje razmijeniti informacije o upućivanjima s provedbenim tijelima koja su uputila predmete, uključujući o stanju upućenih predmeta, u skladu sa zakonima o povjerljivosti i ograničenjima. U mjeri u kojoj je to izvedivo s obzirom na broj i vrstu upućenih predmeta, dostavljene informacije uključivat će ocjenu upućenih pitanja, među ostalim opis znatnih postavljenih pitana i mjere poduzete za rješavanje povreda zakona u nadležnosti FTC-a. FTC daje tijelu koje je uputilo predmet povratne informacije o vrstama zaprimljenih upućenih predmeta u cilju povećanja učinkovitosti napora za suzbijanje nezakonitog postupanja. Ako tijelo koje je uputilo predmet traži informacije o stanju

([1]) Vidjeti *FTC protiv Karnanija*, br. 2:09-cv-05276 (C.D. Cal. 20. svibnja 2011.) (propisani konačni nalog), *dostupno na* https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; *vidjeti isto* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9. lipnja 2011.).

([2]) Dopis Kena Hyatta, zamjenika Ministarstva trgovine za međunarodnu trgovinu Věri Jourovoj, povjerenici za pravosuđe, zaštitu potrošača i ravnopravnost spolova.

određenog upućenog predmeta za potrebe provođenja vlastitih ovršnih postupaka, FTC odgovara uzimajući u obzir broj upućenih predmeta koje razmatra i podložno povjerljivosti i ostalim pravnim zahtjevima.

FTC će također blisko surađivati s nadležnim tijelima za zaštitu podataka EU-a na pružanju pomoći s izvršenjem. To bi u odgovarajućim slučajevima moglo uključivati razmjenu informacija i pomoć s istragom u skladu s američkim Zakonom o sigurnom internetu kojim se FTC ovlašćuje za pružanje pomoći stranim agencijama za provedbu zakona kada strana agencija provodi zakone kojima se zabranjuju prakse koje su slične praksama zabranjenima zakonima koje provodi FTC ([1]). U okviru te pomoći FTC može razmjenjivati informacije prikupljene u vezi s istragom FTC-a, pokrenuti obvezni postupak u ime nadležnog tijela za zaštitu informacija iz EU-a koje provodi vlastitu istragu i tražiti usmeno svjedočenje svjedoka ili tuženika u vezi s postupkom izvršenja nadležnog tijela za zaštitu podataka, u skladu sa zahtjevima američkog Zakona o sigurnom internetu. FTC redovito upotrebljava svoje ovlasti za pomoć drugim nadležnim tijelima u svijetu u predmetima povezanima s privatnošću i zaštitom potrošača ([2]).

Osim davanja prednosti predmetima upućenima iz država članica EU-a i samoregulatornih organizacija za privatnost u okviru sustava za zaštitu privatnosti ([3]), FTC se obvezuje istražiti moguće povrede Okvira na vlastitu inicijativu, prema potrebi uporabom niza alata.

Tijekom posljednjeg desetljeća FTC je održavao pouzdan program istraga pitanja privatnosti i sigurnosti koja uključuju tržišne organizacije. U okviru tih istraga FTC je redovito ispitivao daje li predmetni subjekt izjave u pogledu članstva u „sigurnoj luci". Ako je subjekt davao takve izjave i tijekom istrage utvrđene su očite povrede načela privatnosti programa „sigurne luke", FTC je uključio navode o povredama „sigurne luke" u svoje mjere izvršenja. Takav proaktivni pristup nastavit ćemo primjenjivati i u novom Okviru. Što je još važnije FTC provodi mnogo više istraga nego što ih u konačnici završi javnim mjerama izvršenja. Mnoge istrage FTC-a zaključene su jer osoblje nije utvrdilo očitu povredu zakona. Budući da istrage FTC-a nisu javne i povjerljive su, zatvaranje istrage često se ne objavljuje.

Gotovo 40 mjera izvršenja koje je pokrenuo FTC u vezi s programom „sigurne luke" dokaz su opredijeljenosti agencije za proaktivnu provedbu prekograničnih programa privatnosti. FTC će tražiti moguće povrede okvira u okviru redovitih istraga privatnosti i sigurnosti.

III. SUZBIJANJE LAŽNIH ILI PRIJEVARNIH TVRDNJI O SUDJELOVANJU U SUSTAVU ZAŠTITE PRIVATNOSTI

Kako je prethodno navedeno, FTC će poduzeti mjere protiv tijela koja netočno predstavljaju svoje sudjelovanje u Okviru. FTC će dati prednost razmatranju predmeta koje je uputilo Ministarstvo trgovine u vezi s organizacijama za koje je utvrdilo da se neprimjereno predstavljaju kao aktualni članovi Okvira ili koje upotrebljavaju oznaku članstva u Okviru bez odobrenja.

Nadalje, napominjemo da ako organizacija svojom politikom zaštite privatnosti tvrdi da poštuje načela sustava zaštite privatnosti, ona time što se nije registrirala pri Ministarstvu trgovine vjerojatno neće biti oslobođena izvršenja tih obveza iz Okvira.

([1]) Kada utvrđuje treba li izvršavati svoje ovlasti u skladu s američkim Zakonom o sigurnom internetu, FTC razmatra, među ostalim, sljedeće: „(A) je li se agencija koja podnosi zahtjev složila pružati ili će pružati uzajamnu pomoć Komisiji; (B) hoće li se postupanjem u skladu sa zahtjevom dovesti u pitanje javni interes Sjedinjenih Američkih država; i (C) odnosi li se istraga agencije koja podnosi zahtjev ili provodi ovršni postupak na postupke ili praksu kojima se uzrokuje, ili bi se mogla uzrokovati šteta velikom broju osoba." 15 U.S.C. članak 46. točka (j) podtočka 3. Ta se ovlast ne primjenjuje na izvršenje zakona u području tržišnog natjecanja.

([2]) Tijekom fiskalnih godina 2012. – 2015., na primjer, FTC je upotrijebio svoje ovlasti u skladu sa Zakonom o sigurnom internetu za razmjenu informacija kao odgovor na gotovo 60 zahtjeva stranih agencija i izdao je gotovo 60 građanskih istražnih zahtjeva (koji su jednakovrijedni administrativnim pozivima) kako bi pomogao u 25 stranih istraga.

([3]) Iako FTC ne rješava pojedinačne pritužbe potrošača niti u njima posreduje, on potvrđuje da će davati prednost predmetima upućenima od nadležnih tijela za zaštitu podataka iz EU-a u vezi sa sustavom zaštite privatnosti. Nadalje, FTC upotrebljava pritužbe u svojoj bazi potrošača Sentinel, kojoj mogu pristupiti mnoge druge agencije za provedbu zakona, za utvrđivanje trendova, prioriteta za izvršenje i za utvrđivanje mogućih predmeta istrage. Građani EU-a mogu upotrijebiti isti sustav pritužbi koji je dostupan građanima SAD-a za podnošenje pritužbe FTC-u www ftc.gov/complaint. Međutim, za pojedinačne pritužbe u okviru sustava za zaštitu privatnosti, pojedinicima iz EU-a može biti najkorisnije podnijeti pritužbe nadležnom tijelu za zaštitu privatnosti njihove države članice ili alternativnom pružatelju usluge rješavanja sporova.

IV. PRAĆENJE NALOGA

FTC također potvrđuje svoju obvezu praćenja naloga za izvršenje kako bi osigurao poštovanje načela sustava za zaštitu privatnosti.

Zahtijevat ćemo poštovanje Okvira nizom odgovarajućih privremenih mjera u budućim nalozima FTC-a u vezi s okvirom. To uključuje zabranu lažnih izjava u pogledu Okvira i ostalih programa zaštite privatnosti kada su oni osnova za djelovanje FTC-a.

Predmeti FTC-a kojima se provodi izvorni program „sigurne luke" poučni su. U 36 slučajeva koji uključuju lažne ili prijevarne tvrdnje o certifikaciji „sigurne luke", svakim nalogom zabranjuje se tuženiku da krivo prikazuje svoje sudjelovanje u programu „sigurne luke" ili bilo kojem drugom programu zaštite privatnosti ili sigurnosti i traži se od poduzeća da FTC-u stavi na raspolaganje izvješća o postupanju u skladu s tim nalogom. U predmetima koji su se odnosili na povrede načela sustava za zaštitu privatnosti poduzeća su morala provoditi sveobuhvatne programe zaštite privatnosti i svake druge godine tijekom dvadeset godina pribavljati neovisne ocjene tih programa koje daju treće stranke, a koje moraju dostaviti FTC-u.

Za povrede administrativnih rješenja FTC-a mogu se naplatiti kazne do 16 000 USD po povredi ili 16 000 USD po danu za trajne povrede ([1]), što, u slučaju praksa koje utječu na mnoge potrošače, može iznositi milijune dolara. Svaki nalog za usklađivanje sadržava i odredbe o izvješćivanju i poštovanju načela. Subjekti na koje se odnosi nalog moraju nekoliko godina zadržati dokumente kojima se dokazuje da su postupili u skladu s nalogom. Nalozi se mogu dostavljati i zaposlenicima koji su odgovorni za osiguravanje postupanja u skladu s nalogom.

FTC sustavno prati postupanje u skladu s nalozima iz programa „sigurne luke", kao što čini i u slučaju svih ostalih svojih naloga. FTC ozbiljno shvaća izvršenje svojih naloga za osiguranje privatnosti i sigurnosti podataka i, ako je potrebno, poduzima mjere za njihovo izvršenje. Na primjer, kako je prethodno navedeno, Google je platio 22,5 milijuna USD kazne zbog navoda da je prekršio svoj nalog FTC-a. Što je još važnije, nalozima FTC-a i dalje će se štititi potrošači u cijelom svijetu koji posluju s poduzećem, a ne samo oni potrošači koji su podnijeli pritužbu.

Naposljetku, FTC će na internetu objaviti popis poduzeća na koje se odnose nalozi pribavljeni u vezi s izvršenjem programa „sigurne luke" i novog okvira sustava zaštite privatnosti ([2]). Nadalje, u skladu s načelima sustava zaštite privatnosti sada se zahtijeva od poduzeća kojima je izdan nalog FTC-a ili sudski nalog zbog nepoštovanja načela da objave sve relevantne odjeljke izvješća o usklađenosti ili ocjenjivanju koji su relevantni za Okvir, a kojeg su podnijeli FTC-u u mjeri u kojoj je to u skladu sa zakonima i pravilima o povjerljivosti.

V. ODNOS S TIJELIMA ZA ZAŠTITU PODATKA IZ EU-A I SURADNJA NA IZVRŠENJU

FTC prepoznaje važnu ulogu nadležnih tijela za zaštitu podataka u EU-u u pogledu poštovanja Okvira i potiče ih na pojačano savjetovanje i suradnju na provedbi. Osim savjetovanja o određenim pitanjima s nadležnim tijelima za zaštitu podataka koja su uputila predmet, FTC se obvezuje sudjelovati na povremenim sastancima s imenovanim predstavnicima Radne skupine iz članka 29. radi razgovora o općim uvjetima za poboljšanje suradnje na izvršenju u odnosu na Okvir FTC će surađivati, zajedno s Ministarstvom trgovine, Europskom komisijom i predstavnicima Radne skupine iz članka 29. u godišnjem preispitivanju Okvira radi razgovora o njegovoj provedbi.

FTC potiče i na razvoj alata kojima će se pojačati suradnja izvršenju s nadležnim tijelima EU-a za zaštitu podatka te s drugim tijelima za izvršenje zaštite privatnosti u cijelom svijetu. FTC je posebno, zajedno s partnerima u izvršenju u Europskoj uniji i cijelom svijetu, prošle godine pokrenuo sustav upozoravanja u okviru Globalne mreže za zaštitu privatnosti (dalje u tekstu „GPEN") radi razmjene informacija o istragama i promicanja koordinacije izvršenja. Taj alat za upozoravanje GPEN-a posebno bi mogao biti koristan u kontekstu okvira sustava za zaštitu privatnosti. FTC i nadležna tijela EU-a za zaštitu privatnosti mogla bi ga upotrebljavati za koordinaciju u pogledu Okvira i drugih istraga privatnosti, među ostalim kao početnu točku za razmjenu informacija u cilju pružanja koordinirane i učinkovitije zaštite privatnosti

([1]) 15 U.S.C. članak 45. (m); 16 C.F.R. članak 1.98.
([2]) Vidjeti FTC, Poslovni centar, Pravni resursi, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

potrošača. Veselimo se daljnjoj suradnji s uključenim nadležnim tijelima EU-a u široj primjeni sustava upozoravanja GPEN-a i razvoju drugih alata za poboljšanje suradnje u izvršenju u predmetima povezanima s privatnošću, među ostalima onima koji se odnose na Okvir.

FTC sa zadovoljstvom potvrđuje svoju opredijeljenost za provedbu novog Okvira sustava za zaštitu privatnosti. Veselimo se i daljnjoj suradnji sa svojim kolegama iz EU-a na zaštiti privatnosti potrošača s obje strane Atlantika.

S poštovanjem,

Edith Ramirez

Predsjednica

Dodatak A

Okvir europsko-američkog sustava zaštite privatnosti u kontekstu: pregled sigurnosnih mjera i mjera za zaštitu privatnosti u SAD-u

Zaštita koju pruža okvir europsko-američkog sustava zaštite privatnosti („okvir") postoji u širem kontekstu mjera za zaštitu privatnosti koje je uspostavio cijeli američki pravni sustav. Prvo, Savezna trgovinska komisija („FTC") ima čvrst sigurnosni sustav za zaštitu privatnosti i podataka za trgovinske prakse SAD-a kojim se štite potrošači diljem svijeta. Drugo, mjere za privatnost i sigurnost potrošača stalno se razvijaju u SAD-u od 2000. kad je donesen prvi program „sigurne luke" između EU-a i SAD-a. U međuvremenu su doneseni brojni zakoni o privatnosti i sigurnosti na državnoj i federalnoj razini, a brojn privatnih i javnih sudskih postupaka o izvršenju prava privatnosti znatno se povećao. Široki raspon pravnih zaštita SAD-a za privatnost i sigurnost potrošača koje se primjenjuju na tržišne podatke nadopunjuje zaštite koje pojedincima iz EU-a omogućuje novi Okvir.

I. PROGRAM PROVEDBE OPĆEG PROGRAMA FTC-A ZA SIGURNOST I PRIVATNOST

FTC je vodeća agencija za zaštitu potrošača u SAD-u s naglaskom na privatnost u trgovinskom sektoru. FTC ima ovlasti za sudski progon nepoštenih i prijevarnih radnji ili praksi kojima se krši privatnost potrošača te za provedbu ciljanih zakona o privatnosti kojima su zaštićeni određeni financijski ili zdravstveni podaci, podaci o djeci te podaci na temelju kojih se donose određene odluke o prihvatljivosti o potrošačima.

FTC ima bogato iskustvo u provođenju zakona o zaštiti potrošača. U provedbi FTC je rješavao pitanja nezakonitih praksi na internetu i izvan njega. Naprimjer, FTC je pokrenuo mjere protiv poznatih poduzeća, kao što su Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC i Snapchat, ali i protiv manje poznatih poduzeća. FTC je pokrenuo tužbe protiv poduzeća koja su navodno slala neželjenu poštu potrošačima, postavila softver za prisluškivanje na računala, nisu osigurala osobne podatke potrošača, na prijevaru pratila potrošače na internetu, prekršila pravo djece na privatnost, nezakonito prikupljala podatke o potrošačima na njihovim mobilnim uređajima te koja nisu osigurala uređaje koji se mogu spojiti na internet na kojima se nalaze osobni podaci. Nalozi nakon tih istraga uglavnom su za rezultat imali trajni nadzor FTC-a za razdoblje od dvadeset godina, zabranu daljnjeg kršenja zakona i izdavanje financijskih sankcija za poduzeća zbog kršenja naloga ([1]). Što je još važnije, nalozima FTC-a ne štite se samo pojedinci koji su uložili pritužbu na određeni problem, već se njima štite svi potrošači koji posluju s poduzećima koja su predmet istrage. U prekograničnom kontekstu FTC ima nadležnost za zaštitu potrošača diljem svijeta od praksi koje se odvijaju u SAD-u ([2]).

FTC je dosad prijavio više od 130 predmeta zbog slanja neželjene pošte ili softvera za prisluškivanje, više od 120 slučajeva „Do Not Call" (ne nazivati) u području telemarketinga, više od 100 mjera u okviru Zakona o poštenom izvješćivanju, gotovo 60 predmeta u području sigurnosti podataka, više od 50 općih mjera u području privatnosti te gotovo 30 predmeta kršenja zakona Gramm-Leach-Bliley i više od 20 mjera kojima se provodi Zakon o zaštiti privatnosti djece na internetu (dalje u tekstu „COPPA") ([3]). Uz te slučajeve, FTC je izdao javna pisma upozorenja ([4]).

([1]) Svaki subjekt koji ne poštuje nalog FTC-a može platiti kaznu do 16 000 USD zbog povrede ili 16 000 USD po danu za trajne povrede. Vidjeti 15 U.S.C. članak 45. stavak l.; 16 C.F.R. članak 1.98 točka (c).

([2]) Kongres je izričito potvrdio nadležnost FTC-a da može upotrijebiti sve pravne lijekove, uključujući naknadu štete, za sva djela ili prakse u području inozemne trgovine koja (1) uzrokuju ili mogu uzrokovati razumno predvidljivu štetu Sjedinjenim Američkim Državama ili (2) koja uključuju materijalno postupanje u Sjedinjenim Američkim Državama. Vidjeti 15 U.S.C. članak 45. točka (a) podtočka (4).

([3]) U nekim slučajevima o privatnosti i zaštiti podataka Komisija navodi da je poduzeće poduzimalo nepoštene i prijevarne postupke; u tim slučajevima riječ je ponekad o navodnom kršenju niza zakona, kao što je *Fair Credit Reporting Act*, zakon Gramm-Leach-Bliley Act i COPPA.

([4]) Vidjeti, *npr.*, Priopćenje za medije federalnog odbora za trgovinu, *FTC Warns Children's App Maker BabyBus About Potential COPPA Violations* (22. prosinca 2014.), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Priopćenje za medije federalnog odbora za trgovinu, *FTC Warns Data Broker Operations of Possible Privacy Violations* (7. svibnja 2013.), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Priopćenje za medije federalnog odbora za trgovinu, *FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act* (3. travnja 2013.), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

U okviru svojeg nastojanja da osigura zaštitu privatnosti FTC je istraživao i eventualna kršenja programa „sigurne luke". Od donošenja programa „sigurne luke" FTC je na vlastitu inicijativu pokrenuo brojne istrage o usklađenosti programa i pokrenuo 39 postupaka protiv američkih poduzeća zbog kršenja pravila programa „sigurne luke". FTC će nastaviti s tim proaktivnim pristupom u kojem je provedba novog okvira prioritet.

II. MJERE ZA ZAŠTITU PRIVATNOSTI POTROŠAČA NA DRŽAVNOJ I FEDERALNOJ RAZINI

Pregled provedbe „sigurne luke", prilog odluci Europske komisije o odgovarajućoj razini zaštite „sigurne luke", daje sažetak niza zakona o privatnosti na federalnoj i državnoj razini koji su bili na snazi kad je program „sigurne luke" donesen 2000. ([1]). U tom su razdoblju propisi na saveznoj razini regulirali komercijalno prikupljanje i korištenje osobnih podataka, osim odjeljka 5. Zakona o FTC-u, uključujući: *Cable Communications Policy Act, Driver's Privacy Protection Act, Electronic Communications Privacy Act, Electronic Funds Transfer Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Right to Financial Privacy Act, Telephone Consumer Protection Act* i *Video Privacy Protection Act*. Mnoge države imale su analogne zakone u tim područjima.

Od 2000. poduzeti su brojni koraci na federalnoj i državnoj razini za pružanje dodadtne zaštite privatnosti potrošača ([2]). Naprimjer, FTC je na federalnoj razini izmijenio pravilo COPPA-e kako bi se dodatno zaštitili osobni podaci djece. FTC je izdao i dva propisa o privatnosti i mjerama zaštite kojima se provodi Zakon Gramm- Leach-Bliley kojima se od financijskih institucija ([3]) zahtijeva da otkriju svoje prakse dijeljenja podataka te da u praksi provedu sveukupni program sigurnosti podataka u cilju zaštite podataka o potrošačima ([4]). Slično tome, Zakon o poštenim i pouzdanima kreditnim transakcijama (FACTA), donesen 2003., dopunjuje starije zakone SAD-a u cilju uspostave zahtjeva za prikrivanje, dijeljenje i uporabu određenih financijskih podataka osjetljive prirode. FTC je donio niz propisa u okviru FACTA-e o, među ostalim, pravu potrošača na besplatno godišnje financijsko izvješće, zahtjevima za sigurno brisanje podataka o potrošaču u izvješću, pravu potrošača da traži izuzeće od primanja ponuda o financijskim uslugama i osiguranju, pravu potrošača da traži izuzeće od primanja ponuda pridruženih poduzeća u kojima oglašavaju svoje proizvode i usluge i zahtjeva za financijske institucije i vjerovnike da provedu programe za utvrđivanje krađe identiteta i zaštite ([5]). Osim toga, propisi doneseni u okviru Zakona o zdravstvenom osiguranju (Health Insurance Portability and Accountability Act) revidirani su 2013. i uvele su se dodatne zaštitne mjere za zaštitu i sigurnost podataka osobnih podataka u području zdravstva ([6]). Na snagu su stupili i propisi kojima se potrošači štite od neželjenih poziva telemarketinga, automatskih poziva i neželjene pošte. Kongres je donio i zakone kojima se od određenih poduzeća koja prikupljaju zdravstvene podatke zahtijeva da potrošače obavijeste ako se krše njihova prava ([7]).

Države su također donijele niz zakona o privatnosti i sigurnosti. Od 2000. 47 država, Okrug Columbia, Guam, Puerto Rico i Djevičanski otoci donijeli su zakone kojima se od poduzeća zahtijeva da obavijeste potrošače o sigurnosnim

([1]) *Vidjeti* Ministarstvo trgovine SAD-a, Pregled provedbe „sigurne luke", https://build.export.gov/main/safeharbor/eu/eg_main_018476.
([2]) Za potpuniji pregled sažetka pravnih zaštita u SAD-u vidjeti: Daniel J. Solove i Paul Schwartz, *Information Privacy Law* (5. izdanje 2015).
([3]) Definicija financijskih institucija u okviru Zakona Gramm-Leach-Bliley jako je široka kako bi se uključila sva poduzeća koja su „znatno angažirana" u pružanju financijskih usluga ili nuđenju financijskih proizvoda. To naprimjer uključuje poduzeća za unovčenje čekova, poduzeća za kratkoročne zajmove, hipotekarne posrednike, vjerovnike izvan bankovnog sustava, procjenitelje privatnog vlasništva ili nekretnina te osoba koje pripremaju izradu prijave poreza.
([4]) U okviru Zakona o financijskoj zaštiti potrošača iz 2010. (*Consumer Financial Protection Act* – CFPA), Naslov X Pub. L. 111–203, 124 Stat. 1955 (21. srpnja 2010.) (poznat i pod nazivom *Dodd-Frank Wall Street Reform and Consumer Protection Act*), većina nadležnosti donošenja propisa iz Zakona Gramm-Leach-Bliley FTC-a prebačena je na Ured za financijsku zaštitu potrošača (*Consumer Financial Protection Bureau* – CFPB). FTC je i dalje provedbeno tijelo u okviru Zakona Gramm-Leach- Bliley te i dalje ima nadležnost za donošenja propisa za mjere zaštite i ograničenu nadležnost u okviru propisa o privatnosti u odnosu na trgovce automobilima.
([5]) U okviru CFPA-e Komisija dijeli svoju provedbenu ulogu FCRA-e s CFPB-om, ali se nadležnost u većem dijelu prebacuje na CFPB (uz iznimku propisa *Red Flags* i *Disposal Rules*).
([6]) *Vidjeti* 45 C.F.R. točke 160., 162., 164.
([7]) *Vidjeti, npr., American Recovery & Reinvestment Act* iz 2009, Pub. L. br. 111-5, 123 Stat. 115 (2009) i važne uredbe, 45 C.F.R. članci 164.404 – 164.414; 16 C.F.R. točka 318.

povredama osobnih podataka ([1]). Barem 32 države i Puerto Rico imaju zakone o brisanju podataka kojima se uvode zahtjevi za uništenje ili brisanje privatnih podataka ([2]). Niz je država donio zakone o općoj sigurnosti podataka. Osim toga, Kalifornija je donijela niz zakona o zaštiti privatnosti, uključujući zakon kojim se od poduzeća zahtijeva da provode vlastite pravila o zaštiti privatnosti te otkriju svoje prakse nepraćenja (*Do Not Track*) ([3]), Zakon „Shine the Light" za povećanje transparentnosti za posrednike podataka ([4]) i zakon kojim se uvodi opcija „eraser button" kojim se omogućuje maloljetnicima da zatraže brisanje podataka na društvenim medijima ([5]). Na temelju tih zakona i drugih nadležnosti tijela na federalnoj i državnoj razini izdali su znatan broj kazni poduzećima koja nisu zaštitila privatnost osobnih podataka potrošača ([6]).

Privatne tužbe imale su za rezultat uspješne presude i nagodbe kojima je omogućena dodatna sigurnost i zaštita osobnih podataka potrošača. Naprimjer, poduzeće Target pristalo je isplatiti 2015. 10 milijuna USD u okviru nagodbe s potrošačima koji su tvrdili da je narušena sigurnost njihovih osobnih financijskih podataka zbog veće povrede podataka. Poduzeće AOL pristalo je 2013. isplatiti 5 milijuna USD u okviru nagodbe nakon zajedničke tužbe koja se odnosila na navodno nedostatni postupak anonimizacije nakon što su objavljene pretrage stotine tisuća korisnika AOL-a. Osim toga, federalni sud izdao je Netflixu obvezu isplate odštete u iznosu od 9 milijuna USD jer je sačuvao prijašnju evidenciju posudbe čime se prekršio Zakon o pravu na video privatnost iz 1988. (*Video Privacy Protection Act*). Federalni sudovi u Kaliforniji odobrili dvije zasebne nagodbe s Facebookom, jednu u iznosu od 20 milijuna USD, a drugu u iznosu od 9,5 milijuna USD zbog načina na koji je poduzeće prikupljalo, dijelilo i koristile osobne podatke korisnika. Sud u Kaliforniji odobrio je 2008. nagodbu u visinu od 20 milijuna USD jer je poduzeće LensCrafters nezakonito otkrivalo zdravstvene podatke potrošača.

Ukratko, kako se vidjeti iz navedenog sažetka, Sjedinjene Američke Države omogućuju visoku razinu pravne zaštite za privatnost potrošača i sigurnost. Novi okvir sustava zaštite privatnosti, kojim se osiguravaju zaštitne mjere za pojedince iz EU-a, djelovat će u širem kontekstu u kojem su zaštita potrošača i sigurnost prioritet.

([1]) *Vidjeti, npr.*, dokument s Nacionalne konferencije državnih zakonodavstava (*National Conference of State Legislatures* –NCSL), *State Security Breach Notification Laws* (4. siječnja 2016.), *dostupan na adresi*: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (12. siječnja 2016.), *na adresi:* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) *Cal. Bus. & Professional Code* članci 22575-22579.

([4]) *Cal. Civ. Code* članci 1798.80-1798.84.

([5]) *Cal. Bus. & Professional Code* članci 22580-22582.

([6]) *Vidjeti* Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (17. veljače 2014.), *dostupno na adresi:* http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

PRILOG V.

Dopis Ministra prometa SAD-a Anthonyja Foxxa

19. veljače 2016.

Povjerenica Vera Jourová
Europska komisija
Rue de la Loi/Wetstraat 200
1 049 l 049 Bruxelles
Belgija

Predmet: Okvir europsko-američkog sustava zaštite privatnosti

Poštovana povjerenice Jourová,

Ministarstvo prometa Sjedinjenih Američkih Država (dalje u tekstu „Ministarstvo" ili „DOT") zahvaljuje na prilici da opiše svoju ulogu u provedbi Okvira europsko-američkog sustava zaštite privatnosti. Ovaj Okvir ima ključnu ulogu u zaštiti osobnih podataka koji se dostavljaju u okviru poslovnih transakcija u svijetu koji je sve više međusobno povezan. Time će se omogućiti poduzećima da obavljaju važne operacije u globalnom gospodarstvu i istodobno osiguraju važnu zaštitu privatnosti potrošača iz EU-a.

DOT je prvo javno izjavio svoju predanost izvršenju okvira „sigurne luke" u dopisu koji je posanl Europskoj komisiji prije više od 15 godina. DOT se u tom dopisu obvezao odlučno provoditi načela privatnosti iz programa „sigurne luke". DOT potvrđuje tu obvezu i ona se ovim dopisom ovjekovječuje.

DOT potvrđuje svoju obvezu posebno u sljedećim ključnim područjima: 1. davanje prednosti istrazi navodnih povreda sustava zaštite privatnosti; 2. primjerene mjere izvršenja protiv subjekata koji daju lažne ili prijevarne tvrdnje u vezi sa sustavom zaštite privatnosti; i 3. praćenje i objavljivanje naloga za izvršenje koji se odnose na povrede sustava zaštite privatnosti. U nastavku opisujemo svaku od tih obveza i, radi nužnog konteksta, osnovne informacije o ulozi DOT-a u zaštiti privatnosti potrošača i izvršenju Okvira sustava za zaštitu privatnosti.

I. KONTEKST

A. **Ovlasti Ministarstva prometa za zaštitu privatnosti**

Ministarstvo je odlučno osigurati zaštitu privatnosti informacija koje potrošači daju zračnim prijevoznicima i agentima koji prodaju karte. Ovlasti DOT-a za djelovanje u tom području propisane su u 49. U.S.C. 41712 kojim se zabranjuje prijevozniku „nepoštene ili prijevarne postupke, ili nelojalan način konkurencije" u prodaji zračnoga prijevoza, koji uzrokuju ili mogu izazvati štetu potrošaču. Odjeljak 712 je sastavljen po uzoru na odjeljak 5 Zakona o saveznoj trgovinskoj komisiji (15 U.S.C. 45). Svoj zakon o nepoštenim ili prijevarnim postupcima tumačimo kao da se njime zabranjuje zračnom prijevozniku ili agentu koji prodaje karte da čini sljedeće: (1) povrijedi uvjete svoje politike zaštite privatnosti ili (2) da prikuplja ili otkriva osobne podatke na način kojim se krši javna politike, koji je nemoralan, ili kojim se uzrokuje znatna šteta za potrošače koja se ne nadoknađuje kompenzacijskim koristima. Odjeljak 41712 tumačimo i kao da se njime zabranjuje putničkim agencijama i agentima koji prodaju karte da učine sljedeće: 1. povrijede bilo koje pravilo koje je izdalo Ministarstvo za utvrđivanje da je određena praksa privatnosti nepoštena ili prijevarna; ili 2. prekrše Zakon o zaštiti privatnosti djece na internetu (COPPA) ili pravila FTC-a o provedbi COPPA. U skladu sa saveznim zakonom, DOT ima isključive ovlasti regulirati prakse privatnosti zračnih prijevoznika i s FTC-om dijeli nadležnost u pogledu praksi privatnosti agenata koji prodaju karte u prodaji zračnog prijevoza.

Kada se prijevoznik ili prodavač usluga zračnog prijevoza javno obveze poštovati načela privatnosti okvira sustava za zaštitu privatnosti, Ministarstvo može upotrijebiti svoje zakonske ovlasti iz odjeljka 41712 da osigura poštovanje tih načela. Stoga, jednom kada putnik da podatke prijevozniku ili agentu koji prodaje karte koji se obvezao poštovati načela sustava zaštite privatnosti, svako nepridržavanje istih predstavljalo bi kršenje odjeljka 41712.

B. **Prakse provedbe**

Ured Ministarstva za izvršenje i postupke (Ured za izvršenje u zrakoplovstvu) istražuje i kazneno progoni predmete u skladu s 49 U.S.C. 4171 2. On izvršava zakonske zabrane iz odjeljka 41712 protiv nepoštenog i prijevarnog postupanja uglavnom pregovorima, pripremom naloga za obustavu takve prakse i izradom naloga s ocjenom građanskih kazni. Ured saznaje za moguće povrede većinom iz pritužbi koje zaprima od pojedinaca, putnih agenata, zračnih prijevoznika i agencija SAD-a i stranih državnih agencija. Potrošači mogu na *web*-mjestu DOT-a podnositi pritužbe za povrede privatnosti protiv zračnih prijevoznika i agenata koji prodaju karte- ([1]).

Ako se u određenom predmetu ne postigne razumna i odgovarajuća nagodba, Ured za izvršenje u zrakoplovstvu ovlašten je pokretati postupak izvršenja koji uključuje izvođenje dokaza pred upravnim sucem DOT-a. Upravni sudac ima ovlasti izdati nalog za obustavu i građanske kazne. Povredama odjeljka 41712 može se uzrokovati izdavanja sudskih naloga za obustavu i izricanja građanskopravnih kazni do 27 500 USD za svaku povredu djeljka 41 712.

Odjel nema ovlasti dodijeliti odštetu ili novčanu nadoknadu pojedinačnim podnositeljima pritužbi. Međutim, Ministarstvo ima ovlasti odobriti nagodbe sklopljene na temelju istraga Ureda za izvršene u zrakoplovstvu kojima se izravno koristi potrošačima (npr. gotovina, vaučeri) za prebijanje novčanih kazni koje bi inače bile plative američkoj vladi. To se dogodilo u prošlosti i moglo bi se dogoditi u kontekstu načela okvira za zaštitu privatnosti kada je opravdano zbog okolnosti. Ako neka zrakoplovna tvrtka iz SAD-a više puta prekrši odjeljak 41 712, također bi se postavilo pitanje o spremnosti zrakoplovne tvrtke na poštivanje, što bi moglo u vrlo ozbiljnim situacijama, dovesti do zaključka da zrakoplovna tvrtka više nije sposobna obavljati djelatnost i stoga bi izgubila dozvolu za obavljanje svoje djelatnosti.

DOT je do danas zaprimio relativno malo pritužbi koje se odnose na navodne povrede privatnosti agenata koji prodaju karte ili zračnih prijevoznika. Te se povrede, kada nastanu, istražuju u skladu s gore navedenim načelima.

C. **Pravne zaštite DOT-a koje koriste potrošačima iz EU-a**

U skladu s odjeljkom 41712, zabrana nepoštenih ili prijevarnih postupaka u zračnom prijevozu ili prodaji usluga zračnog prijevoza primjenjuje se na američke i strane zračne prijevoznike i na agente koji prodaju karte. DOT često poduzima mjere protiv američkih i stranih zračnih prijevoznika za prakse koje utječu na strane i američke potrošače na temelju toga da se praksa zračnih prijevoznika dogodila tijekom pružanja usluga prijevoza iz Sjedinjenih Američkih Država i u Sjedinjene Američke Države. DOT upotrebljava i nastavit će upotrebljavati sve pravne lijekove koji su dostupni za zaštitu stranih potrošača i potrošača SAD-a od nepoštenih ili prijevarnih postupaka reguliranih subjekata u zračnom prijevozu.

DOT izvršava, u pogledu zračnih prijevoznika, druge ciljane zakone čija se zaštita proširuje na potrošače izvan EU-a, na primjer Zakonom o zaštiti privatnosti djece na internetu. Zakonom o zaštiti privatnosti djece na internetu propisano je, među ostalim, da operateri *web*-mjesta ili internetskih usluga usmjerenih na djecu ili mjesta za opću publiku koji svjesno prikupljaju osobne podatke od djece mlađe od 13 godine, moraju obavijestiti roditelje i zatražе provjerljivu suglasnost roditelja. Američka *web*-mjesta i usluge na koje se primjenjuje CPPA i koja prikupljaju osobne podatke od strane djece moraju se uskladiti s COPPA-om. Strana *web*-mjesta i internetske usluge također moraju postupati u skladu s COPPA-om ako su usmjereni na djecu u Sjedinjenim Američkim Državama ili ako svjesno prikupljaju osobne podatke od djece u Sjedinjenim Američkim Državama. U mjeri u kojoj SAD ili strani prijevoznici koji posluju u Sjedinjenim Američkim Državama krše COPPA, DOT je nadležan za poduzimanje mjera za izvršenje.

II. PROVEDBA SUSTAVA ZAŠTITE PRIVATNOSTI

Ako zračni prijevoznik ili agent koji prodaje karte odluči da neće sudjelovati u sustavu zaštite privatnosti i Ministarstvo zaprimi pritužbu da taj zračni prijevoznik ili agent koji prodaje karte krši Okvir, Ministarstvo bi poduzelo sljedeće korake za strogu provedbu Okvira:

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Davanje prioriteta navodnim povredama**

Ured Ministarstva za izvršenje u zrakoplovstvu istražuje svaku pritužbu o navodnoj povredi sustava zaštite privatnosti (uključujući pritužbe zaprimljene od tijela za zaštitu podataka iz EU-a) i poduzima mjere izvršenja kada postoje dokazi o povredi. Nadalje, Ured za izvršenje u zrakoplovstvu surađivat će se FTC-om i Ministarstvom trgovine i prvo će razmatrati navode da regulirani subjekti ne poštuju obveze privatnosti preuzete u okviru sustava zaštite privatnosti.

Po primitku navoda o povredi okvira sustava za zaštitu privatnosti, Ured Ministarstva za izvršenje u zrakoplovstvu može u okviru istrage poduzeti niz mjera. Na primjer, on može preispitati politike zaštite privatnosti agenta koji prodaje karte ili zračnog prijevoznika, pribaviti dodatne informacije od agenta koji prodaje karte ili zračnog prijevoznika ili trećih stranaka, tražiti informacije od tijela koje je uputilo predmet i ocijeniti postoji li uzorak povreda ili je pogođen velik broj potrošača. Osim toga, on bi utvrdio jesu li uključena pitanja u nadležnosti Ministarstva trgovine ili FTC-a, ocijenio hoće li biti korisno obrazovanje potrošača i poduzeća i, prema potrebi, pokrenuo postupak izvršenja.

Ako Ministarstvo sazna za moguće povrede sustava zaštite privatnosti koje su počinili agenti koji prodaju karte, ono će to koordinirati s FTC-om. Također ćemo se savjetovati s FTC-om i Ministarstvom trgovine o ishodu mjere izvršenja u sustavu zaštite privatnosti.

B. **Suzbijanje lažnih ili prijevarnih tvrdnji o članstvu u sustavu zaštite privatnosti**

Ministarstvo je i dalje opredijeljeno za istrage povreda sustava zaštite privatnosti, uključujući lažnih i prijevarnih tvrdnji o članstvu u sustavu zaštite privatnosti Davat ćemo prednost razmatranju predmeta koje je uputilo Ministarstvo trgovine u vezi s organizacijama za koje je utvrdilo da se neprimjereno predstavljaju kao aktualni članovi sustava zaštite privatnosti ili koje bez odobrenja upotrebljavaju oznaku članstva u Okviru sustava zaštite privatnosti.

Nadalje, napominjemo da ako organizacija svojom politikom zaštite privatnosti tvrdi da poštuje materijalna načela sustava zaštite privatnosti, ona time što se nije registrirala pri Ministarstvu trgovine vjerojatno neće biti oslobođena toga da DOT izvrši te obveze.

C. **Praćenje i objava naloga o provedbi u vezi s povredama sustava zaštite privatnosti**

Ured Ministarstva za izvršenje u zrakoplovstvu također potvrđuje da se obvezuje prema potrebi pratiti naloge za izvršenje za osiguranje poštovanja načela iz programa sustava zaštite privatnosti. Ako ured izda nalog kojim se traži od zračnog prijevoznika ili agenta koji prodaje karte da prekine povrede i da se suzdrži od daljnjih povreda sustava zaštite privatnosti i odjeljka 41712, on će pratiti postupa li taj subjekt s odredbom o prekidu i suzdržavanju iz naloga. Nadalje, ured će osigurati da su nalozi doneseni u predmetima povezanima za sustavom zaštite privatnosti dostupni na njegovom *web*-mjestu.

Veselimo se daljnjoj suradnji s našim saveznim partnerima i dionicima EU-a na pitanjima povezanima sa sustavom zaštite privatnosti.

Nadam se da će Vam ova informacija biti od koristi. Ako imate kakvih pitanja ili trebate daljnje informacije, slobodno mi se obratite.

S poštovanjem,

Anthony R. Foxx

Ministar prometa

PRILOG VI.

Dopis glavnog savjetnika Roberta Litta
Ured direktora Nacionalne obavještajne službe

22. veljače 2016.

G. Justin S. Antonipillai
Savjetnik
Ministarstvo trgovine SAD-a
1401 Constitution Ave., NW
Washington, DC 20230

G. Ted Dean
Zamjenik pomoćnika Tajnika
Uprava za međunarodnu trgovinu
1401 Constitution Ave., NW
Washington, DC 20230

Poštovana gospodo Antonipillai i Dean:

Tijekom posljednje dvije i pol godine, u kontekstu pregovora o europsko-američkom sustavu zaštite privatnosti, Sjedinjene Američke Države dostavile su znatne informacije o radu aktivnostima prikupljanja obavještajnih podataka elektroničkim izviđanjem koje obavlja američka obavještajna zajednica. To je uključivalo informacije o osnovnom pravnom okviru, višeslojni nadzor tih aktivnosti, opsežna transparentnost tih aktivnosti i opće zaštite privatnosti i građanskih sloboda, kako bi se Europskoj komisiji pomoglo s donošenjem odluke o tome jesu li te informacije odgovarajuće kako se odnose na izuzeće od načela sustava zaštite privatnosti za potrebe nacionalne sigurnosti. U ovom dokumentu sažimaju se dostavljene informacije.

I. PPD-28 I OBAVLJANJE AKTIVNOSTI PRIKUPLJANJA OBAVJEŠTAJNIH PODATAKA ELEKTRONIČKIM IZVIĐANJEM

Obavještajna zajednica SAD-a prikuplja strane obavještajne podatke za pažljivo kontrolirani način u skladu s američkim zakonima i podložno višestrukim slojevima nadzora, s naglaskom na važne strane obavještajne podatke i prioritete nacionalne sigurnosti. Prikupljanje obavještajnih podataka u SAD-u elektroničkim izviđanjem uređeno je različitim zakonima i politikama, među ostalim Ustavom SAD-a, Zakonom o nadzoru stranih obavještajnih službi (50 U.S.C. članak 1801. *i dalje*) (FISA), Izvršnim nalogom br. 12333 i njegovim provedbenim odredbama predsjedničkim smjernicama i brojnim postupcima i smjernicama koje je odobrio Sud FISA-e i glavni državni odvjetnik, a kojima se uspostavljaju dodatna pravila kojima se ograničava prikupljanje zadržavanje, uporaba i širenje stranih obavještajnih podataka ([1]).

a. **Pregled ukaza PPD- 28**

Predsjednik Obama dao je u siječnju 2014. govor u kojem je opisao različite reforme aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem i izdao je Predsjednički ukaz br. 28 (PPD-28) o tim aktivnostima ([2]). Predsjednik je istaknuo da se aktivnostima SAD-a u pogledu prikupljanja obavještajnih podataka elektroničkim izviđanjem pridonosi ne samo sigurnost naše zemlje i naših sloboda već i sigurnosti i sloboda drugih zemalja, među ostalim i država članica EU-a, koje se oslanjaju na podatke koje pribavljaju obavještajne agencije SAD-a kako bi zaštitile svoje građane.

U PPD-28 utvrđen je niz načela i zahtjeva koji se primjenjuju na sve američke aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem i na sve osobe bez obzira na njihovo državljanstvo ili boravište. U njemu su posebno utvrđeni određeni zahtjevi u pogledu postupaka za prikupljanje, zadržavanje i širenje osobnih podataka o osobama izvan EU-a koji su prikupljeni u skladu s američkim aktivnostima prikupljanja obavještajnih podataka elektroničkim izviđanjem. Ti su zahtjevi detaljnije navedeni u nastavku, ali ukratko:

— U predsjedničkom ukazu ponavlja se da Sjedinjene Države prikupljaju obavještajne podatke elektroničkim izviđanjem samo ako je to odobreno zakonom, izvršnim nalogom ili drugim predsjedničkim ukazom.

([1]) Daljnje informacije o aktivnostima prikupljanja stranih obavještajnih koje obavlja SAD navedene su na internetu i javno dostupne na *web*-mjestu *IC on the Record* www.icontherecord.tumblr.com), javnom web-mjestu ODNI-ja posvećenom poticanju veće javne vidljivosti za obavještajne aktivnosti vlade.

([2]) *Dostupno na:* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— Predsjedničkim ukazom uspostavljaju se postupci kojima će se osigurati obavljanje aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem za legitimne i ovlaštene potrebe nacionalne sigurnosti.

— Predsjedničkim ukazom također je propisano da privatnost i građanske slobode moraju biti središnje točke u planiranju aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem. Sjedinjene Američke Države ne prikupljaju obavještajne podatke radi suzbijanja ili otežavanja kritike ili neslaganja; kako bi osobe stavile i nepovoljni položaj zbog njihove nacionalnosti, rase, spola, spolne orijentacije ili vjere; ili radi osiguravanja konkretne tržišne prednosti poduzećima i poslovnim sektorima SAD-a.

— Predsjedničkim ukazom propisano je da aktivnosti prikupljanja obavještajnih podataka praćenjem elektroničkim izviđanjem moraju biti što usmjerenije i da se masovno prikupljeni podaci mogu upotrebljavati samo u posebno nabrojene svrhe.

— Predsjedničkim ukazom propisano je da obavještajna zajednica mora donijeti postupke „koji su razumno oblikovani tako da se njima umanjuje širenje i zadržavanje osobnih podataka prikupljenih aktivnostima prikupljanja obavještajnih podataka elektroničkim izviđanjem", a posebno širenjem određene zaštite osobnih podatka američkih državljana na podatke o osobama koje nisu američki državljani.

— Agencija je donijela i objavila postupke za provedbu PPD-28.

Očita je primjenjivost ovdje propisanih postupaka i zaštita na sustav zaštite privatnosti. Ako su podaci preseneni u korporacije u Sjedinjenim Američkim Državama u skladu sa sustavom zaštite privatnosti ili bilo kojim sredstvom, američke obavještajne agencije mogu tražiti te podatke od tih korporacija samo ako je zahtjev u skladu sa FISA-om ili je podnesen u skladu s jednom od zakonskih odredaba iz dopisa služe nacionalne sigurnosti o kojima je riječ u nastavku ([1]). Nadalje, ne potvrđujući ni ne poričući istinitost izjava u medijima da američka obavještajna zajednica prikupila podatke iz transatlantskih kablova dok se prenose u Sjedinjene Američke Države, kada bi američka obavještajna zajednica prikupljanja podatke iz transatlantskih kablova, ona bi to činila u skladu s ovdje utvrđenim ograničenjima i zaštitnim mjerama, uključujući zahtjeve iz PPD-28.

b. **Ograničenja u pogledu prikupljanja**

U predsjedničkom ukazu br. 28. naveden je niz važnih općih načela koja se primjenjuju na aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem:

— Prikupljanje obavještajnih podataka praćenjem signala elektroničkih sustava mora se temeljiti na zakonu ili predsjedničkom odobrenju i mora se obavljati u skladu s Ustavom ili zakonom.

— Privatnost i građanske slobode moraju biti ključni elementi u planiranju aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem;

— Obavještajni podaci prikupljaju se elektroničkim izviđanjem samo u slučaju valjane potrebe za stranim obavještajnim podacima ili u protuobavještajne potrebe.

— Sjedinjene Američke države neće prikupljati obavještajne podatke elektroničkim izviđanjem za potrebe suzbijanja kritike ili neslaganja.

— Sjedinjene Američke Države neće prikupljati obavještajne podatke elektroničkim izviđanjem osoba s invaliditetom na temelju njihove nacionalnosti, rase, spola, spolne orijentacije ili vjere.

— Sjedinjene Američke Države neće prikupljati obavještajne podatke elektroničkim izviđanjem kako bi osigurale konkurentnu tržišnu prednost poduzećima SAD-a i njegovim poslovnim sektorima.

— Američka aktivnost prikupljanja obavještajnih podataka elektroničkim izviđanjem mora *uvijek* biti što usmjerenija uzimajući u obzir dostupnost drugih izvora informacija. To znači, među ostalim, da se aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem, kad god je to moguće, provode na ciljani način, a ne masovno.

Zahtjev za što usmjerenijom aktivnošću prikupljanja obavještajnih podataka elektroničkim izviđanjem primjenjuje se na način prikupljanja podataka te na što se zapravo prikuplja. Na primjer, kada utvrđuje treba li prikupljati obavještajne podatke elektroničkim izviđanjem, obavještajna zajednica mora razmotriti dostupnost drugih informacija, među ostalim

([1]) Tijela za provedbu zakona i regulatorne agencije mogu tražiti informacije od korporacija za potrebe istrage u Sjedinjenim Američkim državama u skladu s drugim kaznenim, građanskim i regulatornim tijelima koje su izvan područja primjene ovog dokumenta, ali to je pravno ograničeno na nadležna tijela za nacionalnu sigurnost.

iz diplomatskih ili javnih izvora, te dati prednost prikupljanju tim sredstvima, ako je to primjereno i izvedivo. U politikama subjekata obavještajne zajednice trebalo bi biti propisano da, kad god je to izvedivo, prikupljanje bude usmjereno na određene ciljeve prikupljanja stranih obavještajnih podataka ili na teme uporabom razlikovnih čimbenika (npr. posebni objekti, uvjeti odabira i identifikatori.).

Važno je promatrati informacije dostavljene Komisiji u cjelini. O „izvedivosti" ili „praktičnosti" ne odlučuju pojedinci na koje se primjenjuju politike koje su agencije izdale u okviru PPD-28 – koje su objavljene – kao i na druge postupke opisane u nastavku ([1]). U PPD-28 je propisano da je skupno prikupljanje obavještajnih podataka elektroničkim izviđanjem prikupljanje koje se „zbog tehničkih ili operativnih pitanja obavlja bez razlikovnih čimbenika (npr. posebnih identifikatora, posebnih razlikovnih značajki i slično.)" U tom pogledu Predsjedničkim ukazom br. 28 potvrđuje se da subjekti obavještajne zajednice moraju skupno prikupljati obavještajne podatke elektroničkim izviđanjem kako bi mogli utvrditi nove ili nastajuće prijetnje i druge važne informacije za potrebe nacionalne sigurnosti koje su često složene u velikom i složenom sustavu modernih globalnih komunikacija. Njime se također potvrđuje zabrinutost za privatnost i građanske slobode u slučaju skupnog prikupljanja obavještajnih podataka elektroničkim izviđanjem. Predsjedničkim ukazom br. 28 stoga se upućuje obavještajnu zajednicu da odredi prioritete među alternativnim mogućnostima kojima bi se omogućilo prikupljanje obavještajnih podataka elektroničkim izviđanjem, a ne skupno prikupljanje obavještajnih podataka. U skladu s time, subjekti obavještajne zajednice trebali bi kad god je to izvedivo provoditi ciljane aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem, a ne ih skupno prikupljati ([2]). Tim se načelima osigurava da se iznimkom za skupno prikupljanje neće zamijeniti opće pravilo.

Pojam „razumnosti" temeljno je načelo prava SAD-a. On znači da subjekti obavještajne zajednice neće morati donijeti sve teoretski moguće mjere već da će morati uspostaviti ravnotežu između svojih nastojanja da zaštite interese zakonite privatnosti i građanskih sloboda i praktične nužnosti prikupljanja obavještajnih podataka praćenjem signala elektroničkih komunikacija. I u ovom slučaju objavljene su politike agencija koje mogu zajamčiti da se pojmom „razumno osmišljene kako bi se širenje i zadržavanje osobnih podataka sveli na najmanju moguću mjeru" ne ugrožava opće pravilo.

U Predsjedničkom ukazu br. 28 također je predviđeno da se masovno prikupljeni obavještajni podaci mogu upotrebljavati samo u šest posebnih svrha: otkrivanje i suzbijanje određenih aktivnosti stranih sila, borba protiv terorizma, borba protiv širenja oružja, kibersigurnost, otkrivanje i suzbijanje prijetnji američkim ili saveznim vojnim snagama i suzbijanje prekograničnih kaznenih prijetnji, među ostalim izbjegavanja sankcija. Predsjednikov savjetnik za nacionalnu sigurnost, u dogovoru s Direktorom Nacionalne obavještajne službe (DNI), svake će godine preispitati dopuštene uporabe masovno prikupljenih podataka elektroničkim izviđanjem kako bi provjerio treba li ih mijenjati. DNI će se pobrinuti da taj popis bude što dostupniji javnosti, u skladu s pitanjima nacionalne sigurnosti. To je važno i transparentno ograničenje uporabe masovnog prikupljanja obavještajnih podataka elektroničkim izviđanjem.

Nadalje, subjekti obavještajne zajednice koji provode PPD-28 pojačali su postojeće analitičke prakse i standarde za istrage neocijenjenih obavještajnih podataka prikupljenih elektroničkim izviđanjem ([3]). Analitičari moraju oblikovati svoje upite ili druge izraze i tehnike za pretraživanje kako bi osigurali da su oni primjereni za pronalaženje obavještajnih podataka koji su relevantni za zadaće prikupljanja stranih obavještajnih podataka ili tijela kaznenog progona. U tu svrhu subjekti obavještajne zajednice moraju usmjeriti upite o osobama na kategorije obavještajnih podataka koje odgovaraju zahtjevu stranih obavještajnih aktivnosti ili kaznenog progona kako bi se spriječila uporaba osobnih podataka koji nisu važni za zahtjeve stranih obavještajnih aktivnosti ili kazenog progona.

Važno je napomenuti da se svako skupno prikupljanje komunikacije na internetu koje obavještajna zajednica SAD-a obavlja elektroničkim izviđanjem odvija na malom dijelu interneta. Nadalje, uporabom ciljanih upita, kako je prethodno opisano, osigurava se da se analitičarima na ispitivanje dostavljaju samo podaci za koje se vjeruje da imaju obavještajnu vrijednost. Svrha je tih ograničenja zaštititi privatnost i građanske slobode svih osoba, bez obzira kojeg su državljanstva i bez obzira na to gdje im je boravište.

([1]) *Dostupno na* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Tim se postupcima provode pojmovi usmjeravanja i prilagođavanja o kojima je riječ u ovom dopisu na način koji je specifičan za svaki subjekt obavještajne zajednice.

([2]) Na primjer, u postupcima NSA-a za provedbu Predsjedničkoga ukaza br. 28 navedeno je navedeno je da kad god je to moguće, prikupljanje će se izvršiti uporabom jedne ili više posebne razlikovne značajke radi usmjeravanja prikupljanja na određene strane obavještajne ciljeve (npr. posebni poznati međunarodni teroristi ili terorističke skupine) ili na određene teme stranih obavještajnih podataka (npr. širenje oružja za masovno uništenje koje obavlja strana sila ili njezini agenti).

([3]) *Dostupno na* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Sjedinjene Američke Države imaju razrađene postupke za osiguravanje obavljanja aktivnosti prikupljanja podataka elektroničkim izviđanjem samo radi ostvarenja odgovarajuće potrebe nacionalne sigurnosti. Predsjednik svake godine utvrđuje najviše prioritete države za prikupljanje stranih obavještajnih podataka nakon opsežnog, formalnog postupka među agencijama. DNI je odgovoran za prenošenje tih obavještajnih prioriteta u Okvir prioriteta za nacionalne obavještajne službe ili NIPF: Predsjedničkim ukazom br. 28 pojačala se i osnažila međuagencijska suradnja kako bi se osiguralo preispitivanje svih prioriteta obavještajne zajednice te kako bi ih odobrili donositelji politika na visokoj razini. U Predsjedničkom ukazu o obavještajnoj zajednici (ICD) 204 navedene su daljnje smjernice o NIPF-u i on je ažuriran u siječnju 2015. kako bi se u njega uključili zahtjevi iz Predsjedničkog ukaza br. 28. ([1]). Iako je NIPF povjerljiv, informacije povezane s posebnim stranim obavještajnim prioritetima SAD-a navode se svake godine u javnoj DNI-jevoj „Procjeni prijetnji u svijetu", koja je isto dostupna na *web*-mjestu ODNI-ja.

Prioriteti u NIPF-u prilično su općeniti. Oni uključuju teme poput traženje nuklearnih i balističkih sposobnosti posebnih stranih protivnika, učinke korupcije kartela i zlouporabe ljudskih prava u određenim zemljama. I ne primjenjuju se samo na prikupljanje obavještajnih podataka elektroničkim izviđanjem već na sve aktivnosti prikupljanja obavještajnih podataka. Organizacija koja je odgovorna za prenošenje prioriteta iz NIPF-a u stvarno prikupljanje obavještajnih podataka elektroničkim izviđanjem naziva se Nacionalni odbor za prikupljanje obavještajnih podataka elektroničkim izviđanjem ili SIGCOM. On djeluje pod okriljem direktora Nacionalne sigurnosne agencije (NSA) koji je Izvršnim nalogom br. 12333 imenovan „funkcionalnim upraviteljem za prikupljanje obavještajnih podataka elektroničkim izviđanjem" koji je odgovoran za nadzor i koordinaciju prikupljanja obavještajnih podataka u obavještajnoj zajednici pod nadzorom Ministra obrane i DNI-ja. U SIGCOM-u se nalaze predstavnici iz svih subjekata obavještajne zajednice i, budući da Sjedinjene Američke Države u cijelosti provode Predsjednički ukaz br. 28., uključivat će i predstavnike iz drugih odjela i agencija koji imaju interes za prikupljanje obavještajnih podataka elektroničkim izviđanjem.

Svi odjeli i agencije SAD-a koji su potrošači stranih obavještajnih podataka SIGCOM-u podnose svoj zahtjev za prikupljanje. SIGCOM preispituje te zahtjeve, osigurava da su u skladu s NIPF-om i dodjeljuje im prioritete primjenom kriterija poput:

— Mogu li se prikupljanjem obavještajnih podataka elektroničkim izviđanjem u ovom slučaju osigurati korisne informacije ili postoje bolji ili isplativiji izvori informacija za zadovoljavanje zahtjeva, poput slika ili otvorenih izvora komunikacija?

— Koliko je kritična potreba za podacima? Ako je visok prioritet u NIPF-u, obično će biti visok prioritet u pogledu prikupljanja obavještajnih podataka elektroničkim izviđanjem.

— Kakva se vrsta obavještajnih podataka prikupljenih elektroničkim izviđanjem može upotrijebiti?

— Je li prikupljanje što usmjerenije? Trebaju li postojati vremenska, zemljopisna ili druga ograničenja?

Američki zadovoljavanja zahtjeva za prikupljanje obavještajnih podataka elektroničkim izviđanjem zahtijeva i izričito razmatranje drugih čimbenika, odnosno sljedećih:

— Jesu li predmet prikupljanja ili metodologija koja se upotrebljava za prikupljanje posebno osjetljivi? Ako je tako kreatori politika morat će ih preispitati.

— Hoće li prikupljanje činiti neželjeni rizik za privatnost i građanske slobode, neovisno o državljanstvu?

— Jesu li potrebne dodatne zaštitne mjere u pogledu širenja i zadržavanja radi zaštite privatnosti i ostalih interesa nacionalne sigurnosti?

I konačno, na kraju postupka, osposobljeni zaposlenici NSA-a uzimaju prioritete koje je potvrdio SIGCOM i traže i utvrđuju posebne čimbenike za odabir, poput brojeva telefona ili adresa e-pošte, s pomoću kojih se očekuje prikupljanje stranih obavještajnih podataka koji odgovaraju tim prioritetima. Svaki se čimbenika za odabir mora preispitati i odobriti prije unošenja u sustave prikupljanja. Međutim, čak će i tada stvarno vrijeme prikupljanja ovisiti

([1]) *Dostupno na* http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

dijelom o dodatnim pitanjima poput dostupnosti odgovarajućih izvora za prikupljanje. Tim se postupcima osigurava da su ciljevi prikupljanja obavještajnih podataka elektroničkim izviđanjem odraz valjanih i važnih potreba za stranim obavještajnim podacima. Naravno, kada se prikupljanje obavlja u skladu s FISA-om, NSA i druge agencije dužne su primjenjivati dodatna ograničenja koja je odobrio Sud za nadzor stranih obavještajnih aktivnosti. Ukratko, ni NSA ni bilo koja druga obavještajna agencija SAD-a ne odlučuju same što će prikupljati.

Ovim se postupkom općenito osigurava da viši kreatori politike utvrde prioritete za prikupljanje obavještajnih podataka elektroničkim izviđanjem jer su u oni u najboljem položaju da mogu utvrditi zahtjeve SAD-a za stranim obavještajnim podacima te da ti kreatori politika uzmu u obzir ne samo moguću vrijednost prikupljanja obavještajnih podataka već i rizike povezane s tim prikupljanjem, među ostalim rizike za privatnost, nacionalne gospodarske interese i vanjske odnose.

U pogledu podataka prenesenih u Sjedinjene Države u skladu sa sustavom zaštite privatnosti, iako Sjedinjene Američke Države ne mogu potvrditi ni poreći posebne metode ili postupke prikupljanja obavještajnih podataka, zahtjevi iz Predsjedničkog ukaza br. 28. primjenjuju se na sve operacije prikupljanja obavještajnih podataka elektroničkim izviđanjem koje provode Sjedinjene Američke Države bez obzira na vrstu ili izvor podataka koji se prikupljaju. Nadalje, ograničenja i zaštitne mjere koje se primjenjuju na prikupljanje obavještajnih podataka elektroničkim izviđanjem primjenjuju se na obavještajne podatke prikupljene elektroničkim izviđanjem za bilo koju odobren u svrhu, uključujući za strane odnose i svrhe nacionalne sigurnosti.

Prethodno spomenuti postupci upućuju na snažnu obvezu sprječavanja arbitrarnog i neselektivnog prikupljanja obavještajnih podataka elektroničkim izviđanjem i za provedbu načela razumnosti – s najviših razina naše Vlade. Predsjedničkim ukazom br. 28. i provedbenim postupcima agencije pojašnjavaju se nova i postojeća ograničenja i detaljno se opisuje svrha za koju Sjedinjene Američke Države prikupljaju i upotrebljavaju obavještajne podatke prikupljene elektroničkim izviđanjem. Time bi se trebala osigurati jamstva da se aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem obavljaju i da će se nastaviti obavljati za postizanje zakonitih ciljeva prikupljanja stranih obavještajnih podataka.

c. **Ograničenja u pogledu zadržavanja i širenja**

U odjeljku 4. Predsjedničkog ukaza br. 28. propisano je da svaki subjekt obavještajne zajednice ima izričita ograničenja u pogledu zadržavanja i širenja osobnih podataka o osobama koje nisu američki državljani prikupljeni elektroničkim izviđanjem, što je slično ograničenjima za američke državljane. Ta su pravila ugrađena u postupke za svaku agenciju obavještajne zajednice koja su objavljena u veljači 2015. i javno su dostupna. Da bi se mogli zadržavati ili širiti kao strani obavještajni podaci, osobni podaci moraju se odnositi na zahtjev odobrenih obavještajnih podataka, kako je utvrđeno u prethodno opisanom postupku NIPF-a: mora se razumno vjerovati da su dokaz o počinjenom zločinu; ili moraju zadovoljavati jedan od drugih standarda za zadržavanje osobnih podatka američkih državljana iz Izvršnog naloga br. 12333. odjeljak 2.3.

Podaci u odnosu na koje nije utvrđeno ništa ne mogu se zadržavati dulje od pet godina, osim ako je DNI izričito utvrdio da je trajno zadržavanje u interesu nacionalne sigurnosti Sjedinjenih Američkih Država. Stoga subjekti obavještajne zajednice moraju obrisati podatke o osobama koje nisu američki državljani prikupljene elektroničkim izviđanjem, osim ako je, na primjer, utvrđeno za te podatke da su relevantni za odobreni zahtjev za prikupljanje stranih obavještajnih podataka ili ako DNI utvrdi, nakon što je uzeo u obzir stajališta ODNI-ja, službenika za zaštitu građanskih sloboda i službenika agencije za zaštitu privatnosti i građanske slobode, da je trajno zadržavanje u interesu međunarodne sigurnosti.

Nadalje, u svim politikama agencije kojima se provodi Predsjednički ukaz br. 28. sada je izričito propisano da se informacije o osobama ne smiju širiti samo zato što pojedinac nije američki državljanin i ODNI je izdao smjernice svim subjektima obavještajne zajednice ([1]) u kojima je naveden taj zahtjev. Pri izradi i širenju izvješća o prikupljanju obavještajnih podataka, djelatnici obavještajne zajednice posebno moraju uzeti obzir interese privatnosti osoba koje nisu američki državljani. Obavještajni podaci o strancu prikupljeni elektroničkim izviđanjem ne bi se smatrali stranim obavještajnim podacima koji se mogu širiti ili trajno čuvati samo zbog te činjenice, osim ako se na neki drugi način zadovoljava zahtjev ovlaštenih stranih obavještajnih podataka. Time se potvrđuju važna ograničenja i to je odgovor na zabrinutost Europske komisije u pogledu opsega definicije stranih obavještajnih podataka utvrđene u Izvršnom nalogu br. 12333.

([1]) Direktiva o obavještajnoj zajednici (ICD) 203, *dostupna na* http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Usklađenost načela i nadzor**

U američkom sustavu za nadzor stranih obavještajnih podatka osigurava se strogi i višeslojni nadzor u cilju osiguranja poštovanja primjenjivih zakona i postupaka, među ostalim onih koji se odnose na osobne podatke prikupljene elektroničkim izviđanjem kako je navedeno u Predsjedničkom ukazu br. 28. One uključuju sljedeće:

— Obavještajna zajednica zapošljava stotine nadzornika. Samo NSA ima 300 zaposlenih koji rade na poštovanju načela, a i drugi subjekti imaju nadzorne urede. Nadalje, Ministarstvo pravosuđa osigurava opsežan nadzor obavještajnih aktivnosti, a taj se nadzor osigurava i Direktivom

— Svaki subjekt obavještajne zajednice ima vlastiti Ured glavnog inspektora koji je odgovoran za nadzor stranih obavještajnih aktivnosti i drugih pitanja. Glavni inspektori zakonski su neovisni. ni imaju široke ovlasti provodit istrage, revizije i preispitivanja programa, među ostalim prijevare i zlouporabe ili povrede zakona i mogu preporučiti korektivne mjere. Iako preporuke glavnog inspektora nisu obvezujuće, izvješća glavnog inspektora često se objavljuju i, u svakom slučaju, dostavljaju se Kongresu. To uključuje izvješća o praćenju u slučaju u slučaju da korektivne mjere predložene u prethodnim izvješćima još nisu izvršene. Stoga se Kongres obavješćuje o neusklađenosti i može izvršiti pritisak, među ostalim proračunskim sredstvima, za postizanje korektivnih mjera. Brojna su izvješća glavnog inspektora o obavještajnim programima javno objavljena ([1]).

— Ured ODNI-ja za građanske slobode i privatnost (CLPO) zadužen je osigurati da obavještajna zajednica djeluje na način kojim se promiče nacionalna sigurnost uz zaštitu građanskih sloboda i prava privatnosti ([2]). Drugi subjekti obavještajne zajednice imaju vlastite službenike za zaštitu privatnosti.

— Odbor za nadzor privatnosti i građanske slobode (PCLOB), neovisno tijelo osnovano zakonom, zaduženo je za analizu i preispitivanje programa i politika borbe protiv terorizma, među ostalim uporabe prikupljanja obavještajnih podataka elektroničkim izviđanjem kako bi se osiguralo da se njima na odgovarajući način štiti privatnost i građanske slobode. Izdao je nekoliko javnih izvješća o obavještajnim aktivnostima.

— Kako je detaljno opisano u prethodnom tekstu, Sud za nadzor obavještajnih aktivnosti koji je sastavljen od neovisnih saveznih sudaca, odgovoran je za nadzor i usklađenost aktivnosti prikupljanja obavještajnih podataka elektroničkim izviđanjem koje se obavljaju u skladu s FISA-om.

— Naposljetku, Odbori za obavještajne podatke i pravosuđe Donjeg doma i Senata imaju ovlasti nadzora nad svim stranim američkim obavještajnim aktivnostima, uključujući aktivnosti praćenja signala komunikacijskih sustava koje obavlja SAD.

Osim tih formalnih nadzornih mehanizama, obavještajna zajednica uspostavila je brojne mehanizme za osiguranje da obavještajna zajednica postupa u skladu s prethodno opisanim ograničenjima prikupljanja. Na primjer:

— Članovi Kabineta dužni su svake godine potvrditi svoje zahtjeve u pogledu prikupljanja obavještajnih podataka elektroničkim izviđanjem.

— NSA provjerava subjekte prikupljanja obavještajnih podataka elektroničkim izviđanjem tijekom cijelog postupka prikupljanja kako bi utvrdio osiguravaju li se njima zaista vrijedni obavještajni podaci koji odgovaraju prioritetima i zaustavit će prikupljanje podataka o subjektima koji nisu. Dodatnim postupcima osigurava se povremeno preispitivanje razlikovnih značajki.

([1]) *Vidjeti, na primjer,* Opće izvješće inspektora Ministarstva pravosuđa SAD-a „Pregled aktivnosti Saveznog istražnog ureda u skladu s odjeljkom 702. Zakona o o nadzoru stranih obavještajnih službi iz 2008." (rujan 2012.), *dostupno na* https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) *Vidjeti* www.dni.gov/clpo.

— Na temelju preporuka neovisne skupine za preispitivanje koju je imenovao Predsjednik Obama, DNI je uspostavio novi mehanizam za praćenje prikupljanja i širenja obavještajnih podataka prikupljenih elektroničkim izviđanjem koji su posebno osjetljivi zbog prirode subjekta ili načina prikupljanja, kako bi se osiguralo da je to u skladu s onim što su propisali kreatori politika.

— Naposljetku, ODNI svake godine preispituje sredstva dodijeljena obavještajnoj zajednici u odnosu na prioritete NIPF-a i obavještajnu misiju u cjelini. Ovo preispitivanje uključuje ocjenjivanje vrijednosti svih vrsta prikupljanja obavještajnih podatka, među ostalim prikupljanje elektroničkim izviđanjem – koliko uspješna je bila obavještajna zajednica u postizanju svojih ciljeva? – i dalje – što će biti potrebno obavještajnoj zajednici u budućnosti? Tim se osigurava da se sredstva dodijeljena za prikupljanje obavještajnih podataka elektroničkim izviđanjem primjenjuju na najvažnije nacionalne prioritete.

Kako je prikazano ovim sveobuhvatnim pregledom, obavještajna zajednica ne odlučuje sama o tome koje razgovore slušati, ne pokušava prikupljati sve i ne djeluje bez nadzora. Njezine su aktivnosti usmjerene na prioritete koje su odredili kreatori politika u postupku koji uključuje doprinos cijele vlade i koji se nadzire unutar NSA i koji nadziru NSA, ODNI, Ministarstvo pravosuđa i Ministarstvo obrane.

Predsjednički ukaz br. 28. sadržava brojne druge odredbe kojima se osigurava da je prikupljanje obavještajnih podataka elektroničkim izviđanjem zaštićeno, neovisno o državljanstvu osobe čiji se podaci prikupljaju. Na primjer, u Predsjedničkom ukazu br. 28. propisana je sigurnost podataka, pristup i kvalitetni postupci za zaštitu osobnih podataka prikupljenih elektroničkim izviđanjem i predviđa se obvezno osposobljavanje kako bi se osiguralo da radnici razumiju odgovornost zaštite osobnih podataka, neovisno o državljanstvu osobe čiji se podaci prikupljaju. U Predsjedničkom ukazu predviđen je i dodatni nadzor i mehanizmi za osiguravanje poštovanja načela. Oni uključuju povremene revizije i preispitivanja koje provode nadležni službenici za nadzor i usklađenost kako bi osigurali zaštitu osobnih podataka sadržanih u obavještajnim podacima prikupljenima elektroničkim izviđanjem. Tijekom preispitivanja mora se razmotriti i poštuju li agencije postupke za zaštitu takvih podataka.

Osim toga, Predsjedničkim ukazom br. 28. predviđeno je da se važna pitanja poštovanja načela povezana s osobama koje nisu američki državljani rješavaju na višim razinama vlade. Ako se važno pitanje poštovanja načela pojavi u vezi s osobnim podacima bilo koje osobe koji su prikupljeni elektroničkim izviđanjem, o tome se pitanju, pored svih postojećih zahtjeva izvješćivanja, mora odmah izvijestiti DNI. Ako se podaci odnose na osobu koja nije američki državljanin, DNI, u dogovoru s državnim tajnikom i čelnikom predmetnog subjekta obavještajne zajednice, utvrđuje treba li poduzeti korake za obavješćivanje predmetne strane vlade, u skladu sa zaštitom izvora i metoda američkog osoblja. Nadalje, kako je navedeno u Predsjedničkom ukazu br. 28., državni tajnik odredio je višeg dužnosnika, zamjenicu državnog tajnika Catherine Novelli, koji će biti kontaktna točka za strane vlade koje žele izraziti zabrinutost u vezi s aktivnostima prikupljanja obavještajnih podataka elektroničkim izviđanjem. Ova opredijeljenost za djelovanje na visokoj razini primjer je napora koje je američka vlada uložila posljednjih godina kako bi pojačala ovjerenje u brojne i dvostruke zaštite privatnosti osobnih podataka američkih državljana i osoba koje nisu američki državljani.

e. **Sažetak**

U okviru postupaka Sjedinjenih Američkih Država za prikupljanje obavještajnih podataka elektroničkim izviđanjem osiguravaju se važni mehanizmi zaštite privatnosti osobnih podataka svih osoba, bez obzira na njihovo državljanstvo. Tim se postupcima posebno osigurava da naša obavještajna zajednica usmjerava svoje misije zaštite nacionalne sigurnosti na način odobren primjenjivim zakonima, izvršnim nalazima i predsjedničkim ukazima; da štiti podatke od neovlaštenog pristupa, uporabe i otkrivanja; i da obavlja svoje aktivnosti pod višestrukim razinama preispitivanja i nadzora, među ostalim s pomoću kongresnih nadzornih odbora. Predsjednički ukaz br. 28. i postupci za njegovu provedbu predstavljaju naše napore usmjerene na proširenje načela prikupljanja najmanje potrebne količine podataka i drugih važnih načela zaštite podataka na osobne podatke svih osoba bez obzira na državljanstvo. Na osobne podatke dobivene prikupljanjem obavještajnih podataka elektroničkim izviđanjem primjenjuju se načela i zahtjevi zakonodavstva EU-a i predsjedničkog ukaza, uključujući zaštite iz Predsjedničkog ukaza br. 28. Tim se načelima i zahtjevima osigurava da se prema svim osobama postupa s dostojanstvom i poštovanjem, neovisno o njihovom državljanstvu i boravištu i potvrđuje da sve osobe imaju legitimne interese privatnosti u vezi s postupanjem njihovih osobnih podataka.

II. ZAKON O NADZORU STRANIH OBAVJEŠTAJNIH PODATAKA – ODJELJAK 702.

Prikupljanje podataka u skladu s odjeljkom 702. Zakona o nadzoru stranih obavještajnih službi ([1]) nije „masovno i neselektivno", već je strogo usmjereno na prikupljanje stranih obavještajnih podataka o pojedinačno utvrđenim zakonitim ciljevima prikupljanja; jasno je ovlašteno na temelju izričite zakonite ovlasti; i podliježe neovisnoj sudskoj reviziji i znatnom preispitivanju i nadzoru izvršne vlasti i Kongresa. Prikupljanje u skladu s odjeljkom 702. smatra se prikupljanjem obavještajnih podataka elektroničkim izviđanjem koje podliježe zahtjevima iz Predsjedničkog ukaza br. 28. ([2]).

Prikupljanje u skladu s odjeljkom 702. jedan je od najvrjednijih izvora obavještajnih podataka kojim se štite Sjedinjene Američke Države i naši europski partneri. Detaljne informacije o primjeni i nadzoru odjeljka 702. javno su dostupne. Brojni sudski podnesci, sudske odluke i izvješća o nadzoru povezani s programom deklasificirani su i objavljeni su na ODNI-jevom *web*-mjestu za obavješćivanje javnosti, www.icontherecord.tumblr.com. Nadalje, Odbor za nadzor privatnosti i građanske slobode detaljno je analizirao odjeljak 702., a izvješće o tome dostupno je na https://www.pclob.gov/library/702-Report.pdf ([3]).

Odjeljak 702. donesen je u okviru Zakona o izmjenama FISA-e iz 2008 ([4]), nakon opsežne rasprave u Kongresu. Njime se odobrava stjecanje stranih obavještajnih podataka o osobama koje nisu američki državljani i nalaze se izvan Sjedinjenih Američkih Država uz pomoć američkih pružatelja komunikacijskih usluga. Odjeljkom 702. ovlašćuje se Glavni državni odvjetnik i DNI, dva člana Kabineta koje imenuje Predsjednik i potvrđuje Senat, da podnose godišnje certifikacije Sudu za FISA ([5]). Tim se certifikatima utvrđuju posebne kategorije obavještajnih podataka koje se mogu prikupljati, na primjer podaci povezani s borbom protiv terorizma ili oružjem masovnog uništenja, što mora biti u okviru kategorija stranih obavještajnih podataka definiranih u zakonu FISA ([6]). Kako je naveo PCLOB, „tim ograničenjima *ne* dopušta se neograničeno prikupljanje podataka o strancima" ([7]).

Certifikati moraju uključivati i postupke „usmjeravanja" i „prikupljanja najmanje količine podataka" koje mora preispitati i odobriti Sud za FISA ([8]). Postupcima usmjeravanja nastoji se osigurati da se prikupljanje odvija u skladu sa zakonom i da je unutar područja primjene certifikata. Svrha je postupaka kojima se prikuplja najmanja potrebna količina podataka ograničiti stjecanje, širenje i zadržavanje podataka o američkim državljanima, ali i uključiti odredbe kojima se osigurava znatna zaštita podataka o osobama koje nisu američki državljani, kako je opisano u nastavku. Nadalje, kako je prethodno opisano, Predsjednik je u Predsjedničkom ukazu br. 28. odredio da obavještajna zajednica mora osigurati dodatne zaštite osobnih podataka o osobama koje nisu američki državljani i da se te zaštite primjenjuju na podatke prikupljene u skladu s odjeljkom 702.

Kada sud odobri postupke usmjeravanja i prikupljanja najmanje količine podataka, prikupljanje u skladu s odjeljkom 702. ne obavlja se masovno ili neselektivno već se „sastoji potpuno od usmjeravanja na posebne osobe za koje je određeno prikupljanje podataka", kako je izjavio PCLOB ([9]). Prikupljanje se usmjerava uporabom pojedinačnih čimbenika za odabir, na primjer adresa e-pošte ili telefonskih brojeva, za koje su američki subjekti obavještajne zajednice

([1]) 50 U.S.C. članak 1881.a.

([2]) Sjedinjene Američke Države mogu pribaviti sudske naloge za prikupljanje podataka u skladu s drugim odredbama FISA-e, među ostalim podataka prenesenih u skladu sa sustavom zaštite podataka.*Vidjeti* 50 U.S.C. članak 1801. *i dalje*. Za naslove I i III. FISA-e, kojima se ovlašćuje elektronički nadzor i fizički pregledi, potreban je sudski nalog (osim u hitnim slučajevima) i uvijek se moraju temeljiti na opravdanoj osnovi na temelju koje se može smatrati da je subjekt prikupljanja podataka strana sila ili agent strane sile. Glavom IV. ovlašćuje se uporaba uređaja za bilježenje ulaznih i izlaznih poziva na temelju sudskog naloga (osim u hitnim slučajevima) u odobrenim istragama u okviru prikupljanja stranih obavještajnih podataka, protuobavještajnih aktivnosti i suzbijanja terorizma. Glavom V. FISA-e dopušta se FBI-ju, na temelju sudskog naloga (osim u iznimnim okolnostima) da pribavi poslovnu evidenciju koja je relevantna za odobrene istrage u okviru prikupljanja stranih obavještajnih podataka, protuobavještajne aktivnosti i suzbijanja terorizma. Kako je prethodno navedeno, u američkom Zakonu o slobodi posebno je zabranjena uporaba naloga za prisluškivanje ili prikupljanje poslovne evidencije za potrebe masovnog prikupljanja i određuje se zahtjev „posebne razlikovne značajke" kako bi se osiguralo da se te ovlasti upotrebljavaju na ciljani način.

([3]) Odbor za zaštitu privatnosti i građanske slobode „Izvješće o programu nadzora koji se provodi u skladu s odjeljkom 702. Zakona o nadzoru stranih obavještajnih službi" (2. srpnja 2014. („Izvješće PCLOB-a").

([4]) *Vidjeti* Pub. L. No. 110-261, 122 Stat. 2436 (2008.).

([5]) *Vidjeti* 50 U.S.C. članak 1881.a(a) i (b).

([6]) *Vidjeti id*. članak 1801.(e).

([7]) *Vidjeti* Izvješće o PCLOB-u na 99.

([8]) *Vidjeti* 50 U.S.C. članak 1881.a točke (d) i (e).

([9]) *Vidjeti* Izvješće o PCLOB-u na 111.

utvrdili da će se vjerojatno upotrebljavati za prijenos stranih obavještajnih podataka vrste koja je obuhvaćena certifikatom koji je dostavljen sudu ([1]). Osnova za odabir subjekta prikupljanja mora biti evidentirana i Ministarstvo pravosuđa naknadno preispituje dokumentaciju za svaki čimbenik za odabir ([2]). Američka vlada objavila je informacije iz kojih je razvidno da je 2014. prikupljanje u skladu s odjeljkom 702. bilo usmjereno na 90 000 osoba, što je vrlo mali dio od više od 3 milijarde korisnika interneta u cijelom svijetu ([3]).

Na primjer podaci prikupljeni u skladu s odjeljkom 702. podliježu postupcima kojima se prikupljanje svodi na najmanju moguću razinu i kojima se osigurava zaštita osobama koje nisu američki državljani kao i američkim državljanima i koji su javno objavljeni ([4]). Na primjer, komunikacijski podaci prikupljeni u skladu s odjeljkom 702. o američkim državljanima i osobama koje nisu američki državljani pohranjeni su u bazama podataka sa strogim kontrolama pristupa. Te podatke mogu pregledavati samo djelatnici obavještajne službe koji su osposobljeni za postupke kojima se prikupljanje svodi na najmanju moguću razinu i kojima je posebno odobren pristup tim podacima kako bi mogli obavljati zadaće za koje su ovlašteni ([5]). Uporaba podataka ograničena je na pronalaženje stranih obavještajnih podataka ili dokaza o zločinu ([6]). U skladu s Predsjedničkim ukazom br. 28., ti se podaci mogu širiti samo ako postoji valjana svrha prikupljanja stranih obavještajnih podataka ili svrha provedbe zakona; nije dovoljna sama činjenica da jedna strana u postupku komunikacije nije američki državljanin ([7]). Postupcima kojima se prikupljanje svodi na najmanju moguću razinu i Predsjedničkim ukazom br. 28. ograničava se duljina zadržavanja podataka prikupljenih u skladu s odjeljkom 702 ([8]).

Nadzor iz odjeljka 702. opsežan je i obavljaju ga sva tri ogranka vlasti. Agencije koje provode zakon imaju višestruke razine unutarnjeg preispitivanja koje provode, među ostalim, glavni inspektori, te tehnološku kontrolu nad pristupom podacima. Ministarstvo pravosuđa i ODNI pažljivo preispituju i nadziru uporabu odjeljka 702. radi provjere usklađenosti sa zakonskim pravilima; agencije imaju također neovisnu obvezu izvješćivanja o mogućim slučajevima nepoštovanja pravila. Ti se slučajevi istražuju i svi se slučajevi nepoštovanja pravila prijavljuju Sudu za nadzor stranih obavještajnih aktivnosti, predsjednikovom Odboru za nadzor obavještajnih službi i Kongresu te se, prema potrebi, ispravljaju ([9]). Do danas nje bilo slučajeva namjernih pokušaja povrede zakona ili izbjegavanja pravnih zahtjeva ([10]).

Sud FISA ima važnu ulogu u provedbi odjeljka 702. On je sastavljen od neovisnih saveznih sudaca koji služe kao suci na Sudu za FISA sedam godine, ali koji, kao i savezni suci, imaju doživotni mandat. Kako je prethodno navedeno, Sud mora preispitati godišnje certifikacije i usmjeravanje prikupljanja podataka kao i postupke kojima se prikupljanje svodi na najmanju moguću razinu u skladu sa zakonom. Nadalje, kako je prethodno navedeno, Vlada mora odmah obavijestiti Sud o slučajevima nepoštovanja pravila ([11]) i nekoliko sudskih mišljenja deklasificirano je i pokazalo je iznimni stupanj sudskog nadzora i neovisnosti u preispitivanju tih slučajeva.

Zahtjevne postupke Suda opisao je bivši predsjedavajući sudac u dopisu Kongresu koje je javno objavljeno ([12]). Na temelju Zakona o slobodi SAD-a, koji je opisan u nastavku, Sud je sada izričito ovlašten imenovati vanjskog odvjetnika kao neovisnog zaštitnika privatnosti u slučajevima kada se javljaju nova ili važna pravna pitanja ([13]). Ovakav stupanj uključenosti neovisnog sudstva države u aktivnostima prikupljanja stranih obavještajnih podataka o osobama koje nisu državljani te zemlje niti borave u toj zemlji nije neuobičajeno i njime se osigurava prikupljanje u skladu s odjeljkom 702. unutar odgovarajućih zakonskim granica.

([1]) *Id*.

([2]) *Id*. pod 8; 50 U.S.C. članak 1881.a točka I.: *vidjeti isto* Izvješće direktora NSA o zaštiti građanskih sloboda i privatnosti, „Primjena odjeljka 702. Zakona o stanom obavještajnom nadzoru u radu NSA" (dalje u tekstu: „Izvješće NSA") pod 4., *dostupno na* http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Izvješće o transparentnosti direktora Nacionalne obavještajne službe iz 2014, *dostupno na* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Postupci kojima se prikupljanje svodi na najmanju moguću razinu dostupni su na: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf („Postupci koje NSA primjenjuje na prikupljanje podataka svođenjem prikupljanja na najmanju moguću razinu"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; i http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) *Vidjeti* Izvješće NSA pod 4.

([6]) *Vidjeti npr.*Postupci NSA za svođenje prikupljanja na najmanju moguću razinu pod 6.

([7]) Postupci obavještajne agencije u skladu s predsjedničkim ukazom 28 dostupni su na http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) *Vidjeti* Postupci NSA za svođenje prikupljanja na najmanju moguću razinu PPD-28, odjeljak 4.

([9]) *Vidjeti* 50 U.S.C. članak 1881. točka I:; *vidjeti isto* Izvješće PCLOB-a na 66. – 76.

([10]) *Vidjeti* Polugodišnja ocjena usklađenosti s postupcima i smjernicama u skladu s odjeljkom 702. Zakona o nadzoru stranih obavještajnih službi, koju su dostavili Glavni državni odvjetnik i direktor Nacionalne obavještajne službe pod 2-3, dostupno na http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Pravilo 13. Poslovnika Suda za nadzor stranih obavještajnih aktivnostima *dostupno na* http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) 29. srpnja 2013. Dopis časnog suca Reggiea B. Waltona časnom sucu Patricku J. Leahyju, *koji je dostupan na* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) *Vidjeti* Odjeljak 401. Zakon o slobodi SAD-a, P.L. 114. – 23.

Kongres izvršava nadzor s pomoću zakonom propisanih izvješća odborima za nadzor obavještajnih službi i sudova te čestim izvješćivanjem i raspravama. To uključuje polugodišnje izvješće glavnog državnog odvjetnika u kojem je opisana primjena odjeljka 702. i svi slučajevi nepridržavanja ([1]); posebnu polugodišnju ocjenu glavnog državnog odvjetnika i DNI-a u kojem je evidentirana usklađenost s postupcima usmjeravanja i svođenja prikupljanja na najmanju moguću razinu, uključujući postupanje u skladu s pravilima kojima se osigurava prikupljanje u opravdane strane obavještajne svrhe ([2]); i godišnje izvješće čelnika subjekata obavještajne zajednice koje uključuje potvrdu da se prikupljanjem u skladu s odjeljkom 702. osiguravaju strani obavještajni podaci ([3]).

Drugim riječima, prikupljanje u skladu s odjeljkom 702. odobreno je zakonom; podliježe brojnim razinama preispitivanja, sudskog nadzora i kontrole i, kako je izjavio Sud za FISA u nedavno deklasificiranom mišljenju „nije masovno i nasumično", već „se obavlja... diskretnim odlukama o usmjeravanju na pojedinačne [komunikacijske] objekte" ([4]).

III. ZAKON SAD-a O SLOBODI

Zakonom SAD-a o slobodi koji je stupio na snagu u lipnju 2015. znatno su se izmijenile ovlasti SAD-a u pogledu nadzora i druge ovlasti povezane s nacionalnom sigurnošću i povećala se transparentnost u pogledu uporabe tih ovlasti i odluka Suda za FISA, kako je navedeno u nastavku ([5]). Zakonom se osigurava da naši obavještajni stručnjaci i stručnjaci za provedbu zakona imaju ovlasti koje su im potrebne za zaštitu zemlje, ali se istodobno osigurava primjerena zaštita pojedinaca pri izvršavanju tih ovlasti. Njime se jača privatnost i građanske slobode i povećava transparentnost.

Zakonom je zabranjeno skupno prikupljanje svih podataka, među ostalim o američkim državljanima i osobama koje nisu američki državljani, u skladu s različitim odredbama FISA-a ili na temelju dopisa o nacionalnoj sigurnost, oblika zakonom propisanih administrativnih naloga ([6]). Ova zabrana posebno uključuje telefonske metapodatke koji se odnose na pozive između osoba u SAD-u i osoba izvan SAD-a i uključivala bi i prikupljanje podataka u okviru sustava zaštite privatnosti u skladu s tim ovlastima. Zakonom je propisano da mora temeljiti svaki zahtjev za evidenciju na temelju tih ovlasti na „posebnoj razlikovnoj značajki" kojom se posebno određuje osoba, račun, adresa ili osobni uređaj na način kojim se ograničava opseg traženih informacija u najvećoj mogućoj mjeri ([7]). Time se dodatno osigurava da je prikupljanje podataka u obavještajne svrhe posebno usredotočeno i usmjereno.

Zakonom su također izvršene znatne izmjene postupaka pred Sudom za FISA, kojima se povećava transparentnost i osiguravaju dodatna jamstva da će biti zaštićena privatnost. Kako je prethodno navedeno, njime je ovlašteno stvaranje stalnog odbora provjerenih odvjetnika koji su stručni za pitanja privatnosti i građanskih sloboda, prikupljanje obavještajnih podataka, komunikacijsku tehnologiju ili ostala relevantna područja, a koji mogu biti imenovani kao *amicus curiae* u slučajevima koji uključuju znatna ili nova tumačenja zakona. Ti odvjetnici ovlašteni su davati pravne argumente kojima se potiče zaštita privatnosti i građanskih sloboda osoba i imat će pristup svim informacijama, uključujući povjerljive informacije, za koje je sud odredio da su nužni za izvršavanje njihovih dužnosti ([8]).

Zakon se temelji i na transparentnosti američke vlade o obavještajnim aktivnostima, koja je bez presedana, u skladu s kojom se traži od DNI-ja da, u dogovoru s Glavnim državnim odvjetnikom, deklasicifira ili objavi neklasificirani sažetak svake odluke, naloga ili mišljenja Suda FISA-e ili Suda za nadzor stranih obavještajnih aktivnosti, što uključuje znatno oblikovanje ili tumačenje bilo koje odredbe zakona.

([1]) *Vidjeti* 50 U.S.C. članak 1881.f.
([2]) *Vidjeti id*. članak 1881.a točka I. podtočka 1.
([3]) *Vidjeti id*. članak 1881.a točka I. podtočka 3. Neka od tih izvješća klasificirana su
([4]) Mem. Mišljenje i nalog na 26 (FISC 2014), *dostupno na* http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) *Vidjeti* Zakon SAD-a o slobodi iz 2015., Pub. L. br. 114. – 23., članak 401., 129 Stat. 268.
([6]) *Vidjeti id*. članak 103., 201., 501. Dopisi o nacionalnoj sigurnosti odobreni su nizom zakona i njima se omogućuje FBI-ju da prikupi podatke iz izvješća o kreditnoj sposobnosti, financijske evidencije i elektroničke pretplatničke i transakcijske evidencije određenih vrsta poduzeća u cilju zaštite od međunarodnog terorizma ili trajnih obavještajnih aktivnosti. *Vidjeti* 12 U.S.C.,članak 3414.; 15 U.S.C., članak 1681.u – 1681v; 18 U.S.C. članak 2709. Dopise o nacionalnoj sigurnosti obično upotrebljava FBI za prikupljanje ključnih podataka bez sadržaja u ranim fazama borbe protiv terorizma i protuobavještajnih istraga, na primjer o identitetu pretplatnika računa koji je komunicirao s agentima terorističke skupine poput ISIL-a. Primatelji dopisa o nacionalnoj sigurnosti imaju pravo osporiti ih pred sudom. *Vidjeti* 18 U.S.C., članak 3511.
([7]) *Vidjeti id*.
([8]) *Vidjeti id*. članak 401.

Nadalje, u Zakonu je predviđeno opsežno otkrivanje podataka o prikupljanju ISA-e i o zahtjevima iz dopisa o nacionalnoj sigurnosti. Sjedinjene Američke Države moraju svake godine otkriti Kongresu i javnosti broj naloga FISA-e i traženih i dobivenih certifikacija; procjene broja američkih državljana i osoba koje nisu američki državljani na koje je nadzor bio usmjeren i koji su pogođeni nadzorom; i broj imenovanih *amici curiae*, te ostale informacije ([1]). Zakonom se zahtijeva dodatno javno izvješćivanje vlada o broju zahtjeva za dopis o nacionalnoj sigurnosti u odnosu na američke državljane i osobe koje nisu američki državljani ([2]).

U pogledu korporativne transparentnosti, zakonom se poduzećima pružaju različite mogućnosti za javno izvješćivanje o ukupnom broju naloga FISA-e i ukaza ili o dopisima za nacionalnu sigurnost koje su zaprimili od vlade te o broju potrošačkih računa na koje su ti nalozi usmjereni ([3]). Nekoliko poduzeća već je tako objavilo podatke o broju potrošača čiji su podaci traženi.

Iz tih je korporativnih izvješća o transparentnosti razvidno da se američki zahtjevi za pružanjem obavještajnih podataka odnose samo na vrlo mali dio podataka. Na primjer, iz izvješća o transparentnosti jednog velikog poduzeća razvidno je da je ono zaprimilo zahtjeve povezane s nacionalnom sigurnošću (u skladu s FISA-om ili dopisima o nacionalnoj sigurnosti) za manje od 20 000 njihovih računa, u trenutku kada je imalo najmanje 400 milijuna pretplatnika. Drugim riječima, svi zahtjevi povezani s nacionalnom sigurnošću SAD-a koje je prijavilo ovo poduzeće odnosili su se na manje od 0'005 % njegovih pretplatnika. Čak i da su se svi ti zahtjevi odnosili na podatke iz „sigurne luke", što naravno nije slučaj, očito je da su zahtjevi usmjereni i primjerenog opsega te da se podaci ne prikupljaju masovno ili nasumično.

Naposljetku, iako su zakonima kojim se odobrava uporaba dopisa o nacionalnoj sigurnosti već ograničene okolnosti pod kojima bi se primatelju takvog dopisa moglo zabraniti njegovo otkrivanje, u zakonu je dalje predviđeno da se takvi zahtjevi povezani s neotkrivanjem moraju povremeno preispitivati; da primatelji dopisa o nacionalnoj sigurnosti moraju biti obaviješteni kada činjenice više nisu u skladu sa zahtjevom o neotkrivanju te da moraju biti ozakonjeni postupci kojima primatelji mogu osporiti zahtjeve povezane s neotkrivanjem ([4]).

Ukratko, važne izmjene vlasti obavještajnih službi SAD-a uvedene Zakonom SAD-a o slobodi jasan su dokaz o opsežnim naporima koje su Sjedinjene Američke Države kako bi zaštitu osobnih podataka, privatnosti, građanskih sloboda i transparentnosti učinile najvažnijim čimbenicima u svim obavještajnim aktivnostima SAD-a.

IV. TRANSPARENTNOST

Osim transparentnosti propisane Zakonom SAD-a o slobodi, američka obavještajna zajednica stavlja na raspolaganje javnosti mnogo dodatnih informacija tako dajući važan uvođenjem transparentnosti u svoje obavještajne aktivnosti. Obavještajna zajednica objavila je mnoge politike, postupke, odluke Suda za nadzor stranih obavještajnih aktivnosti i druge deklasificirane materijale osiguravajući izniman stupanj transparentnosti. Nadalje, obavještajna zajednica objavljuje znatno više statističkih podataka o mjeri u kojoj se vlada ovlastima za prikupljanje podatka za potrebe sigurnosti. Obavještajna zajednica izdala je 22. travnja 2015. svoje drugo godišnje izvješće u kojem je navela statističke podatke o tome koliko često vlada upotrebljava te važne ovlasti. ODNI je također objavio, na *web*-mjestu ODNI-ja i na *web*-mjestu *IC On the Record* skup konkretnih načela transparentnosti ([5]) i plan provedbe kojim se načela pretvaraju u konkretne, mjerljive inicijative ([6]). Direktor Nacionalne obavještajne službe objavio je u listopadu 2015. da svaka obavještajna agencija može među svojim rukovodećim djelatnicima odrediti službenika za transparentnost obavještajnih aktivnosti koji će poticati transparentnosti i provoditi inicijative za povećanje transparentnosti ([7]). Službenik za transparentnost blisko će surađivati sa službenikom za zaštitu privatnosti i građanske slobode svake obavještajne agencije kako bi osigurao da su transparentnost, privatnost i građanske slobode glavni prioriteti.

([1]) *Vidjeti id*. članak 602.
([2]) *Vidjeti id*.
([3]) *Vidjeti id*. članak 603.
([4]) *Vidjeti id*. članak 502.(f) 503.
([5]) *Dostupno na* http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) *Dostupno na* http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) *Vidjeti id*.

Kao primjer tih napora, Glavni dužnosnik NSA za zaštitu privatnosti i građanske slobode objavio je posljednjih nekoliko godina nekoliko deklasificiranih izvješća o aktivnostima u skladu s odjeljkom 702., Izvršnim nalogom 12333. i Zakonom SAD-a o slobodi ([1]). Nadalje, obavještajna zajednica blisko surađuje s PCLOB-om, Kongresom i američkom zajednicom za poticanje zaštite privatnosti u cilju osiguravanja daljnje transparentnosti o američkim obavještajnim aktivnostima, kada je to izvedivo i u skladu sa zaštitom izvora i metoda prikupljanja osjetljivih obavještajnih podataka. Obavještajne aktivnosti SAD-a u u cjelini jednako su transparentne, ako ne i više, od aktivnosti bilo koje druge države u svijetu i onoliko koliko je moguće da bi mogle biti u skladu s potrebom za zaštitom osjetljivih izvora i metoda.

Opsežna transparentnost u pogledu američkih obavještajnih aktivnosti može se sažeti kako slijedi:

— Obavještajna zajednica objavila je na internetu tisuće stranica sudskih mišljenja i postupaka agencija u kojima su opisani posebni postupci i zahtjevi u pogledu naših obavještajnih aktivnosti. Također smo objavili izvješća o usklađenosti obavještajnih agencija s primjenjivim ograničenjima.

— Viši dužnosnici obavještajne zajednice redovito javno govore o ulogama i aktivnostima svojih organizacija, među ostalim opisuju mehanizme kojima se osigurava poštovanje načela i zaštitne mjere na kojima se temelji njihov rad.

— Obavještajna zajednica objavila je brojne dodatne dokumente o obavještajnim aktivnostima u skladu sa našim Zakonom o slobodi informacija.

— Predsjednik je izdao Predsjednički ukaz br. 28. javno određujući dodatna ograničenja naših obavještajnih aktivnosti i ODNI je objavio dva javna izvješća o provedbi tih ograničenja.

— Obavještajna zajednica sada ima zakonsku obvezu objavljivati važna pravna mišljenja Suda za FISA ili sažetke tih mišljenja.

— Vlada je dužna redovito izvješćivati o mjeri u kojoj upotrebljava određene ovlasti za potrebe nacionalne sigurnosti, a poduzeća su dužna učiniti isto.

— PCLOB je objavio nekoliko detaljnih javnih izvješća o obavještajnim aktivnostima i to će nastaviti činiti.

— Obavještajna zajednica dostavlja nadzornim odborima u Kongresu opsežne klasificirane podatke.

— DNI je izdao načela transparentnosti na kojima se moraju temeljiti aktivnosti obavještajne zajednice.

Ta će se transparentnost nastaviti u budućnosti. Sve javno objavljene informacije bit će, naravno, dostupne Ministarstvu trgovine i Europskoj komisiji. U okviru godišnjeg preispitivanja provedbesustava zaštite privatnosti koje će obavljati Ministarstvo trgovine i Europska komisija osigurat će se Europskoj komisiji prilike za razgovor o pitanjima koja se javljaju zbog objavljenih informacija te o drugim pitanjima povezanima sa sustavom za zaštitu privatnosti i njegovim radom i shvaćamo da Ministarstvo može, po vlastitom nahođenju, pozvati predstavnike drugih agencija, među ostalim iz obavještajne zajednice, da sudjeluju u tom preispitivanju. To je naravno dodatno uz mehanizam predviđen Predsjedničkim ukazom br. 28. za države članice EU-a koji one mogu upotrijebiti da se obrate službeniku Ministarstva vanjskih poslova s dodatnim pitanjima povezanim as nadzorom.

V. PRAVNA ZAŠTITA

U američkom zakonodavstvu predviđen je niz mogućnosti pravne zaštite osoba koje su bile podvrgnute nezakonitom nadzoru elektroničkih komunikacija za potrebe nacionalne sigurnosti. U skladu s FISA-om, pravo traženja pravne zaštite na sudu SAD-a nije ograničeno na američke državljane. Osoba koja ima osnovu za podnošenje tužbe imala bi na

([1]) *Distupno na:* 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.

raspolaganju pravne lijekove za osporavanje nezakonitog nadzora elektroničkih komunikacija u skladu s FISA-om. Na primjer, FISA-om se dopušta osobama koje su podvrgnute nezakonitom elektroničkom nadzoru da osobno tuže američke državne službenike tražeći novčanu odštetu, uključujući novčanu odštetu i pokrivanje sudskih troškova. *Vidjeti* 50 U.S.C., članak 1810. Osobe koje mogu dokazati osnovanost tužbe mogu pokrenuti i parnicu za traženje novčane odštete, među ostalim za pokrivanje sudskih troškova, protiv Sjedinjenih Američkih Država kada su se podaci o njima prikupljeni elektroničkim izviđanjem u skladu s FISA nezakonito i voljno upotrijebljeni ili otkriveni. *Vidjeti* 18 U.S.C., članak 2712. Ako vlada planira upotrijebiti ili otkriti podatke prikupljene nadzorom elektroničkih komunikacija bile koje osobe kojoj je nanesena šteta u skladu s FISA-om protiv te osobe u sudskom ili upravnom postupku u Sjedinjenim Američkim Državama, ona mora unaprijed najaviti svoju namjeru sudu i toj osobi, koja može osporiti zakonitost nadzora i tražiti obustavu objave informacija. *Vidjeti* 50 U.S.C., članak 1806. Naposljetku, FISA-om se osiguravaju i kaznene sankcije protiv osoba koje namjerno obavljaju nezakoniti nadzor elektroničkih komunikacijskih sustava ili koje namjerno otkrivaju ili upotrebljavaju podatke prikupljene nezakonitim nadzorom. *Vidjeti* 50 U.S.C., članak 1809.

Američki državljani imaju na raspolaganju i druge načine za traženje pravne zaštite protiv američkih državnih službenika zbog nezakonite uporabe tih podataka ili pristupa tim podacima, među ostalim protiv državnih službenika koji su prekršili zakon nezakonitim pristupom podacima ili njihovom nezakonitom uporabom u predviđene svrhe zaštite nacionalne sigurnosti. Zakonom o računalnoj prijevari i zlouporabi zabranjuje se namjerni neovlašteni pristup (ili prekoračenje ovlaštenog pristupa) u cilju prikupljanja podataka od financijske ustanove, računalnog sustava američke vlade ili računala kojem se pristupa internetom te prijetnje nanošenjem štete zaštićenm računalima za potrebe iznude ili prijevare. *Vidjeti* 18 U.S.C., članak 1030. Svaka osoba, bez obzira na državljanstvo, koja je pretrpjela gubitak ili štetu zbog povrede ovog zakona može tužiti počinitelja (među ostalim državnog službenika) za naknadu štete i drugu privremenu ili drugu jednakovrijednu naknadu u skladu s odjeljkom 1030. točkom (g), neovisno o tome je li pokrenut kazneni postupak, ako postupanje uključuje najmanje jednu od nekoliko okolnosti navedenih u zakonu. Zakonom o privatnosti u području elektroničke komunikacije (ECPA) uređuje se pristup vlade pohranjenim elektroničkim komunikacijama i evidenciji o transakcijama te podacima o pretplatnicima koje čuvaju pružatelji komunikacijskih usluga treće stranke. Vidjeti 18 U.S.C., članak 2701. – 2712. ECPA-om se oštećene osobe ovlašćuju da tuže državne službenike zbog namjernog nezakonitog pristupa pohranjenim podacima. ECPA se primjenjuje na sve osobe bez obzira na njihovo državljanstvo i oštećene osobe mogu dobiti odštetu i plaćene sudske troškove. Zakonom o pravu na privatnost financijskih podataka (EFPA) ograničava se pristup američke vlade bankarskoj i brokerskoj evidenciji o pojedinim klijentima. Vidjeti 12 U.S.C., članci 3401. – 3422. U skladu s RFPA-om, klijent banke ili brokera može tužiti američku vladu tražeći zakonsku, stvarnu i kaznenu odštetu zbog nezakonitog pristupa evidenciji o klijentima i ako se tvrdi da je takav nezakoniti pristup bio voljan automatski se pokreće istraga i moguće stegovne mjere protiv predmetnih državnih službenika. Vidjeti 12 U.S.C., članak 3417.

Naposljetku, Zakonom o pravu na pristup informacijama (FOIA) osobama se osigurava sredstvo za traženje pristupa evidenciji postojeće savezne agencije o bilo kojoj temi podložno određenim kategorijama iznimki. Vidjeti 5 U.S.C., članak 552.(b). One uključuju ograničenja pristupa klasificiranim podacima povezanima s nacionalnom sigurnošću, osobnim podacima trećih osoba i podacima o istragama tijela za provedbu zakona i mogu se usporediti s ograničenjima koja je odredila svaka država vlastitim zakonom o pristupu podacima. Ta se ograničenja jednako primjenjuju na američke državljane i osobe koje nisu američki državljani. Protiv odluka u sporovima o puštanju evidencije zatraženom u skladu s FOIA-om moguće je podnijeti upravu žalbu ili žalbu saveznom sudu. Sud je dužan ponovno utvrditi je li neotkrivanje podataka u skladu sa zakonom, 5. U.S.C. članak 552. točka (a) podtočka 4. (B) i može obvezati vladu da osigura pristup evidenciji. U nekim slučajevima sudovi su odbacili tvrdnje vlade da se podaci ne bi trebali otkriti jer su povjerljivi ([1]). Iako nije moguće tražiti naknadu novčane štete, sudovi mogu dodijeliti nadoknadu odvjetničkih troškova.

VI. ZAKLJUČAK

Sjedinjene Američke Države potvrđuju da se našim aktivnostima prikupljanja obavještajnih podataka praćenjem signala elektroničkih sustava i ostalim obavještajnim aktivnostima mora uzeti u obzir da se prema svim osobama treba postupati s dostojanstvom i poštovanjem, neovisno o njihovom državljanstvu ili boravištu, i da sve osobe imaju legitimne interese zaštite privatnosti pri obradi njihovih osobnih podataka. Sjedinjene Američke Države upotrebljavaju prikupljanje obavještajnih podataka praćenjem signala elektroničkih sustava za jačanje svoje nacionalne sigurnosti i interesa vanjske politike te da zaštite svoje građane i građane svojih saveznika i partnera. Ukratko, obavještajna zajednica ne obavlja nasumični nadzor svih osoba, među ostalim običnih europskih građana. Prikupljanje obavještajnih podataka praćenjem signala elektroničkih sustava odvija se samo kada je odobreno i na način koji je strogo u skladu s

([1]) *Vidjeti, na primjer New York Times protiv Department of Justice*, 756 F.3d 100 (2d Cir. 2014.); Vidjeti *American Civil Liberties Union protiv CIA*, 710 F.3d 422 (D.C. Cir. 2014.).

tim ograničenjima; tek nakon razmatranja raspoloživosti alternativnih izvora, među ostalim diplomatskih i javnih izvora i na način kojim se daje prednost odgovarajućim i izvedivim alternativama. Kad god je to izvedivo, prikupljanjae obavještajnih podataka praćenjem signala elektroničkih sustava usmjereno je na određene ciljeve ili teme stranih obavještajnih aktivnosti primjenom razlikovnih čimbenika.

Politika SAD-a u tom području potvrđena je u Predsjedničkom ukazu br. 28. Unutar tog okvira, američke obavještajne agencije nemaju zakonske ovlasti, sredstva, tehničke sposobnosti ili želju presretati sve svjetske komunikacije. Te agencije ne čitaju poruke e-pošte svih stanovnika Sjedinjenih Američkih Država ili svih osoba na svijetu. U skladu s Predsjedničkim ukazom br. 28., Sjedinjene Američke Države osiguravaju pouzdanu zaštitu osobnih podataka osoba koje nisu američki državljani koji se prikupljaju aktivnostima prikupljanja obavještajnih podataka praćenjem signala elektroničkih sustava. U mjeri u kojoj je to izvedivo i u skladu s pitanjima nacionalne sigurnosti, to uključuje politike i postupke kojima se na najmanju moguću razinu svodi zadržavanje i širenje osobnih informacija o osobama koje nisu američki državljani u odnosu na zaštite koje uživaju američki državljani. Nadalje, kako je prethodno navedeno, nigdje ne postoji sveobuhvatni sustav nadzora jednak onom koji postoji u skladu s posebnim ovlastima iz odjeljka 702. FISA-e. Naposljetku, znatnim izmjenama američkog zakona o obavještajnim aktivnostima utvrđenima u Zakon SAD-a o slobodi i inicijativama koje provodi ODNI usmjerenima na povećanje transparentnosti obavještajne zajednice znatno se povećava zaštita privatnosti i građanskih sloboda svih osoba, neovisno o njihovom državljanstvu.

S poštovanjem

Robert S. Litt

21. lipnja 2016.

G. Justin S. Antonipillai
Savjetnik
Ministarstvo trgovine SAD-a
1401 Constitution Ave., NW
Washington, DC 20230

G. Ted Dean
Zamjenik pomoćnika Tajnika
Uprava za međunarodnu trgovinu
1401 Constitution Ave., NW
Washington, DC 20230

Poštovana gospodo Antonipillai i Dean:

Pišem Vam kako bih Vam pružio informacije o načinu na koji Sjedinjene Američke Države skupno elektronički prikupljaju obavještajne podatke. Kako je objašnjeno u bilješki 5. Predsjedničkog ukaza br. 28 (PPD-28) „skupno" prikupljanje odnosi se na pribavljanje relativno velike količine elektronički prikupljenih obavještajnih informacija ili podataka u okolnostima u kojima se obavještajna zajednica ne može koristiti identifikatorom povezanim s određenom ciljanom osobom (kao što je adresa e-pošte ili telefonski broj ciljane osobe) Međutim, to ne znači da je takvo prikupljanje „masovno" ili „neselektivno". Naime, prema PPD-28-u „aktivnosti prikupljanja podataka bit će što je moguće usmjerenija". U ostvarivanju tog mandata obavještajna zajednica poduzima korake kako bi osigurala da čak i kad ne možemo koristiti posebne identifikatore za ciljano prikupljanje, podaci koje prikupljamo i dalje mogu sadržavati podatke stranih obavještajnih službi koji će odgovarati zahtjevima američkih tvoraca politike u skladu s postupkom opisanim u mom prethodnom dopisu i tako da se količina nerelevatnih informacija koje se prikupljaju svede na minimum.

Naprimjer, od obavještajne zajednice može se zatražiti da prikupi podatke elektroničkim izviđanjem o aktivnostima terorističke skupine koja djeluje u regiji zemlje na Bliskom istoku za koju se smatra da planira napade na zapadnoeuropske zemlje, ali ne zna imena, brojeve telefona, adrese e-pošte ili druge posebne identifikatore povezane s tom terorističkom skupinom. Možemo odlučiti usmjeriti se na tu skupinu prikupljanjem komunikacijskih podataka usmjerenih prema i iz te regije za daljnji pregled i analizu kako bismo utvrdili podatke koji se odnose na tu skupinu. Obavještajna zajednica tako usmjerava prikupljanje u najvećoj mogućoj mjeri. To bi se smatralo „skupnim" prikupljanjem jer se nije moguće koristiti razlikovnim čimbenicima, no nije riječ o „masovnom" ili „neselektivnom" prikupljanju. Točnije, riječ je o što je moguće usmjerenijem prikupljanju.

Stoga, čak i kad ciljano prikupljanje nije moguće putem konkretnih čimbenika za odabir, Sjedinjene Američke Države ne prikupljaju sve komunikacijske podatke preko svih uređaja za komunikaciju u cijelom svijetu, već se primjenjuju filteri i drugi tehnički alati za usmjeravanje prikupljanja prema onim uređajima koji bi mogli sadržavati komunikaciju povezanu sa stranim obavještajnim aktivnostima. Sjedinjene Američke Države u elektroničkom prikupljanju podataka tako se dotiču samo djelića komunikacija na internetu.

Štoviše, kao što sam napomenuo u prijašnjem dopisu, upravo zato što „skupno" prikupljanje nosi veći rizik od prikupljanja nerelevantnih komunikacija, u PPD-28 ograničava se uporaba skupnog elektroničkog prikupljanja podataka na šest konkretnih ciljeva. Nadalje, u PPD-28 i agencijskim politikama kojima se provodi PPD–28 ograničava se zadržavanje i širenje osobnih podataka koji su elektronički prikupljeni, neovisno o tome jesu li podaci skupno ili ciljano prikupljeni te novisno o državaljanstvu pojedinca.

Stoga „skupno" prikupljanje nije „masovno" ili „neselektivno", već uključuje primjenu metoda i alata za filtriranje prikupljanja kako bi se prikupljanje usmjerilo na materijal koji će odgovarati jasnim stranim obavještajnim zahtjevima tvoraca politika a pritom smanjilo prikupljanje nerelevantnih podataka. Nadalje, ono pruža stroga pravila za zaštitu

nerelebantnih podataka koji se mogu prikupiti. Politike i postupci koji se navodu u ovom dopisu primjenjuju se na svo skupno elektroničko prikupljanje, uključujući sve skupno elektronički prikupljene komunikacije usmjerene prema Europi i iz nje. Pritom se ne potvrđuje postoji li takvo skupno prikupljanje podataka.

Zatražili ste dodatne informacije o Odboru za nadzor privatnosti i građanskih sloboda (PCLOB) i glavnim inspektorima te njihovim nadležnim tijelima. PCLOB neovisna je agencija u izvršnom sektoru vlasti. Pet članova dvostranačkog odbora imenuje predsjednik, a potvrđuje Senat ([1]). Svakom članu odbora mandat traje šest godina. Članovi odbora i osoblje prolaze primjerenu sigurnosnu provjeru kako bi u potpunosti izvršavali svoje zakonske dužnosti i odgovornosti ([2]).

Cilj PCLOB-a je osigurati da su nastojanja federlane vlade da suzbiju terorizam u skladu sa zaštitom privatnosti i građanskih sloboda. Odbor ima dvije temeljne odgovornosti, nadzor i savjetovanje. PCLOB određuje vlastiti radni raspored te koje aktivnosti savjetovanja i nadzora želi poduzeti.

U ulozi *nadzornika* PCLOB preispituje i analizira mjere koje izvršna vlast poduzima kako bi zaštitila naciju od terorizma, pod uvjetom da je potreba za tim mjerama u skladu s potrebom za zaštitom privatnosti i građanskih sloboda ([3]). U posljednjem PCLOB-ovu pregledu nadzora naglasak je na programima nadzora koji se provode u okviru odjeljka 702. FISA-e ([4]). Trenutačno provodi preispitivanje obavještajnih aktivnosti u okviru Izvršnog naloga 12333. ([5]).

U *savjetodavnoj* ulozi PCLOB osigurava da se primjereno vodi računa o slobodama u razvoju i provedbi zakona, propisa i politika povezanih s nastojanjima za zaštitu države od terorizma ([6]).

Kako bi ispunio svoju zadaću, odboru je zakonski odobren pristup svim relevantnim evidencijama agencija, izvješćima, pregledima, revizijama, dokumentima, preporukama i drugim relevantnim materijalima, uključujući klasificirane podatke u skladu sa zakonima ([7]). Osim toga, odbor može voditi intervjue, uzimati izjave i saslušati svjedočanja bilo kojeg službenika ili zaposlenika izvršne vlasti ([8]). Osim toga, odbor može pismeno zatražiti da glavni državni odvjetnik u ime odbora izda naloga u kojima strankama izvan izvršne vlasti može naložiti da pruže relevantne informacije ([9]).

Konačno, PCLOB ima zakonsku obvezu javne transparentnosti. To uključuje informiranje javnosti o aktivnostima odbora putem javnih saslušanja i objavom izvješća, u najvećoj mogućoj mjeri i u skladu sa zaštitom povjerljivih podataka ([10]). Osim toga, PCLOB treba izdati izvješće ako agencija izvršne vlasti ne postupi po naputku odbora.

Glavni inspektori u obavještajnoj zajednici provode revizije, inspekcije i preispitivanja programa i aktivnosti u obavještajnoj zajednici kako bi utvrdili i riješili sustavne rizike, ranjivosti i nedostatke. Glavni inspektori provode i istrage o pritužbama te o informacija o navodnim kršenjima zakona, propisa ili o lošem upravljanju, o velikoj pronevjeri

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) *Vidjeti za opće informacije:* https://www.pclob.gov/library.html#oversightreports.
([5]) *Vidjeti za opće informacije:* https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); *vidjeti PCLOB Advisory Function Policy and Procedure, Policy 2015-004, dostupno na:* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

sredstava, zlouporabi nadležnosti ili znatne i konkretne opasnosti za javno zdravlje i sigurnost u programima i aktivnostima obavještajne zajednice. Neovisnost glavnih inspektora nužna je za objektivnost i integritet svakog njihovog izvješća, nalaza i preporuke. Neki od glavnih elemenata za status neovisnosti glavnih inspektora odnose se na njihovo imenovanje i razrješenje, odvojena tijela za proračun, operativno djelovanje i odabir osoblja te dvostruke obveze izvješćivanja agenciji izvršne vlasti i Kongresu.

Kongres je uspostaviti neovisni ured glavnih inspektora u svakoj agenciji izvršne vlasti, uključujući svaki element obavještajne zajednice ([1]). S donošenjem Zakona o odobrenju prikupljanja obavještajnih podataka za fiskalnu godinu 2015. gotovo sve glavne inspektore koji imaju nadzor nad elementima obavještajne zajednice imenuje predsjednik i potvrđuje Senat, uključujući Ministarstvo pravosuđa, Središnju obavještajnu agenciju (CIA), Nacionalnu sigurnosnu agenciju (NSA) te obavještajnu zajednicu ([2]). Nadalje, ti su glavni inspektori stalni nestranački dužnosnici koje može razriješiti samo predsjednik. Iako prema Ustavu SAD-a predsjednik ima ovlast razriješiti glavne inspektore dužnosti, ta se ovlast rijetko provodila u praksi, a predsjednik mora Kongresu pružiti razlog u pisanom obliku u roku od mjeseca dana prije razrješenja glavnog inspektora ([3]). Takav postupak imenovanja glavnog inspektora omogućuje da nema neprimjerenog utjecaja službenika izvršne vlasti na odabir, imenovanje ili razrješenje glavnog inspektora.

Drugo, glavni inspektori imaju znatne zakonske nadležnosti za provođenje reviizija, istraga i preispitivanja programa i operativnih djelatnosti izvršne vlasti. Osim nadzora i preispitivanja propisanih zakonom, glavni inspektori imaju široko diskrecijsko pravo za provođenje nadzora za preispitivanje programa i aktivnosti koje su odabrali ([4]). Prilikom izvršenja nadležnosti, prema zakonu glavni inspektori imaju neovisne resurse za provođenje svojih odgovornosti, uključujući nadležnost da zapošljavaju osoblje i zasebno šalju svoje zahtjeve za proračun Kongresu ([5]). Zakon osigurava da glavni inspektori imaju pristup informacijama koje su im potrebne za izvršavanje svojih zadaća. To uključuje nadležnost za izravni pristup svim evidencijama agencija i podacima o programima i operativnim djelatnostima agencija neovisno o klasifikaciji, nadležnost da sudskim putem zatraže podatke i dokumente i nadležnost zaprisezanja ([6]). U ograničenom broju slučajeva agencija izvršne vlasti može zabraniti rad glavnom inspektoru ako, naprimjer, revizija ili istraga koju provodi može znatno ugroziti nacionalne sigurnosne interese Sjedinjenih Američkih Država. No takva provedba nadležnosti je iznimno rijetka, a voditelj agencije treba o razlozima obavijestiti Kongres u roku od 30 dana ([7]). Direktor nacionalne obavještajne službe dosad se nije pozvao na tu nadležnost nad radom glavnih inspektora.

Treće, glavni inspektori imaju obvezu potpunog i pravovremenog izvješćivanja oba voditelja agencija izvršne vlasti o prijevarama i drugim ozbiljnim problemima, zlouparabama te nedostatcima povezanim s programima i djelatnostima izvršne vlasti ([8]). Dvostruko izvješćivanje jača neovisnost glavnih inspektora, osigurava transparentnost te omogućuje voditeljima agencija da provedu preporuke glavnih inspektora prije no što Kongres može poduzeti zakonodavne mjere. Naprimjer, prema zakonu glavni inspektori moraju dovršiti polugodišnja izvješća u kojima se navode ti problemi te korektivne mjere koje su u međuvremenu poduzete ([9]). Agencije izvršne vlasti ozbiljno razmatraju zaključke i preporuke glavnih inspektora. U svoja izvješća i preporuke koja se šalju Kongresu, a u nekim slučajevima i javnosti, glavni

([1]) Odjeljci 2 i 4 Zakona o glavnim inspektorima (1978.), kako je izmijenjen (dalje u tekstu, „IG Act"); Odjeljak 103H(b) i (e) Zakon o nacionalnoj sigurnosti iz 1947., kako je izmijenjen (dalje u tekstu„„Nat'l Sec. Act"); Odjeljak 17(a) Zakona o središnjoj obavještajnoj agenciji (dalje u tekstu, „CIA Act").

([2]) *Vidjeti* Pub. L. br. 113-293, 128 Stat. 3990, (19. prosinca 2014.). Predsjednik ne imenuje samo glavne inspektore za Obrambenu obavještajnu agenciju i Nacionalnu geoprostornu obavještajnu agenciju. Međutim, glavni inspektor za Ministarstvo obrane i glavni inspektor za obavještajnu zajednicu imaju alternativnu nadležnost nad tim agencijama.

([3]) Odjeljak 3. IG Act-a iz 1978., kako je izmijenjen; Odjeljak 103H(c) Nat'l Sec. Act-a i odjeljak 17(b) CIA Act-a

([4]) *Vidjeti* Odjeljci 4(a) i 6(a)(2) IG Act-a iz 1947.; Odjeljak 103H(e) i (g)(2)(A) Nat'l Sec. Act-a; Odjeljak 17(a) i (c) CIA Act-a.

([5]) Odjeljci 3(d), 6(a)(7) i 6(f) IG Act-a. Odjeljci 103H(d), i., (j) i (m) Nat'l Sec. Act-a. Odjeljci 17(e)(7) i (f) CIA Act-a.

([6]) Odjeljak 6(a)(1), (3), (4), (5) i (6) IG Act-a. Odjeljci 103H(g)(2) Nat'l Sec. Act-a. Odjeljak 17(e)(1), (2), (4) i (5) CIA Act-a.

([7]) *Vidjeti, npr.* Odjeljci 8(b) i 8E(a) IG Act-a; Odjeljak 103H(f) Nat'l Sec. Act-a. Odjeljak 17(b) CIA Act-a.

([8]) Odjeljak 4(a)(5) IG Act-a. Odjeljak 103H(a)(b)(3) i (4) Nat'l Sec. Act-a. Odjeljak 17(a)(2) i (4) CIA Act-a.

([9]) Odjeljak 2(3), 4(a), i 5. IG Act-a. Odjeljak 103H(k) Nat'l Sec. Act-a. Odjeljak 17(d) CIA Act-a. Glavni inspektor Ministarstva pravosuđa javno objavljuje izvješća, dostupna na sljedećoj adresi: http://oig.justice.gov/reports/all.htm. Slično tome, glavni inspektor za obavještajnu zajednicu objavljuje polugodišnja izvješća na sljedećoj adresi: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

inspektori često mogu uključiti provedbu preporuka koje su sami izdali ([1]). Osim tog sustava dvostrukog izvješćivanja, glavni su inspektori odgovorni i za pratnju zviždača u okviru izvršne vlasti pred odgovarajuće nadzorne odbore Kongresa. Tim odborima zviždači otkrivaju slučajeve navodnih prijevara, pronevjere sredstava ili zlouporabe moći u okviru djelatnosti i programa izvršne vlasti. Zviždačima koji izađu u javnost s informacijama jamči se da im identitet neće biti otkriven izvršnoj vlasti što ih štiti od mogućih zabranjenih stegovnih mjera ili sigurnosne provjere koje bi se mogle poduzeti jer su izvijestili glavne inspektore ([2]). Budući da su zviždači izvor informacija za istrage glavnih inspektora, mogućnost da se o njihovim zabrinutostima izvijesti Kongres bez utjecaja izvršne vlasti povećava učinkovitost nadzora glavnih inspektora. Zbog tog statusa neovisnosti, glavni inspektori mogu promicati štednju, učinkovitost i odgovornost u agencijama izvršne vlasti na objektivan i moralan način.

Konačno, Kongres je uspostavio Vijeće glavnih inspektora o integritetu i učinkovitosti. Među ostalim, Vijeće razvija norme glavnih inspektora za revizije, istrage i preispitivanja, promiče osposobljavanje te ima nadležnost voditi preispitivanja za optužbe o prekršajima glavnih inspektora. Tako ima kritički nadzor nad glavnim inspektorima koji imaju nadležnost nadgledati rad ostalih službi ([3]).

Nadam se da će Vam ova informacija biti od koristi.

Srdačan pozdrav
Robert S. Litt
Glavni savjetnik

([1]) Odjeljak 2(3), 4(a), i 5. IG Act-a. Odjeljak 103H(k) Nat'l Sec. Act-a. Odjeljak 17(d) CIA Act-a. Glavni inspektor Ministarstva pravosuđa javno objavljuje izvješća, dostupna na sljedećoj adresi: http://oig.justice.gov/reports/all.htm. Similarly, the Inspector General for the Intelligence Community makes it semi-annual reports publicly available at https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Odjeljak 7. IG Act-a. Odjeljak103H(g)(3) Nat'l Sec. Act-a. Odjeljak 17(e)(3) CIA Act-a.

([3]) Odjeljak 11. IG Act-a.

PRILOG VII.

Dopis zamjenika pomoćnika Glavnog državnog odvjetnika i savjetnika za međunarodna pitanja, g. Brucea Swartza, Ministarstvo pravosuđa SAD-a

19. veljače 2016.

G. Justin S. Antonipillai
Savjetnik
Ministarstvo trgovine SAD-a
1401 Constitution Ave., NW
Washington, DC 20230

G. Ted Dean
Zamjenik pomoćnika tajnika
Uprava za međunarodnu trgovinu
1401 Constitution Ave., NW
Washington, DC 20230

Poštovana gospodo Antonipillai i Dean:

U ovom dopisu prikazan je kratak pregled glavnih istražnih alata koji se upotrebljavaju za prikupljanje tržišnih podataka i ostalih podataka iz evidencije korporacija u Sjedinjenim Američkim Državama za potrebe provedbe kaznenog prava ili za potrebe javnog interesa (građanske i regulatorne), među ostalim ograničenja pristupa utvrđena u tim ovlastima ([1]). Ti su pravni postupci nediskriminacijski jer se upotrebljavaju za prikupljanje podataka od korporacija u Sjedinjenim Američkim Državama, među ostalim od poduzeća koja će obaviti samostalno certificiranje u okviru europsko-američkog sustava zaštite privatnosti, bez obzira na državljanstvo osobe čiji se podaci obrađuju. Nadalje, protiv kojih je pokrenut sudski postupak u Sjedinjenim Američkim Državama mogu ga osporiti pred sudom ([2]).

U pogledu zapljene podataka koje obavljaju javna tijela posebno treba spomenuti četvrti amandman Ustava Sjedinjenih Američkih Država u kojem je predviđeno „ne smije se kršiti pravo osoba da se osjećaju sigurno te da su njihove kuće, dokumenti i imovina zaštićeni od nerazumnih pretresa i zapljena i nalozi se ne smiju izdavati osim ako postoji opravdana sumnja potkrijepljena zakletvom ili potvrdom i u njima mora biti posebno opisano mjesto koje će se pretraživati i osobe ili stvari koje će se oduzeti." Amandman Ustava SAD-a IV. Vrhovni sud Sjedinjenih Američkih Država izjavio je u predmetu *Berger protiv države New York* da je „osnovna svrha ovog amandmana, potvrđena u brojnim odlukama Suda, zaštititi privatnosti i sigurnost osoba od arbitrarnih neovlaštenih narušavanja privatnosti od strane državnih službenika." 388 U.S. 41, 53 (1967.) (*citing Camara protiv Mun. Sud u San Franciscu*, 387 U.S. 523, 528 (1967.)). Četvrtim amandmanom zahtijeva se da u domaćim kaznenim istragama službenici za provedbu zakona dobiju sudski nalog za pretragu. *Vidjeti Katz protiv Sjedinjenih Američkih Država*, 389 U.S. 347, 357 (1967.). Ako se ne primjenjuje zahtjev posjedovanja sudskog naloga, aktivnosti vlade podliježu testu „razumnosti" u skladu s četvrtim amandmanom. Stoga se samim Ustavom osigurava da američka vlada nema neograničene, ili arbitrarne, ovlasti zapljene osobnih podataka.

Tijela za provedbu kaznenog zakona:

Savezni tužitelji, koji su zaposlenici Ministarstva pravosuđa (DOJ) i savezni agenti, uključujući agente Saveznog istražnog ureda (FBI), agencije za provedbu zakona u okviru Ministarstva pravosuđa, mogu zahtijevati od korporacija u Sjedinjenim Američkim Državama da dostave dokumente i ostale podatke iz evidencije za potrebe kaznene istrage s

([1]) U ovom pregledu nisu opisani istražni alati za potrebe nacionalne sigurnosti koje upotrebljavaju tijela za provedbu zakona u slučaju istraga terorizma i drugih istraga povezanih s nacionalnom sigurnošću, među ostalim dopisi o nacionalnoj sigurnosti (NSL) za određene informacije iz izvješća o kreditnom stanju, financijske evidencije i elektroničke evidencije o pretplatnicima i transakcijama, *vidjeti* 12 U.S. C., članak 3414.; 15 U.S.C., članak 1681.u; 15 U.S.C., članak 1681.v; 18 U.S.C. članak 2709., i za elektronički nadzor, naloge za pretragu, poslovnu evidenciju i ostale načine prikupljanja komunikacija u skladu sa Zakonom o nadzoru stranih obavještajnih službi, *vidjeti* 50 U.S.C., članak 1801.*i dalje*.

([2]) U ovom dokumentu razmatraju se savezna tijela za provedbu zakona i regulatorna tijela; povrede državnih zakona istražuju države i rješavaju na državnim sudovima. Državna tijela za provedbu zakona upotrebljavaju jamstva i sudske pozive u skladu s državnim zakonima na prethodno opisani način, ali postoji mogućnost da državni sudski postupci podliježu zaštitnim mjerama koje osiguravaju državni ustavi koje prekoračuju ovlasti iz američkog Ustava. Zaštita u skladu s državnim zakonom mora biti barem jednaka zaštiti koju osigurava američki Ustav, uključujući, ali ne samo, četvrti amandman.

pomoću nekoliko vrsta obveznih zakonskih mjera, među ostalim na temelju poziva velike porote, administrativnih poziva i naloga za pretragu te mogu tražiti druge podatke o komunikacijama u skladu sa saveznim tijelima nadležnim za prikupljanje podataka prislušnim uređajima.

Pozivi velike porote ili sudski pozivi: Kazneni sudski pozivi upotrebljavaju se kao pomoć u ciljanim kaznenim istragama. Poziv velike porote službeni je zahtjev koji izdaje porota (obično na zahtjev saveznog tužitelja) kao pomoć u istrazi koju provodi porota zbog sumnje na povredu kaznenog prava. Velike porote istražni su dio suda koje sastavlja sudac. Sudskim pozivom može se zahtijevati od osobe da bude svjedok u postupku ili da dostavi dostupnu poslovnu evidenciju, elektronički pohranjene podatke, ili druge opipljive dokumente. Podaci moraju biti relevantni za istragu i poziv ne smije biti nerazuman jer je pretjeran ili zato što je opterećujući. Primatelj može upotrijebiti te osnove za osporavanje sudskog poziva. *Vidjeti* Fed. R. Crim. str. 17. U ograničenim okolnostima sudski pozivi za dostavu dokumenata mogu se upotrebljavati kada velika porota izda optužnicu.

Ovlast izdavanja upravnog naloga: Ovlasti izdavanja upravnog naloga mogu se ostvarivati u kaznenim ili građanskim istragama. U kontekstu provedbe kaznenog zakona, s nekoliko saveznih zakona ovlašćuje se uporaba administrativnih poziva za dostavljanje ili objavu poslovne evidencije, elektronički pohranjenih podataka ili drugih opipljivih predmeta u istragama povezanima sa prijevarom u području zdravstvene skrbi, zaštitom tajne službe, slučajevima povezanima s kontroliranim tvarima i istragama glavnog inspektora protiv državnih agencija. Ako vlada želi primijeniti administrativne pozive na sudu, primatelj administrativnog poziva, kao i primatelj poziva velike porote, može tvrditi da je poziv nerazuman jer je pretjeran ili jer je opresivan ili opterećujući.

Sudski nalozi za prikupljanje podataka prislušnim uređajima: U skladu s odredbama o prikupljanju podataka prislušnim uređajima, tijela za provedbu zakona mogu dobiti sudski nalog za prikupljanje podataka o biranim brojevima, usmjeravanju, adresiranju i signaliziranju bez sadržaja u stvarnom vremenu o telefonskom broju ili e-pošti nakon potvrde da su dostavljene informacije važne za istragu u kaznenom postupku koja je u tijeku. *Vidjeti* 18 U.S.C., članak 3121. – 3127. Nezakonita uporaba ili postavljanje takvog uređaja savezno je kazneno djelo.

Zakon o privatnosti u području elektroničke komunikacije (ECPA): Dodatna pravila primjenjuju se na pristup vlade podacima o pretplatnicima, podacima o prometu i pohranjenom sadržaju komunikacija koje čuvaju telefonski operateri ISP-a i drugi pružatelji telefonskih usluga u skladu s glavnom II. ECPA-a, koji se naziva i Zakonom o pohranjenim komunikacijama (SCA), 18 U.S.C. članci 2701. – 2712. U SCA-u je uspostavljen sustav zakonske zaštite prava na privatnost kojim se tijelima za provedbu zakona omogućuje pristup podacima o klijentima i pretplatnicima pružatelja internetskih usluga samo u mjeri u kojoj je to propisano ustavnim zakonom. SCA-om se osigurava veća razina zaštite privatnosti ovisno o tome koliko se prikupljanjem narušava privatnost. Za prikupljanje registracijskih podataka korisnika, IP adresa i povezanih vremenskih žigova te podataka za naplatu tijela za provedbu zakona moraju pribaviti sudski nalog. Za većinu ostalih pohranjenih podataka koji ne uključuju sadržaj, poput zaglavlja poruka e-pošte bez predmeta, tijela za provedbu zakona moraju sucu obrazložiti zašto su ti podaci relevantni i od ključne važnosti za tekuću kaznenu istragu. Da bi mogla pribaviti pohranjeni sadržaj elektroničkih komunikacija, tijela za provedbu kaznenog zakona moraju pribaviti sudski nalog na temelju osnovane sumnje da predmetni račun sadržava dokaze o kaznenom djelu. U SCA je propisana i građanska odgovornost i kazne.

Sudski nalozi za nadzor u skladu sa saveznim Zakonom o uporabi prislušnih uređaja: Nadalje, tijela za provedbu zakona mogu u stvarno vrijeme presresti žičanu, usmenu ili elektroničku komunikaciju u svrhe kaznene istrage u skladu sa saveznim Zakonom o uporabi prislušnih uređaja. *Vidjeti* 18 U.S.C., članak 2510. – 2522. Ta se ovlast dobiva samo na

temelju sudskog naloga u kojem je sudac utvrdio, među ostalim, da postoji osnovana sumnja vjerovati da će se prisluškivanjem ili elektroničkim presretanjem prikupiti dokazi o saveznom kaznenom djelu ili o lokaciji bjegunca od kaznenog progona. U zakonu je predviđena građanska odgovornost i kazne u skladu sa kaznenim pravom za povrede odredaba o prisluškivanju

Nalog za pretragu – pravilo 41.: Tijela za provedbu zakona mogu fizički pretražiti prostorije u Sjedinjenim Državama kada ih je za to ovlastio sudac. Tijela za provedbu zakona moraju sucu dokazati da postoji „opravdana sumnja" da je počinjeno kazneno djelo ili da će ono biti počinjeno i da se predmeti povezani s kaznenim djelom vjerojatno nalaze na mjestu navedenom u nalogu. Ta se ovlast najčešće upotrebljava kada policija mora fizički pretražiti prostorije jer postoji opasnost od uništavanja dokaza u slučaju dostave sudskog ili drugog naloga korporaciji. *Vidjeti* Ustav SAD-a 4. amandman (o kojem se detaljno govorilo u prethodnom testu). Fed R. Crim. str. 41. Subjekt naloga za pretragu može tražiti poništavanje naloga kao pretjeranog, neosnovanog ili pribavljenog na neki drugi neprimjereni način i oštećene stranke mogu podnijeti zahtjev za odbacivanje dokaza pribavljenih nezakonitom pretragom. *Vidjeti Mapp protiv Ohio*, 367 U.S. 643 (1961.).

Smjernice i politike Ministarstva pravosuđa: Povrh ovih ustavnih i zakonskih ograničenja u pogledu pristupa državnih tijela podacima i ograničenja utemeljenih na pravilima, Glavni državni odvjetnik izdao je smjernice kojima se dodatno ograničava pristup tijela za provedbu zakona podacima i koje sadržavaju i mjere za zaštitu privatnosti i građanskih sloboda. Na primjer, Smjernicama glavnog državnog odvjetnika za postupke Saveznog istražnog ureda (FBI) (rujan 2008.) (dalje u tekstu: Smjernice glavnog državnog odvjetnika za FBI), dostupne na http://www.justice.gov/archive/opa/docs/guidelines.pdf, utvrđena su ograničenja u pogledu uporabe istražnih sredstava za traženje informacija povezanih s istragama kaznenih djela. Tim je smjernicama propisano da FBI mora upotrebljavati istražne metode kojima se najmanje narušava privatnost uzimajući u obzir učinak na privatnost i građanske slobode i moguću štetu za ugled. Nadalje, u njima se napominje da se „podrazumijeva da FBI mora provoditi svoje istrage i druge aktivnosti na zakonit i razuman način kojim se poštuje privatnost i sloboda i izbjegava nepotreban utjecaj na živote osoba koje poštuju zakone." *Vidjeti* Smjernice glavnog državnog odvjetnika za FBI na 5. FBI je provodio te smjernice s pomoću Vodiča FBI-ja za domaće istrage i operacije (DIOG) koji je dostupan na https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), sveobuhvatni priručnik koji uključuje detaljna ograničenja uporabe istražnih alata i smjernica za osiguranje zaštite građanskih sloboda u svakoj istrazi. Dodatna pravila i politike kojima se propisuju ograničenja istražnih aktivnosti saveznih tužitelja propisane su u **Priručniku za državne tužitelje SAD-a** (USAM), koji je dostupan i na internetu na http://www.justice.gov/usam/united-states-attorneys-manual.

Građanske i regulatorne ovlasti (javni interes):

Postoje velika ograničenja i u pogledu građanskog ili regulatornog (*npr.*„javni pristup") pristupa podacima korporacija u Sjedinjenim Američkim Državama. Agencije s građanskim i regulatornim ovlastima mogu izdavati sudske pozive korporacijama za poslovnu evidenciju, elektroničkih pohranjene podatke ili ostale opipljive stavke. Te agencije imaju ograničene ovlasti za izvršavanje ovlasti iz administrativnih ili g građanskih sudskih poziva ne samo zbog svojih statusa već i zbog neovisnog sudskog preispitivanja sudskih poziva prije mogućeg sudskog izvršenja. *Vidjeti npr.* Fed. R. Civ. str. 45. Agencije mogu tražiti pristup samo onim podacima koji su važni za pitanja unutar njihove nadležnosti. Nadalje, primatelj administrativnog sudskog poziva može osporiti izvršenje tog sudskog poziva na sudu dostavljanjem dokaza da agencija nije postupila u skladu s osnovnim standardima razumnosti, kako je prethodno navedeno.

Postoje i druge pravne osnove na temelju kojih poduzeća mogu osporavati zahtjeve upravnih agencija zbog posebnosti svoje industrijske grade i vrste podataka koje posjeduju. Na primjer, financijska institucija može osporiti administrativne sudske zahtjeve kojima sud traži određene podate kao povrede Zakona o bankarskoj tajni i njegovih provedbenih propisa. *Vidjeti* 31 U.S.C., članak 5318., 31 C.F.R. dio X. Druga poduzeća mogu se oslanjati na Zakon o poštenom izvješćivanju o kreditnom stanju, *vidjeti* 15 U.S.C. članak 1681.b ili na nizu drugih posebnih zakona. Zlouporaba ovlasti agencije za izdavanje naloga može dovesti do pozivanja agencije na odgovornost ili do osobne odgovornosti zaposlenika agencije. Vidjeti, na primjer Zakon o pravu na privatnost financijskih podataka, 12 U.S.C:, članak 3401. – 3422. Sudovi u Sjedinjenim Američkim Državama stoga su čuvari od nezakonitih regulatornih zahtjeva i osiguravaju neovisni nadzor djelovanja saveznih agencija.

Naposljetku, zakonske ovlasti upravnih tijela za fizičku zapljenu evidencije poduzeća u Sjedinjenim Američkim Državama tijekom administrativne pretrage moraju biti u skladu sa zahtjevima iz četvrtog amandmana. *Vidjeti See protiv grada Seattle*, 387 U.S. 541 (1967.).

Zaključak

Sve aktivnosti provedbe zakona i regulatorne aktivnosti u Sjedinjenim Američkim Državama moraju biti u skladu s primjenjivim zakonima, među ostalim s Ustavom SAD-a, zakonima, pravilima i propisima. Te aktivnosti moraju biti u skladu i s primjenjivim politikama, među ostalim sa Smjernicama Glavnog državnog odvjetnika kojima se uređuju savezne aktivnosti provedbe zakona. Prethodno opisanim pravnim okvirom ograničava se mogućnost američkih agencija za provedbu zakona i regulatornih agencija da pribavljaju podatke od korporacija u Sjedinjenim Američkim Državama, neovisno o tome odnose li se ti podaci na američke državljane ili osobe koje nisu američki državljani, te je dopušteno sudsko preispitivanje svih zahtjeva vlade za dostavljanje podataka u skladu s tim ovlastima.

S poštovanjem

Bruce C. Swartz

Zamjenik pomoćnika Glavnog državnog odvjetnika
i savjetnik za međunarodne poslove