PROVEDBENA ODLUKA KOMISIJE (EU) 2023/1795

od 10. srpnja 2023.

u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenoj razini zaštite osobnih podataka u skladu s okvirom EU-a i SAD-a za privatnost podataka

(priopćeno pod brojem dokumenta (C(2023) 4745)

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (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) ([1]), a posebno njezin članak 45. stavak 3.,

budući da:

1. UVOD

(1) Uredbom (EU) 2016/679 ([2]) utvrđuju se pravila za prijenos osobnih podataka od voditelja obrade ili izvršitelja obrade u Uniji trećim zemljama i međunarodnim organizacijama u mjeri u kojoj je takav prijenos obuhvaćen njezinim područjem primjene. Pravila o međunarodnim prijenosima podataka utvrđena su u poglavlju V. te uredbe. Iako je protok osobnih podataka u zemlje izvan Europske unije i iz njih bitan za širenje prekogranične trgovine i međunarodne suradnje, razina zaštite osobnih podataka u Uniji ne smije se narušiti prijenosima trećim zemljama ili međunarodnim organizacijama ([3]).

(2) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 Komisija može u provedbenom aktu odlučiti da treća zemlja, područje ili jedan ili više određenih sektora unutar treće zemlje osigurava primjerenu razinu zaštite. Pod tim uvjetom prijenosi osobnih podataka trećoj zemlji mogu se obavljati bez potrebe za bilo kakvim dodatnim odobrenjem, kako je predviđeno u članku 45. stavku 1. i uvodnoj izjavi 103. Uredbe (EU) 2016/679.

(3) Kako je navedeno u članku 45. stavku 2. Uredbe (EU) 2016/679, donošenje odluke o primjerenosti mora se temeljiti na sveobuhvatnoj analizi pravnog poretka treće zemlje, koja obuhvaća i pravila koja se primjenjuju na uvoznike podataka i ograničenja i zaštitne mjere u pogledu pristupa tijela javne vlasti osobnim podacima. Komisija u procjeni mora utvrditi jamči li predmetna treća zemlja razinu zaštite koja je „u načelu istovjetna" onoj koja je osigurana u Uniji (uvodna izjava 104. Uredbe (EU) 2016/679). To se ocjenjuje s obzirom na zakonodavstvo Unije, ponajprije na Uredbu (EU) 2016/679, te sudsku praksu Suda Europske unije (Sud) ([4]).

([1]) SL L 119, 4.5.2016., str. 1.
([2]) Radi lakšeg snalaženja popis kratica koje se upotrebljavaju u ovoj Odluci nalazi se u Prilogu VIII.
([3]) Vidjeti uvodnu izjavu 101. Uredbe (EU) 2016/679.
([4]) Vidjeti nedavni predmet C-311/18, Facebook Ireland i Schrems (*Schrems II*), ECLI:EU:C:2020:559.

(4) Kako je pojasnio Sud u presudi od 6. listopada 2015. u predmetu C-362/14, *Maximillian Schrems / Data Protection Commissioner* ([5]) *(Schrems)*, to ne zahtijeva utvrđivanje potpuno istovjetne razine zaštite. Naime, pravna sredstva kojima se predmetna treća zemlja koristi za zaštitu osobnih podataka mogu se razlikovati od onih koja se primjenjuju u Uniji, pod uvjetom da se u praksi pokažu djelotvornima za osiguravanje primjerene razine zaštite ([6]). Prema tome, standard primjerenosti ne podrazumijeva doslovno ponavljanje pravila Unije. Umjesto toga ispituje se pruža li predmetni strani sustav kao cjelina potrebnu razinu zaštite podataka sadržajem prava na privatnost i njihovom djelotvornom provedbom, nadzorom i ostvarivanjem ([7]). Nadalje, Komisija bi u skladu s presudom pri primjeni tog standarda prvenstveno trebala ocijeniti sadržava li pravni okvir predmetne treće zemlje pravila za ograničavanje zadiranja u temeljna prava osoba čiji se podaci prenose iz Unije koja su državna tijela te zemlje ovlaštena provoditi kad ostvaruju legitimne ciljeve kao što je nacionalna sigurnost, i pruža li učinkovitu pravnu zaštitu protiv takvog zadiranja ([8]). Smjernice o tome daju se i u Referentnom dokumentu o primjerenosti Europskog odbora za zaštitu podataka, u kojem se nastoji dodatno pojasniti taj standard ([9]).

(5) Standard koji se primjenjuje na takvo zadiranje u temeljna prava na privatnost i zaštitu podataka Sud je dodatno pojasnio u presudi od 16. srpnja 2020. u predmetu C-311/18, *Data Protection Commissioner / Facebook Ireland Limited i Maximillian Schrems (Schrems II)*, kojom je Provedbena odluka Komisije (EU) 2016/1250 ([10]) o prethodnom okviru za transatlantski protok podataka, europsko-američkom sustavu zaštite privatnosti (sustav zaštite privatnosti), proglašena nevaljanom. Sud je smatrao da ograničenja zaštite osobnih podataka koja proizlaze iz nacionalnog prava Sjedinjenih Američkih Država (SAD) o pristupu američkih javnih tijela podacima prenesenima iz Unije u SAD i njihovoj uporabi tih podataka u svrhe nacionalne sigurnosti nisu uređena na način koji ispunjava zahtjeve koji su u načelu istovjetni zahtjevima iz prava Unije, u skladu s kojima zadiranje u pravo na zaštitu podataka mora biti nužno i proporcionalno ([11]). Sud je smatrao i da osobe čiji su podaci preneseni u SAD nisu raspolagale pravnim sredstvom pred tijelom koje bi im pružilo jamstva koja su u načelu istovjetna onima propisanima člankom 47. Povelje o pravu na djelotvoran pravni lijek ([12]).

(6) Nakon što je donesena presuda u predmetu *Schrems II*, Komisija je započela pregovore s američkom vladom kako bi se donijela nova odluka o primjerenosti koja bi ispunjavala zahtjeve iz članka 45. stavka 2. Uredbe (EU) 2016/679 kako ih tumači Sud. Pregovori su završeni 7. listopada 2022., kad je SAD donio Izvršni nalog br. 14086 o poboljšanju zaštitnih mjera u američkim aktivnostima elektroničkog izviđanja, koji je dopunjen Uredbom o Žalbenom sudu za zaštitu podataka (DPRC) koju je donio glavni državni odvjetnik SAD-a („Uredba glavnog državnog odvjetnika") ([13]). Nadalje, okvir za poslovne subjekte koji obrađuju podatke koji se prenose iz Unije ažuriran je ovom Odlukom o okviru EU-a i SAD-a za privatnost podataka.

(7) Komisija je pažljivo analizirala američko pravo i praksu, uključujući Izvršni nalog br. 14086 i Uredbu glavnog državnog odvjetnika. Na temelju zaključaka iz uvodnih izjava od 9. do 200. Komisija zaključuje da SAD osigurava primjerenu razinu zaštite osobnih podataka koje u skladu s okvirom EU-a i SAD-a za zaštitu podataka voditelj ili izvršitelj obrade u Uniji ([14]) prenosi certificiranim organizacijama u SAD-u.

([5]) Predmet C-362/14, Maximilian Schrems / Data Protection Commissioner (*Schrems*), ECLI:EU:C:2015:650, t. 73.

([6]) *Schrems*, t. 74.

([7]) Vidjeti Komunikaciju Komisije Europskom parlamentu i Vijeću, Razmjena i zaštita osobnih podataka u globaliziranom svijetu, COM(2017) 7 od 10. siječnja 2017., odjeljak 3.1., str. 6.–7.

([8]) *Schrems*, t. 88.–89.

([9]) Europski odbor za zaštitu podataka, Referentni dokument o primjerenosti, WP 254 rev.01, dostupan na adresi: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

([10]) 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 (SL L 207, 1.8.2016., str. 1.).

([11]) *Schrems II*, t. 185.

([12]) *Schrems II*, t. 197.

([13]) Glava 28. odjeljak 302. Kodeksa saveznih propisa.

([14]) Ova je Odluka značajna za EGP. U Sporazumu o Europskom gospodarskom prostoru („Sporazum o EGP-u") predviđeno je proširenje unutarnjeg tržišta Europske unije na tri države EGP-a: Island, Lihtenštajn i Norvešku. Odluku Zajedničkog odbora o uključivanju Uredbe (EU) 2016/679 u Prilog XI. Sporazumu o EGP-u donio je Zajednički odbor EGP-a 6. srpnja 2018. te je stupila na snagu 20. srpnja 2018. Uredba je stoga obuhvaćena tim sporazumom. Za potrebe ove Odluke upućivanja na EU i države članice EU-a trebalo bi stoga tumačiti tako da ona obuhvaćaju i države EGP-a.

(8) Ova Odluka znači da za prijenose osobnih podataka od voditelja i izvršitelja obrade u Uniji ([15]) certificiranim organizacijama u SAD-u nisu potrebna daljnja odobrenja. Ona ne utječe na izravnu primjenu Uredbe (EU) 2016/679 na takve organizacije ako su ispunjeni uvjeti u pogledu teritorijalnog područja primjene te uredbe utvrđeni u njezinu članku 3.

2. OKVIR EU-a i SAD-a ZA PRIVATNOST PODATAKA

2.1. Osobno i materijalno područje primjene

2.1.1. *Certificirane organizacije*

(9) Okvir EU-a i SAD-a za privatnost podataka temelji se na sustavu certificiranja u okviru kojeg se američke organizacije obvezuju da će se pridržavati skupa načela privatnosti koji čine „Načela okvira EU-a i SAD-a za privatnost podataka" i Dodatna načela (zajedno: „Načela"), koji je objavilo Ministarstvo trgovine SAD-a i koji se nalazi u Prilogu I. ovoj Odluci ([16]). Da bi ispunila uvjete za certificiranje u skladu s okvirom EU-a i SAD-a za privatnost podataka, organizacija mora podlijegati istražnim i provedbenim ovlastima Savezne trgovinske komisije (FTC) ili Ministarstva prometa SAD-a ([17]). Načela se primjenjuju odmah nakon certificiranja. Kako je detaljnije objašnjeno u uvodnim izjavama od 47. do 51., svakih godinu dana organizacije uključene u okvir EU-a i SAD-a za privatnost podataka moraju se ponovno certificirati kako bi se potvrdilo da se pridržavaju Načela ([18]).

2.1.2. *Definicija osobnih podataka i pojmova „voditelj obrade" i „posrednik"*

(10) Okvir EU-a i SAD-a za privatnost podataka štiti sve osobne podatke koji se iz Unije prenose organizacijama u SAD-u koje posjeduju certifikat Ministarstva trgovine o pridržavanju Načela, osim podataka koji se prikupljaju za objavljivanje, emitiranje ili druge oblike javnog priopćavanja novinarskih materijala i informacija iz već objavljenih materijala iz medijskih arhiva ([19]). Stoga se takve informacije ne moraju prenositi u skladu s okvirom EU-a i SAD-a za privatnost podataka.

(11) Osobni podaci/osobne informacije u Načelima su definirani na isti način kao u Uredbi (EU) 2016/679, tj. kao „podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi i koji su obuhvaćeni područjem primjene Opće uredbe o zaštiti podataka (OUZP) te koje je organizacija u SAD-u primila iz EU-a i koji su zabilježeni u bilo kojem obliku" ([20]). To znači da obuhvaćaju i pseudonimizirane (ili šifrirane) istraživačke podatke (među ostalim i ako se šifra ne daje američkoj organizaciji koja ih prima) ([21]). Slično tomu, obrada je definirana kao „svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima, bilo automatiziranim bilo neautomatiziranim sredstvima, kao što su prikupljanje, bilježenje, organizacija, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje ili širenje te brisanje ili uništavanje" ([22]).

(12) Okvir EU-a i SAD-a za privatnost podataka primjenjuje se na organizacije u SAD-u koje se smatra voditeljima obrade (tj. osoba ili organizacija koja sama ili s drugima utvrđuje svrhe i sredstva obrade osobnih podataka) ([23]) ili izvršiteljima obrade (tj. posrednici koji djeluju u ime voditelja obrade) ([24]). Izvršitelji obrade iz SAD-a moraju se ugovorno obvezati da će postupati samo prema uputama voditelja obrade iz EU-a i pomagati mu da odgovori

([15]) Ova Odluka ne utječe na zahtjeve Uredbe (EU) 2016/679 koji se primjenjuju na subjekte (voditelje i izvršitelje obrade) u Uniji koji prenose podatke, npr. zahtjevi koji se odnose na ograničavanje svrhe, smanjenje količine podataka, transparentnost i sigurnost podataka (vidjeti i članak 44. Uredbe (EU) 2016/679).

([16]) U tom pogledu vidjeti presudu u predmetu *Schrems*, t. 81., u kojoj je Sud potvrdio da sustav samocertificiranja može osigurati primjerenu razinu zaštite.

([17]) Odjeljak I.2 Priloga I. Postoje određene iznimke od široke nadležnosti FTC-a u području tržišnih aktivnosti, na primjer u odnosu na banke, zračne prijevoznike, djelatnost osiguranja i zajedničke operaterske aktivnosti pružatelja telekomunikacijskih usluga (iako je odlukom od 26. veljače 2018. u predmetu FTC protiv AT&T-a Žalbeni sud 9. okruga potvrdio da FTC ima nadležnost u odnosu na samostalne operaterske aktivnosti takvih subjekata). Vidjeti i bilješku 2. Priloga IV. Ministarstvo prometa nadležno je za osiguravanje usklađenosti zračnih prijevoznika i posrednika u prodaji karata (za zračni prijevoz), vidjeti Prilog V. odjeljak A.

([18]) Odjeljak III.6 Priloga I.

([19]) Odjeljak III.2 Priloga I.

([20]) Odjeljak I.8.a Priloga I.

([21]) Odjeljak III.14.g Priloga I.

([22]) Odjeljak I.8.b Priloga I.

([23]) Odjeljak I.8.c Priloga I.

([24]) Vidjeti npr. odjeljak II.2.b Priloga I. i odjeljke II.3.b i 7.d, u kojima je pojašnjeno da posrednici djeluju u ime voditelja obrade u skladu s njegovim uputama i posebnim ugovornim obvezama.

pojedincima koji ostvaruju svoja prava u skladu s Načelima ([25]). Nadalje, u slučaju podobrade izvršitelj obrade mora sklopiti ugovor s izvršiteljem podobrade u kojem se jamči razina zaštite jednaka onoj koja je predviđena Načelima te poduzeti korake za njegovu ispravnu provedbu ([26]).

2.2. **Načela okvira EU-a i SAD-a za privatnost podataka**

2.2.1. ***Ograničavanje svrhe i izbor***

(13) Osobni podaci trebali bi se obrađivati zakonito i pošteno. Trebali bi se prikupljati u određenu svrhu i zatim se upotrebljavati samo ako to nije nespojivo sa svrhom obrade.

(14) U skladu s okvirom EU-a i SAD-a za privatnost podataka to je osigurano Načelima. Prvo, u skladu s *načelom cjelovitosti podataka i ograničavanja svrhe*, slično kao u skladu s člankom 5. stavkom 1. točkom (b) Uredbe (EU) 2016/679, organizacija ne smije obrađivati osobne podatke na način koji nije u skladu sa svrhom za koju su izvorno prikupljeni ili za koju je ispitanik naknadno dao odobrenje ([27]).

(15) Drugo, prije nego što upotrijebi osobne podatke za novu (izmijenjenu) svrhu koja je bitno drukčija no i dalje u skladu s izvornom svrhom ili ih otkrije trećoj strani, organizacija mora ispitanicima omogućiti prigovor (izuzeće), u skladu s *načelom izbora* ([28]), u okviru jasnog, vidljivog i lako dostupnog mehanizma. Važno je istaknuti da to načelo ne zamjenjuje izričitu zabranu neusklađene obrade ([29]).

([25]) Odjeljak III.10.a Priloga I. Vidjeti i smjernice koje je Ministarstvo trgovine u dogovoru s Europskim odborom za zaštitu podataka pripremilo u okviru sustava zaštite privatnosti kako bi se pojasnile obveze izvršitelja obrade iz SAD-a koji primaju osobne podatke iz Unije u skladu s tim okvirom. Budući da se ta pravila nisu promijenila, te smjernice odnosno najčešća pitanja i dalje su relevantni za okvir EU-a i SAD-a za privatnost podataka (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Odjeljak II.3.b Priloga I.

([27]) Odjeljak II.5.a Priloga I. Usklađene svrhe među ostalim uključuju reviziju, sprečavanje prijevare ili druge svrhe u skladu s očekivanjima razumne osobe s obzirom na kontekst prikupljanja podataka (vidjeti bilješku 6. Priloga I.).

([28]) Odjeljak II.2.a Priloga I. Ne primjenjuje se kad organizacija osobne podatke otkriva izvršitelju obrade koji postupa u njezino ime i prema njezinim uputama (odjeljak II.2.b Priloga I.). Pritom organizacija ipak mora imati sklopljen ugovor i osigurati usklađenost s načelom *odgovornosti za daljnji prijenos*, kako je detaljnije objašnjeno u uvodnoj izjavi 43. Nadalje, načelo *izbora* (kao i načelo *obavješćivanja*) može se ograničiti kad se osobni podaci obrađuju u kontekstu dubinske analize (za potrebe mogućeg spajanja ili preuzimanja) ili revizija na mjeru i razdoblje koji su nužni da se zadovolje zakonski zahtjevi ili zahtjevi javnog interesa odnosno na mjeru i razdoblje u kojima bi primjena tih načela naškodila legitimnim interesima organizacije u konkretnom kontekstu dubinskih analiza ili revizija (odjeljak III.4 Priloga I.). Izuzeće od načela izbora (i načela obavješćivanja i odgovornosti za daljnji prijenos) predviđeno je i dodatnim načelom br. 15 (odjeljci III.15.a i b Priloga I.) u slučaju osobnih podataka iz javno dostupnih izvora (osim ako izvoznik podataka iz EU-a ne navede da informacije podliježu ograničenjima zbog kojih se moraju primjenjivati ta načela) i osobnih podataka prikupljenih iz evidencija koje su općenito otvorene na uvid javnosti (ako se ne pojavljuju u kombinaciji s informacijama iz evidencije koja nije javna i ako se poštuju uvjeti za ostvarivanje uvida). Slično tomu, izuzeće od načela *izbora* (i načela *obavješćivanja* i *odgovornosti za daljnji prijenos*) predviđeno je i dodatnim načelom br. 14 (odjeljak III.14.f Priloga I.) u slučaju osobnih podataka koje poduzeće koje proizvodi farmaceutske ili medicinske proizvode obrađuje u okviru praćenja sigurnosti i učinkovitosti proizvoda ako se zbog pridržavanja Načela ne mogu ispuniti regulatorni zahtjevi.

([29]) To se odnosi na sve prijenose podataka u skladu s okvirom EU-a i SAD-a za privatnost podataka, uključujući prijenos podataka prikupljenih u kontekstu radnog odnosa. Iako se certificirana američka organizacija stoga u načelu smije koristiti podacima o ljudskim resursima u svrhe koje nisu povezane s radnim odnosom (npr. određeni promidžbeni sadržaji), mora se pridržavati zabrane neusklađene obrade i smije to činiti samo u skladu s načelima *obavješćivanja* i *izbora*. Organizacija iznimno može upotrebljavati osobne podatke u dodatnu usklađenu svrhu bez poštovanja načela *obavješćivanja* i *izbora*, ali samo u mjeri i razdoblju koje je potrebno da se izbjegne ugrožavanje sposobnosti organizacije da donosi odluke o promaknućima, imenovanjima ili druge slične odluke o zapošljavanju (vidjeti odjeljak III.9.b.iv Priloga I.). Zabranom američkim organizacijama 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. Vidjeti odjeljak III.9.b.i Priloga I.

2.2.2. ***Obrada posebnih kategorija osobnih podataka***

(16) Trebale bi postojati posebne zaštitne mjere ako se obrađuju „posebne kategorije" podataka.

(17) U skladu s *načelom izbora* posebne zaštitne mjere primjenjuju se ako se obrađuju „osjetljive informacije", tj. osobni podaci o medicinskom ili zdravstvenom stanju, rasi ili etničkom podrijetlu, političkim stavovima, vjerskim ili filozofskim uvjerenjima, članstvu u sindikatu ili informacije o spolnom životu pojedinca ili sve druge informacije primljene od treće strane koje ta strana smatra osjetljivima i postupa s njima kao takvima ([30]). To znači da će sve podatke koji se smatraju osjetljivima u skladu s pravom Unije o zaštiti podataka (uključujući podatke o spolnoj orijentaciji, genetske i biometrijske podatke) certificirane organizacije smatrati osjetljivima i u skladu s okvirom EU-a i SAD-a za privatnost podataka.

(18) Organizacije u pravilu moraju ishoditi izričitu privolu (tj. pristanak) pojedinaca za uporabu osjetljivih informacija ili njihovo otkrivanje trećim stranama u neku drugu svrhu osim one za koju su izvorno prikupljene ili za koju je pojedinac naknadno dao odobrenje (pristankom) ([31]).

(19) Ta privola ne mora se dobiti u ograničenim okolnostima koje su slične usporedivim izuzećima predviđenima pravom Unije o zaštiti podataka, na primjer ako je obrada osjetljivih podataka od životno važnog interesa za osobu, ako je potrebna za postavljanje pravnih zahtjeva ili ako je potrebna da bi se pružila medicinska skrb ili dijagnoza ([32]).

2.2.3. ***Točnost, smanjenje količine i sigurnost podataka***

(20) Podaci bi trebali biti točni i prema potrebi ažurni. Trebali bi biti i primjereni i relevantni i ne bi trebali biti pretjerani u odnosu na svrhe u koje se obrađuju te bi se načelno trebali čuvati samo onoliko dugo koliko je potrebno u svrhe u koje se osobni podaci obrađuju.

(21) U skladu s načelom *cjelovitosti podataka i ograničavanja svrhe* ([33]) osobni podaci moraju biti ograničeni na ono što je relevantno za svrhu obrade. Nadalje, ako je to potrebno za te svrhe, organizacije moraju poduzeti razumne korake da osobni podaci budu pouzdani za namjeravanu uporabu, točni, potpuni i ažurni.

(22) Osim toga, osobne informacije mogu se čuvati u obliku kojim se utvrđuje identitet pojedinca ili koji omogućuje utvrđivanje njegova identiteta (dakle u obliku osobnih podataka) ([34]) samo dok služe svrsi za koju su izvorno prikupljene ili za koju je pojedinac naknadno dao odobrenje u skladu s *načelom izbora*. Ta obveza ne sprečava organizacije da nastave obrađivati osobne informacije i dulje, ali samo onoliko dugo i u onoj mjeri u kojoj takva obrada razumno služi jednoj od sljedećih posebnih svrha koje su slične usporedivim izuzećima predviđenima pravom Unije o zaštiti podataka: arhiviranju u javnom interesu, novinarstvu, književnosti i umjetnosti, znanstvenim i povijesnim istraživanjima i statističkim analizama ([35]). Ako se osobni podaci čuvaju u jednu od tih svrha, njihova obrada podliježe zaštitnim mjerama iz Načela ([36]).

(23) Osobni podaci trebali bi se obrađivati tako da se jamči njihova sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja. U tu bi svrhu voditelji i izvršitelji obrade trebali poduzeti odgovarajuće tehničke ili organizacijske mjere za zaštitu osobnih podataka od mogućih prijetnji. Te bi mjere trebalo procijeniti uzimajući u obzir najnovija dostignuća, povezane troškove te prirodu, opseg, kontekst i svrhe obrade, kao i rizike za prava pojedinaca.

([30]) Odjeljak II.2.c Priloga I.
([31]) Odjeljak II.2.c Priloga I.
([32]) Odjeljak III.1 Priloga I.
([33]) Odjeljak II.5 Priloga I.
([34]) Vidjeti bilješku 7. Priloga I. u kojoj je pojašnjeno da se smatra da se pojedinčev „identitet može utvrditi" sve dok organizacija ili treća strana mogu u razumnoj mjeri identificirati pojedinca s obzirom na sredstva identificiranja za koja se može razumno očekivati da će se upotrijebiti (uzimajući u obzir, među ostalim, troškove i vrijeme potrebne za utvrđivanje identiteta te tehnologiju dostupnu u trenutku obrade).
([35]) Odjeljak II.5.b Priloga I.
([36]) Vidjeti prethodnu *bilješku*.

(24) U skladu s okvirom EU-a i SAD-a za privatnost podataka to se postiže *načelom sigurnosti*, kojim je slično kao člankom 32. Uredbom (EU) 2016/679 predviđeno poduzimanje razumnih i odgovarajućih sigurnosnih mjera uzimajući u obzir rizike povezane s obradom i prirodom podataka ([37]).

2.2.4. ***Transparentnost***

(25) Ispitanike bi trebalo obavijestiti o glavnim obilježjima obrade njihovih osobnih podataka.

(26) Tomu služi *načelo obavješćivanja* ([38]), kojim je slično kao zahtjevima transparentnosti iz Uredbe (EU) 2016/679 predviđeno da organizacije među ostalim obavješćuju ispitanike o i. tome da je organizacija uključena u okvir za privatnost podataka, ii. vrsti prikupljenih podataka, iii. svrsi obrade, iv. vrsti ili identitetu trećih strana kojima bi se osobni podaci mogli otkriti i svrhama za to, v. njihovim pojedinačnim pravima, vi. načinu na koji se obratiti organizaciji i vii. dostupnim oblicima pravne zaštite.

(27) Ta obavijest mora biti jasno i razumljivo navedena kad se od pojedinaca prvi put traži da dostave osobne podatke ili što prije nakon toga, no u svakom slučaju prije nego što se podaci upotrijebe u neku bitno drukčiju (no usklađenu) svrhu od one u koju su prikupljeni ili prije nego što ih se otkrije trećoj strani ([39]).

(28) Osim toga, organizacije moraju objaviti svoje politike zaštite privatnosti kojima se prenose Načela (ili ih, u slučaju podataka o ljudskim resursima, učiniti dostupnima pojedincima na koje se odnose) te navesti poveznice na internetske stranice Ministarstva trgovine (uz dodatne pojedinosti o certificiranju, pravima ispitanika i dostupnim mehanizmima pravne zaštite), popis organizacija uključenih u okvir za privatnost podataka i internetske stranice odgovarajućeg pružatelja usluga alternativnog rješavanja sporova ([40]).

2.2.5. ***Prava pojedinaca***

(29) Ispitanici bi trebali imati određena prava koja mogu ostvariti u odnosu na voditelja ili izvršitelja obrade, osobito pravo na pristup podacima, pravo na prigovor na obradu i pravo na ispravak ili brisanje podataka.

(30) *Načelom pristupa* ([41]) iz okvira EU-a i SAD-a za privatnost podataka ta su prava osigurana pojedincima. Točnije, ispitanici imaju pravo, bez potrebe za opravdanjem, na to da od organizacije dobiju potvrdu o tome obrađuje li ona osobne podatke koji se odnose na njih, da im dostavi te podatke i da dobiju informacije o svrsi obrade, kategorijama osobnih podataka koji se obrađuju i primateljima (kategorijama primatelja) kojima se podaci otkrivaju ([42]). Organizacije moraju odgovoriti na zahtjeve za pristup u razumnom roku ([43]). Organizacija može u razumnoj mjeri

([37]) Odjeljak II.4.a Priloga I. Osim toga, u skladu s okvirom EU-a i SAD-a za privatnost podataka poslodavci bi pri obradi podataka o ljudskim resursima trebali poštovati želje zaposlenika u pogledu privatnosti tako što će ograničiti pristup osobnim podacima, anonimizirati određene podatke ili dodijeliti šifre odnosno pseudonime (odjeljak III.9.b.iii Priloga I.).

([38]) Odjeljak II.1 Priloga I.

([39]) Odjeljak II.1.b Priloga I. U dodatnom načelu br. 14. (odjeljci III.14.b i c Priloga I.) utvrđene su posebne odredbe o obradi osobnih podataka u kontekstu zdravstvenih istraživanja i kliničkih ispitivanja. Točnije, tim se načelom organizacijama dopušta da obrađuju podatke iz kliničkih ispitivanja čak i nakon što se osoba povuče iz ispitivanja ako je u obavijesti to bilo jasno navedeno kad je pojedinac pristao sudjelovati. Slično tomu, ako organizacija uključena u okvir EU-a i SAD-a za privatnost podataka primi osobne podatke za potrebe zdravstvenih istraživanja, može ih upotrijebiti za novo istraživanje samo u skladu s načelima *obavješćivanja* i *izbora*. U tom bi slučaju pojedinca u načelu trebalo obavijestiti o svim budućim posebnim načinima uporabe podataka (npr. povezane studije). Ako u početnoj obavijesti nije moguće navesti sve buduće načine uporabe podataka (jer bi nova saznanja ili napredak u medicini/istraživanju mogli dovesti do novih načina uporabe u istraživanju), u njoj se mora objasniti da bi se podaci mogli upotrijebiti u budućim nepredviđenim medicinskim i farmaceutskim istraživanjima. Ako takva daljnja uporaba nije u skladu s općim svrhama istraživanja u koje su podaci prikupljeni (tj. ako su nove svrhe bitno drukčije no i dalje u skladu s izvornom svrhom, vidjeti uvodne izjave 14. i 15.), mora se dobiti nova privola (tj. pristanak). Vidjeti i posebna ograničenja/izuzeća od načela *obavješćivanja* opisana u bilješci 28.

([40]) Odjeljak III.6.d Priloga I.

([41]) Vidjeti i dodatno načelo o pristupu (odjeljak III.8 Priloga I.).

([42]) Odjeljci III.8.a.i–ii Priloga I.

([43]) Odjeljak III.8.i Priloga I.

ograničiti broj zahtjeva za pristup istog pojedinca kojima će udovoljiti u određenom razdoblju i može naplatiti naknadu koja nije pretjerana, na primjer ako su zahtjevi očigledno pretjerani jer se ponavljaju ([44]).

(31) Pravo pristupa može se ograničiti samo u izvanrednim okolnostima koje su slične onima predviđenima pravom Unije o zaštiti podataka, osobito ako bi bila povrijeđena legitimna prava drugih osoba, ako bi teret ili trošak omogućivanja pristupa bio nerazmjeran rizicima za privatnost pojedinca u okolnostima slučaja (iako trošak i teret nisu presudni u odlučivanju o tome je li omogućivanje pristupa razumno), ako je vjerojatno da će otkrivanje narušiti zaštitu bitnih prevladavajućih javnih interesa, kao što su nacionalna sigurnost, javna sigurnost ili obrana, ako informacije sadržavaju povjerljive poslovne informacije ili ako se informacije obrađuju isključivo u istraživačke ili statističke svrhe ([45]). Svako uskraćivanje ili ograničavanje mora biti nužno i opravdano, a organizacija snosi teret dokazivanja ispunjenosti tih zahtjeva ([46]). U toj procjeni organizacija mora osobito uzeti u obzir interese pojedinca ([47]). Ako se predmetne informacije mogu izdvojiti od drugih podataka na koje se primjenjuje ograničenje, organizacija mora ispustiti zaštićene informacije i otkriti ostale informacije ([48]).

(32) Nadalje, ispitanici imaju pravo na ispravak ili izmjenu netočnih podataka odnosno brisanje podataka koji su obrađeni u suprotnosti s Načelima ([49]). Osim toga, kako je objašnjeno u uvodnoj izjavi 15., pojedinci imaju pravo prigovora na obradu njihovih podataka u bitno drukčije (no usklađene) svrhe od onih za koje su podaci prikupljeni te na njihovo otkrivanje trećim stranama odnosno imaju pravo na izuzeće od takve obrade i otkrivanja. Ako se osobni podaci upotrebljavaju u svrhe izravnog marketinga, pojedinci imaju opće pravo na izuzeće od takve obrade u bilo kojem trenutku ([50]).

(33) U Načelima se izričito ne spominje pitanje odluka koje utječu na ispitanika, a donesene su isključivo na temelju automatizirane obrade osobnih podataka. No, sve odluke koje se temelje na automatiziranoj obradi osobnih podataka prikupljenih u Uniji obično donosi voditelj obrade u Uniji (koji ima izravan odnos s ispitanikom na kojeg se odnose podaci) i stoga se na njih izravno primjenjuje Uredba (EU) 2016/679 ([51]). To uključuje scenarije prijenosa u kojima obradu vrši strani (npr. američki) poslovni subjekt koji djeluje kao posrednik (izvršitelj obrade) u ime voditelja obrade u Uniji (ili kao izvršitelj podobrade koji djeluje u ime izvršitelja obrade iz Unije nakon što je podatke dobio od voditelja obrade iz Unije koji ih je prikupio) koji onda na temelju toga donosi odluku.

(34) To je potvrđeno u studiji čiju je izradu Komisija naručila 2018. u kontekstu drugog godišnjeg preispitivanja funkcioniranja sustava zaštite privatnosti ([52]) i u kojoj se zaključilo da u trenutku izrade nisu postojali dokazi za to da organizacije uključene u sustav zaštite privatnosti obično donose odluke na temelju automatizirane obrade osobnih podataka prenesenih u okviru tog sustava.

([44]) Odjeljci III.8.a.i–ii i III.8.g Priloga I.
([45]) Odjeljci III.4, 8.b, c i e, 14.e i f te 15.d Priloga I.
([46]) Odjeljak III.8.e.ii Priloga I. Organizacija mora obavijestiti pojedinca o razlozima za uskraćivanje/ograničavanje i kontaktnoj točki za daljnje upite, odjeljak III.8.a.iii.
([47]) Odjeljci III.8.a.ii–iii Priloga I.
([48]) Odjeljak III.8.a.i Priloga I.
([49]) Odjeljci II.6 i III.8.a.i Priloga I.
([50]) Odjeljak III.8.12 Priloga I.
([51]) Suprotno tomu, u iznimnom slučaju kad američka organizacija ima izravan odnos s ispitanikom iz Unije, to je obično posljedica toga što se ciljano usmjerila na tog pojedinca u Uniji ponudom robe ili usluga ili praćenjem njegova ponašanja. U tom će scenariju sama američka organizacija biti obuhvaćena područjem primjene Uredbe (EU) 2016/679 (članak 3. stavak 2.) te se mora izravno pridržavati prava Unije o zaštiti podataka.
([52]) SWD(2018) 497 final, odjeljak 4.1.5. Studija je bila usmjerena na i. mjeru u kojoj organizacije uključene u sustav zaštite privatnosti donose odluke koje utječu na pojedince na temelju automatizirane obrade osobnih podataka prenesenih iz poduzeća u EU-u u okviru sustava zaštite privatnosti te ii. zaštitne mjere za pojedince koje su američkim saveznim pravom predviđene za takve situacije i uvjete za primjenu tih zaštitnih mjera.

(35) U svakom slučaju, u područjima gdje će poduzeća najvjerojatnije primijeniti automatiziranu obradu osobnih podataka za donošenje odluka koje utječu na pojedinca (npr. odobravanje kredita, ponude hipotekarnih kredita, zapošljavanje, stanovanje i osiguranje) američkim pravom predviđeni su posebni oblici zaštite od negativnih odluka ([53]). Tim se zakonima obično osigurava pravo pojedinaca na informiranost o konkretnim razlozima na kojima se temelji odluka (npr. odbijanje kredita), na osporavanje nepotpunih ili netočnih informacija (kao i oslanjanja na nezakonite čimbenike) i na pravnu zaštitu. Kad je riječ o potrošačkim kreditima, Zakonom o poštenom izvješćivanju o kreditnoj sposobnosti (Fair Credit Reporting Act – FCRA) i Zakonom o jednakim mogućnostima za dobivanje kredita (Equal Credit Opportunity Act – ECOA) predviđene su zaštitne mjere koje potrošačima omogućuju neki oblik prava na objašnjenje i prava na osporavanje odluke. Ti se zakoni primjenjuju u nizu područja, uključujući kreditiranje, zapošljavanje, stanovanje i osiguranje. Osim toga, određenim zakonima o zabrani diskriminacije, kao što su glava VII. Zakona o građanskim pravima (Civil Rights Act) i Zakon protiv diskriminacije pri prodaji ili iznajmljivanju stambenog prostora (Fair Housing Act), štiti se pojedince od modela koji se upotrebljavaju u automatiziranom donošenju odluka i koji bi mogli dovesti do diskriminacije na temelju određenih značajki te se pojedincima dodjeljuju prava na osporavanje takvih odluka, uključujući automatizirane odluke. Pravilo zaštite privatnosti iz Zakona o prenosivosti i odgovornosti u zdravstvenom osiguranju (Health Insurance Portability and Accountability Act – HIPPA) pak stvara određena prava koja su slična onima iz Uredbe (EU) 2016/679, a odnose se na pristup osobnim zdravstvenim informacijama. Nadalje, prema smjernicama američkih tijela pružatelji zdravstvenih usluga moraju dobiti informacije koje im omogućuju da pojedince informiraju o sustavima za automatizirano donošenje odluka koji se upotrebljavaju u medicinskom sektoru ([54]).

(36) Stoga ta pravila pružaju oblike zaštite koji su slični onima predviđenima pravom Unije o zaštiti podataka u malo vjerojatnoj situaciji u kojoj bi organizacija uključena u okvir EU-a i SAD-a za privatnost podataka donosila automatizirane odluke.

2.2.6. ***Ograničenja daljnjih prijenosa***

(37) Razina zaštite osobnih podataka koji se prenose iz Unije organizacijama u SAD-u ne smije se ugroziti daljnjim prijenosom tih podataka primateljima u SAD-u ili drugoj trećoj zemlji.

(38) U skladu s *načelom odgovornosti za daljnji prijenos* ([55]) primjenjuju se posebna pravila za „daljnje prijenose”, tj. prijenose osobnih podataka iz organizacije uključene u okvir EU-a i SAD-a za privatnost podataka voditelju ili izvršitelju obrade koji je treća strana, neovisno o tome nalazi li se ta strana u SAD-u ili trećoj zemlji izvan SAD-a (i Unije). Daljnji prijenos dopušten je samo i. u ograničene i određene svrhe, ii. na temelju ugovora između organizacije uključene u okvir EU-a i SAD-a za privatnost podataka i treće strane ([56]) (ili usporedivog sporazuma grupe poduzeća ([57])) i iii. samo ako je treća strana ugovorno obvezana pružati razinu zaštite jednaku onoj koja je zajamčena Načelima.

(39) Kad se ta obveza pružanja razine zaštite jednake onoj koja je zajamčena Načelima tumači u kombinaciji s *načelom cjelovitosti podataka i ograničavanja svrhe*, ona prvenstveno znači da treća strana može obrađivati osobne informacije koje su joj prenesene samo u svrhe koje su usklađene sa svrhama u koje su prikupljene ili za koje je pojedinac naknadno dao odobrenje (u skladu s *načelom izbora*).

([53]) Vidjeti npr. Zakon o jednakim mogućnostima za dobivanje kredita (glava 15. članak 1691. i dalje Zakonika SAD-a), Zakon o poštenom izvješćivanju o kreditnoj sposobnosti (glava 15. članak 1681. i dalje Zakonika SAD-a) ili Zakon protiv diskriminacije pri prodaji ili iznajmljivanju stambenog prostora (glava 42. članak 3601. i dalje Zakonika SAD-a). Osim toga, Sjedinjene Američke Države prihvatile su Načela o umjetnoj inteligenciji Organizacije za ekonomsku suradnju i razvoj, koja među ostalim sadržavaju načela transparentnosti, objašnjivosti, sigurnosti i odgovornosti.

([54]) Vidjeti npr. smjernice dostupne na 2042-Kojim osobnim zdravstvenim informacijama u posjedu pružatelja zdravstvene zaštite i iz zdravstvenog osiguranja pojedinci imaju pravo pristupiti na temelju HIPAA-e? | HHS.gov

([55]) Vidjeti odjeljak II.3. Priloga I. i dodatno načelo o obveznim ugovorima za daljnje prijenose (odjeljak III.10 Priloga I.)

([56]) Iznimno od tog općeg načela organizacija može osobne podatke manjeg broja zaposlenika dalje prenositi, a da pritom ne sklapa ugovor s primateljem, za povremene operativne potrebe povezane s radnim odnosom, npr. rezerviranje leta ili hotelske sobe ili ugovaranje osiguranja. No i u tom slučaju organizacija se mora pridržavati načela *obavješćivanja* i *izbora* (vidjeti odjeljak III.9.e Priloga I.).

([57]) Vidjeti i dodatno načelo o obveznim ugovorima za daljnje prijenose (odjeljak III.10.b Priloga I.). Iako to načelo omogućuje prijenose i na osnovi izvanugovornih instrumenata (npr. unutargrupni programi usklađenosti i kontrole), iz njegove je formulacije jasno da ti instrumenti uvijek moraju jamčiti „kontinuitet zaštite osobnih informacija u skladu s Načelima”. Nadalje, budući da će certificirana američka organizacija i dalje biti odgovorna za usklađenost s Načelima, imat će jak poticaj za uporabu instrumenata koji su doista djelotvorni u praksi.

(40) *Načelo odgovornosti za daljnji prijenos* trebalo bi isto tako tumačiti u vezi s *načelom obavješćivanja*, a u slučaju daljnjeg prijenosa voditelju obrade koji je treća strana ([58]) i s *načelom izbora* prema kojem se ispitanike mora obavijestiti (među ostalim) o vrsti/identitetu primatelja koji je treća strana, svrsi daljnjeg prijenosa i ponuđenom izboru te prema kojem ispitanici imaju pravo na prigovor (izuzeće) ili, u slučaju osjetljivih podataka, na „izričitu privolu" (pristanak) za daljnji prijenos.

(41) Obveza pružanja razine zaštite jednake onoj koja se zahtijeva Načelima primjenjuje se na sve treće strane uključene u obradu tako prenesenih podataka neovisno o njihovoj lokaciji (SAD ili druga treća zemlja) i kad sam izvorni primatelj koji je treća strana prenese te podatke drugom primatelju koji je treća strana, na primjer u svrhu podobrade.

(42) U svim slučajevima u ugovoru s primateljem koji je treća strana treba biti navedeno da će, ako utvrdi da više ne može ispunjavati svoju obvezu, primatelj o tome obavijestiti organizaciju uključenu u okvir EU-a i SAD-a za privatnost podataka. Ako se to utvrdi, obrada koju provodi treća strana mora prestati ili se moraju poduzeti drugi razumni i odgovarajući koraci za rješavanje te situacije ([59]).

(43) Dodatni oblici zaštite primjenjuju se u slučaju daljnjeg prijenosa posredniku koji je treća strana (tj. izvršitelju obrade). U tom slučaju američka organizacija mora se pobrinuti za to da posrednik postupa samo prema njezinim uputama te mora poduzeti razumne i odgovarajuće korake i. kako bi osigurala da posrednik stvarno obrađuje prenesene osobne informacije u skladu s obvezama organizacije iz Načela i ii. kako bi nakon što primi obavijest, zaustavila i ispravila neovlaštenu obradu ([60]). Ministarstvo trgovine moglo bi tražiti od organizacije da dostavi sažetak ili reprezentativni primjerak odredbi o zaštiti privatnosti iz ugovora ([61]). Ako se u lancu (pod)obrade pojave problemi zbog neusklađenosti, organizacija koja je voditelj obrade osobnih podataka u načelu će snositi odgovornost u skladu s *načelom pravne zaštite, provedbe i odgovornosti* osim ako dokaže da nije odgovorna za događaj zbog kojeg je nastala šteta ([62]).

2.2.7. ***Odgovornost***

(44) Na temelju načela odgovornosti subjekti koji obrađuju podatke moraju uvesti odgovarajuće tehničke i organizacijske mjere kako bi djelotvorno ispunili svoje obveze u pogledu zaštite podataka te mogli dokazati da su ispunjene, prije svega nadležnom nadzornom tijelu.

(45) Nakon što se organizacija dobrovoljno odluči za certificiranje ([63]) u skladu s okvirom EU-a i SAD-a za privatnost podataka, preuzima izvršivu obvezu da stvarno postupa u skladu s Načelima. U skladu s *načelom pravne zaštite, provedbe i odgovornosti* ([64]) organizacije uključene u okvir EU-a i SAD-a za privatnost podataka moraju uspostaviti djelotvorne mehanizme za jamčenje usklađenosti s Načelima. Osim toga, organizacije moraju poduzeti mjere kako bi provjerile ([65]) jesu li njihove politike zaštite privatnosti u skladu s Načelima i potvrdile da se stvarno postupa u skladu s njima. To se može učiniti u okviru sustava samoprocjene, koji mora uključivati unutarnje postupke za osposobljavanje zaposlenika u području provedbe politika zaštite privatnosti organizacije te periodično objektivno preispitivanje usklađenosti ili vanjsko preispitivanje usklađenosti, koje može uključivati reviziju, nasumične provjere ili uporabu tehnologije.

([58]) Pojedinci neće imati pravo zatražiti izuzeće ako se osobni podaci prenose trećoj strani koja u ulozi posrednika izvršava zadaće u ime i prema uputama američke organizacije. Međutim, američka organizacija pritom mora imati sklopljen ugovor s posrednikom te izvršavanjem svojih ovlasti za davanje uputa jamči da će se primjenjivati oblici zaštite predviđeni Načelima.

([59]) 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 prestane s obradom ili poduzme druge razumne i odgovarajuće korake za rješavanje situacije. U drugom slučaju organizacija uključena u okvir EU-a i SAD-a za privatnost podataka, kao voditelj obrade u skladu s čijim uputama postupa posrednik, mora poduzeti te mjere. Vidjeti odjeljak II.3 Priloga I.

([60]) Odjeljak II.3.b Priloga I.

([61]) *Vidjeti prethodnu* bilješku.

([62]) Odjeljak II.7.d Priloga I.

([63]) Vidjeti i dodatno načelo o samocertificiranju (odjeljak III.6 Priloga I.).

([64]) Vidjeti i dodatno načelo o rješavanju sporova i provedbi (odjeljak III.11 Priloga I.).

([65]) Vidjeti i dodatno načelo o provjeri (odjeljak III.7 Priloga I.).

(46) Osim toga, organizacije moraju čuvati evidenciju o provedbi svoje prakse u skladu s okvirom EU-a i SAD-a za privatnost podataka i, u kontekstu istrage neusklađenosti ili pritužbe zbog neusklađenosti, na zahtjev ih dati na uvid neovisnom tijelu za rješavanje sporova ili nadležnom provedbenom tijelu ([66]).

2.3. **Upravljanje, nadzor i provedba**

(47) Ministarstvo trgovine upravljat će okvirom EU-a i SAD-a za privatnost podataka i nadzirati ga. Okvir obuhvaća nadzorne i provedbene mehanizme kako bi se moglo provjeriti i osigurati da organizacije uključene u okvir postupaju u skladu s Načelima i kako bi se ispravili svi slučajevi neusklađenosti. Ti su mehanizmi utvrđeni u Načelima (Prilog I.) i obvezama Ministarstva trgovine (Prilog III.), FTC-a (Prilog IV.) i Ministarstva prometa (Prilog V.).

2.3.1. ***(Ponovno) certificiranje***

(48) Za certificiranje u skladu s okvirom EU-a i SAD-a za privatnost podataka (ili godišnje ponovno certificiranje) organizacije moraju javno izjaviti da su se obvezale postupati u skladu s Načelima, omogućiti uvid u svoje politike zaštite privatnosti i u cijelosti ih provoditi ([67]). Pri podnošenju molbe za (ponovno) certificiranje organizacije moraju dostaviti informacije Ministarstvu trgovine, uključujući naziv predmetne organizacije, opis svrha u koje će organizacija obrađivati osobne podatke, popis osobnih podataka koji će se obuhvatiti certificiranjem te informacije o odabranom načinu provjere, relevantnom neovisnom mehanizmu pravne zaštite i zakonskom tijelu koje je nadležno za osiguranje usklađenosti s Načelima ([68]).

(49) Organizacije mogu primati osobne podatke na temelju okvira EU-a i SAD-a za privatnost podataka od datuma kad ih Ministarstvo trgovine unese na popis organizacija uključenih u okvir za privatnost podataka. Radi pravne sigurnosti i izbjegavanja „lažnih izjava" organizacije koje su prvi put u postupku certificiranja ne smiju javno isticati da se pridržavaju Načela prije nego što Ministarstvo trgovine utvrdi da je prijava za certificiranje organizacije dovršena i doda organizaciju na navedeni popis ([69]). Da bi i dalje mogle primati osobne podatke iz Unije u skladu s okvirom EU-a i SAD-a za privatnost podataka, takve organizacije moraju svake godine ponovno certificirati svoje sudjelovanje u okviru. Ako organizacija napusti okvir EU-a i SAD-a za privatnost podataka iz bilo kojeg razloga, mora ukloniti sve izjave iz kojih bi se moglo zaključiti da i dalje sudjeluje u njemu ([70]).

(50) U skladu s obvezama utvrđenima u Prilogu III. Ministarstvo trgovine provjeravat će ispunjavaju li organizacije sve zahtjeve za certificiranje i jesu li uspostavile (javnu) politiku zaštite privatnosti koja sadržava informacije propisane *načelom obavješćivanja* ([71]). Oslanjajući se na iskustvo s (ponovnim) certificiranjem u okviru sustava zaštite privatnosti, Ministarstvo trgovine provest će niz provjera kako bi, među ostalim, utvrdilo sadržavaju li politike zaštite privatnosti organizacija poveznicu na ispravan obrazac za pritužbu na internetskim stranicama relevantnog neovisnog mehanizma rješavanja sporova te, ako je više subjekata i podružnica iste organizacije obuhvaćeno prijavom za certificiranje, ispunjavaju li politike zaštite privatnosti svakog od tih subjekata zahtjeve za certificiranje i jesu li lako dostupne ispitanicima ([72]). Nadalje, Ministarstvo trgovine prema potrebi će stupiti u kontakt s FTC-om i Ministarstvom prometa kako bi provjerilo jesu li organizacije u nadležnosti nadzornog tijela navedenog u prijavi za (ponovno) certificiranje te će surađivati s tijelima za alternativno rješavanje sporova kako bi provjerilo jesu li se organizacije registrirale za neovisni mehanizam pravne zaštite naveden u prijavi za (ponovno) certificiranje ([73]).

([66]) Odjeljak III.7 Priloga I.
([67]) Odjeljak I.2 Priloga I.
([68]) Odjeljak III.6.b Priloga I. i odjeljak „Provjera zahtjeva za samocertificiranje" Priloga III.
([69]) Bilješka 12. Priloga I.
([70]) Odjeljak III.6.h Priloga I.
([71]) Odjeljak III.6.a i bilješka 12. Priloga I. te odjeljak „Provjera zahtjeva za samocertificiranje" Priloga III.
([72]) Odjeljak „Provjera zahtjeva za samocertificiranje" Priloga III.
([73]) Slično tomu, Ministarstvo trgovine surađivat će s trećom stranom koja je čuvar sredstava prikupljenih naplatom naknade za rad odbora tijela za zaštitu podataka (vidjeti uvodnu izjavu 73.) kako bi provjerilo jesu li organizacije koje su kao neovisni mehanizam pravne zaštite odabrale tijela za zaštitu podataka platile naknadu za predmetnu godinu. Vidjeti odjeljak „Provjera zahtjeva za samocertificiranje" Priloga III.

(51) Ministarstvo trgovine obavijestit će organizacije da, ako žele biti (ponovno) certificirane, moraju riješiti sve probleme utvrđene u preispitivanju. Ako organizacije ne poduzmu mjere u roku koji je utvrdilo Ministarstvo trgovine (na primjer, u slučaju ponovnog certificiranja postupak bi trebao biti dovršen u roku od 45 dana) ([74]) ili na neki drugi način ne dovrše postupak certificiranja, smatrat će se da su odustale od prijave. U tom slučaju lažno prikazivanje sudjelovanja u okviru EU-a i SAD-a za privatnost podataka ili usklađenosti s okvirom može biti predmet provedbenih mjera FTC-a ili Ministarstva prometa ([75]).

(52) Radi pravilne primjene okvira EU-a i SAD-a za privatnost podataka zainteresirane strane, kao što su ispitanici, izvoznici podataka i nacionalna tijela za zaštitu podataka, moraju moći utvrditi koje se organizacije pridržavaju Načela. Kako bi postupak već na samom početku bio transparentan, Ministarstvo trgovine obvezalo se na vođenje i objavu popisa organizacija koje su certificirane da se pridržavaju Načela i u nadležnosti su najmanje jednog provedbenog tijela iz priloga IV. i V. ovoj Odluci ([76]). Ministarstvo trgovine ažurirat će taj popis na temelju godišnjih prijava organizacija za ponovno certificiranje i svaki put kad se organizacija povuče ili je isključena iz okvira EU-a i SAD-a za privatnost podataka. Osim toga, kako bi i s druge strane sve bilo transparentno, Ministarstvo trgovine vodit će i objavljivati evidenciju organizacija koje su uklonjene s popisa te za svaku navesti razlog zbog kojeg je uklonjena ([77]). Naposljetku, navest će poveznicu na internetsku stranicu FTC-a o okviru EU-a i SAD-a za privatnost podataka, na kojoj će biti popisane provedbene mjere koje FTC provodi u skladu s okvirom ([78]).

2.3.2. ***Praćenje usklađenosti***

(53) Ministarstvo trgovine kontinuirano će raznim mehanizmima pratiti postupaju li organizacije uključene u okvir EU-a i SAD-a za privatnost podataka stvarno u skladu s Načelima ([79]). Točnije, provodit će „terenske provjere" nasumično odabranih organizacija te ad hoc terenske provjere određenih organizacija kad se utvrde mogući problemi zbog neusklađenosti (npr. ako ih treće strane prijave Ministarstvu trgovine) kako bi provjerilo i. jesu li kontaktne točke za rješavanje pritužbi i zahtjeva ispitanika dostupne i odgovaraju li na njih, ii. je li politika zaštite privatnosti organizacije lako dostupna na njezinim internetskim stranicama i na poveznici na internetskim stranicama Ministarstva trgovine, iii. je li politika zaštite privatnosti organizacije i dalje u skladu sa zahtjevima za certificiranje te iv. je li neovisni mehanizam rješavanja sporova koji je organizacija odabrala dostupan za rješavanje pritužbi ([80]).

(54) Ako postoje uvjerljivi dokazi da organizacija ne ispunjava svoje obveze u skladu s okvirom EU-a i SAD-a za privatnost podataka (među ostalim ako Ministarstvo trgovine zaprimi pritužbe ili ako organizacija ne odgovori na njegove upite na zadovoljavajući način), Ministarstvo trgovine zahtijevat će od organizacije da ispuni i dostavi detaljni upitnik ([81]). Organizaciju koja na upitnik ne odgovori pravodobno i na zadovoljavajući način uputit će se nadležnom tijelu (FTC ili Ministarstvo prometa) radi mogućeg izricanja provedbene mjere ([82]). Neke od aktivnosti kojima je Ministarstvo trgovine nadziralo usklađenost u okviru sustava zaštite privatnosti bile su redovite terenske

([74]) Bilješka 2. Priloga III.
([75]) Vidjeti odjeljak „Provjera zahtjeva za samocertificiranje" Priloga III.
([76]) Informacije o upravljanju popisom organizacija uključenih u okvir za privatnost podataka mogu se pronaći u Prilogu III. (vidjeti uvod u odjeljku „Upravljanje programom za okvir za privatnost podataka i njegov nadzor koje provodi Ministarstvo trgovine") i Prilogu I. (odjeljci I.3, I.4, III.6.d i III.11.g).
([77]) Vidjeti uvod u odjeljku „Upravljanje programom za okvir za privatnost podataka i njegov nadzor koje provodi Ministarstvo trgovine" Priloga III.
([78]) Vidjeti odjeljak „Prilagođavanje internetskih stranica okvira za privatnost podataka ciljanoj publici" Priloga III.
([79]) Vidjeti odjeljak „Provedba periodičkih preispitivanja usklađenosti po službenoj dužnosti i ocjena programa za okvir za privatnost podataka" Priloga III.
([80]) Ministarstvo trgovine može na razne načine provoditi svoje nadzorne aktivnosti, npr. provjeravati funkcioniraju li poveznice na politike zaštite privatnosti ili aktivno pratiti navode li se u vijestima uvjerljivi dokazi o neusklađenosti.
([81]) Vidjeti odjeljak „Provedba periodičkih preispitivanja usklađenosti po službenoj dužnosti i ocjena programa za okvir za privatnost podataka" Priloga III.
([82]) Vidjeti odjeljak „Provedba periodičkih preispitivanja usklađenosti po službenoj dužnosti i ocjena programa za okvir za privatnost podataka" Priloga III.

provjere iz uvodne izjave 53. i neprekidno praćenje javnih izvješća na temelju kojih je moglo utvrditi, razmotriti i riješiti probleme zbog neusklađenosti ([83]). Organizacije koje ustrajno ne postupaju u skladu s Načelima uklonit će se s popisa organizacija uključenih u okvir za privatnost podataka te moraju vratiti ili izbrisati osobne podatke koje su primile u skladu s okvirom ([84]).

(55) U drugim slučajevima uklanjanja, kao što je dobrovoljno povlačenje iz sudjelovanja ili izostanak ponovnog certificiranja, organizacija mora izbrisati ili vratiti podatke ili ih smije čuvati ako svake godine Ministarstvu trgovine potvrdi da se obvezuje primjenjivati Načela odnosno ako osigura primjerenu zaštitu osobnih podataka drugim odobrenim sredstvima (npr. ugovorom koji je u potpunosti u skladu sa zahtjevima relevantnih standardnih ugovornih odredbi koje je odobrila Komisija) ([85]). U tom slučaju organizacija mora odrediti i kontaktnu točku za sva pitanja povezana s okvirom EU-a i SAD-a za privatnost podataka.

2.3.3. ***Utvrđivanje i suzbijanje lažnih izjava o sudjelovanju***

(56) Sve lažne izjave o sudjelovanju u okviru EU-a i SAD-a za privatnost podataka odnosno neprimjerenu uporabu certifikacijske oznake tog okvira Ministarstvo trgovine pratit će po službenoj dužnosti i na temelju pritužbi (npr. kad ih primi od tijela za zaštitu podataka) ([86]). Točnije, Ministarstvo trgovine kontinuirano će provjeravati jesu li organizacije i. koje se povuku iz sudjelovanja u okviru EU-a i SAD-a za privatnost podataka, ii. koje nisu dovršile godišnje ponovno certificiranje (tj. pokrenule su postupak, no nisu ga pravodobno dovršile ili ga uopće nisu pokrenule), iii. koje su uklonjene kao sudionik, prije svega zbog „ustrajne neusklađenosti", ili iv. koje nisu dovršile početno certificiranje (tj. pokrenule su postupak, no nisu ga pravodobno dovršile) iz objavljenih politika zaštite privatnosti uklonile sva relevantna upućivanja na okvir EU-a i SAD-a za privatnost podataka iz kojih bi se moglo zaključiti da organizacija aktivno sudjeluje u okviru ([87]). Ministarstvo trgovine pretraživat će i internet kako bi pronašlo upućivanja na okvir EU-a i SAD-a za privatnost podataka u politikama zaštite privatnosti organizacija, među ostalim radi pronalaska lažnih izjava organizacija koje nikad nisu sudjelovale u tom okviru ([88]).

(57) Ako Ministarstvo trgovine utvrdi da upućivanja na okvir EU-a i SAD-a za privatnost podataka nisu uklonjena ili se neprimjereno upotrebljavaju, obavijestit će organizaciju o mogućem upućivanju slučaja FTC-u ili Ministarstvu prometa ([89]). Ako organizacija ne odgovori na zadovoljavajući način, Ministarstvo trgovine uputit će predmet nadležnoj agenciji radi mogućeg izricanja provedbene mjere ([90]). Organizacija koja obmanjujućim izjavama ili praksom javnosti lažno prikazuje da se pridržava Načela podliježe provedbenim mjerama FTC-a, Ministarstva prometa ili drugih nadležnih američkih provedbenih tijela. Lažno prikazivanje Ministarstvu trgovine kažnjivo je u skladu sa Zakonom o davanju lažnog iskaza (False Statements Act, glava 18. članak 1001. Zakonika SAD-a).

([83]) U okviru drugog godišnjeg preispitivanja sustava zaštite privatnosti Ministarstvo trgovine izvijestilo je da je provelo terenske provjere 100 organizacija i poslalo upitnike o usklađenosti u 21 slučaju (nakon čega su ispravljeni otkriveni problemi), vidjeti radni dokument službi Komisije SWD(2018) 497 final, str. 9. Slično tomu, u okviru trećeg godišnjeg preispitivanja sustava zaštite privatnosti Ministarstvo trgovine izvijestilo je da je nadzorom javnih izvješća otkrilo tri slučaja neusklađenosti i da je počelo provoditi terenske provjere 30 poduzeća svaki mjesec, na temelju kojih je u 28 % slučajeva poslalo upitnike o usklađenosti (nakon čega su otkriveni problemi odmah ispravljeni ili, u tri slučaja, riješeni nakon pisma upozorenja), vidjeti radni dokument službi Komisije SWD(2019) 495 final, str. 8.

([84]) Odjeljak III.11.g Priloga I. Točnije, ustrajna neusklađenost nastaje kad organizacija odbija postupati u skladu s konačnom odlukom samoregulatornog tijela za zaštitu privatnosti, neovisnog tijela za rješavanje sporova ili provedbenog tijela.

([85]) Odjeljak III.6.f Priloga I.

([86]) Prilog III. odjeljak „Traženje i suzbijanje lažnih izjava o sudjelovanju".

([87]) Vidjeti prethodnu bilješku.

([88]) Vidjeti prethodnu bilješku.

([89]) Vidjeti prethodnu bilješku.

([90]) U okviru trećeg godišnjeg preispitivanja sustava zaštite privatnosti Ministarstvo trgovine izvijestilo je da je utvrdilo 669 slučajeva lažnih izjava o sudjelovanju (od listopada 2018. do listopada 2019.), od kojih je većina riješena nakon što je ministarstvo poslalo pismo upozorenja, dok ih je 143 upućeno FTC-u (vidjeti uvodnu izjavu 62.). Vidjeti radni dokument službi Komisije SWD(2019) 495 final, str. 10.

2.3.4. ***Izvršenje***

(58) Kako bi se u praksi osigurala primjerena razina zaštite podataka, trebalo bi uspostaviti neovisno nadzorno tijelo s ovlastima za praćenje i provedbu usklađenosti s pravilima o zaštiti podataka.

(59) Organizacije uključene u okvir EU-a i SAD-a za privatnost podataka moraju biti u nadležnosti američkih tijela koja imaju istražne i provedbene ovlasti potrebne da bi se stvarno osigurala usklađenost s Načelima, a to su FTC i Ministarstvo prometa ([91]).

(60) FTC je neovisno tijelo koje se sastoji od pet povjerenika koje imenuje predsjednik nakon što dobije savjete i suglasnost Senata ([92]). Povjerenici se imenuju na sedmogodišnji mandat i može ih razriješiti jedino predsjednik zbog neučinkovitog izvršavanja službenih obveza, zanemarivanja dužnosti ili zlouporabe položaja. U FTC-u najviše tri povjerenika smiju pripadati istoj političkoj stranci i povjerenici se tijekom mandata ne smiju baviti nikakvim drugim poslovnim djelatnostima i zanimanjima niti se zaposliti.

(61) FTC može istraživati usklađenost s Načelima i lažne izjave organizacija koje više nisu na popisu organizacija uključenih u okvir za privatnost podataka ili nikada nisu bile certificirane o tome da se pridržavaju Načela ili sudjeluju u okviru EU-a i SAD-a za privatnost podataka ([93]). FTC može osigurati usklađenost ishođenjem upravnih ili saveznih sudskih naloga (uključujući „ukaze o suglasnosti" donesene u postupcima nagodbe) ([94]) za prethodnu zabranu ili zabranu do okončanja postupka ili druga pravna sredstva te će sustavno pratiti izvršenje tih naloga ([95]). Ako organizacija ne postupi u skladu s tim nalozima, FTC može tražiti izricanje građanskopravnih sankcija i drugih pravnih sredstava, među ostalim za sve štete nastale nezakonitim postupanjem. Svaki ukaz o suglasnosti koji se izda organizaciji uključenoj u okvir EU-a i SAD-a za privatnost podataka morat će sadržavati odredbe o samoizvješćivanju ([96]), a organizacije će morati objaviti sve relevantne dijelove svojih izvješća o usklađenosti ili procjeni koja su podnijele FTC-u koji se odnose na okvir EU-a i SAD-a za privatnost podataka. Naposljetku, FTC će voditi internetski popis organizacija obuhvaćenih nalogom FTC-a ili sudskim nalogom u predmetima povezanima s okvirom EU-a i SAD-a za privatnost podataka ([97]).

(62) U okviru sustava zaštite privatnosti FTC je izrekao provedbene mjere u oko 22 slučaja zbog povreda određenih zahtjeva okvira (npr. organizacija nije potvrdila Ministarstvu trgovine da i dalje primjenjuje oblike zaštite u skladu sa sustavom zaštite privatnosti nakon što je napustila okvir, organizacija nije ni u okviru samoprocjene ni u okviru vanjskog preispitivanja usklađenosti provjerila postupa li u skladu s okvirom) ([98]) i zbog lažnih izjava o sudjelovanju u okviru (npr. izjave organizacija koje nisu dovršile korake potrebne za certificiranje ili koje su dopustile da im certifikat istekne, no lažno su prikazivale da i dalje sudjeluju u okviru) ([99]). Do tih provedbenih mjera došlo je, među ostalim, zbog proaktivne uporabe upravnih sudskih poziva za dobivanje dokumenata od određenih sudionika sustava zaštite privatnosti kako bi se provjerilo je li došlo do materijalnih povreda obveza iz sustava zaštite privatnosti ([100]).

([91]) Organizacija uključena u okvir EU-a i SAD-a za privatnost podataka mora javno izjaviti da se obvezala postupati u skladu s Načelima, objaviti svoje politike zaštite privatnosti u skladu s Načelima i u cijelosti ih provoditi. Neusklađenost je kažnjiva u skladu s člankom 5. Zakona o FTC-u, kojim se zabranjuje nepošteno i prijevarno postupanje u trgovini ili koje utječe na trgovinu (glava 15. članak 45. Zakonika SAD-a), i glavom 49. člankom 41712. Zakonika SAD-a, kojim se prijevozniku ili posredniku u prodaji karata zabranjuje nepoštena ili prijevarna praksa u zračnom prijevozu ili prodaji usluga zračnog prijevoza.

([92]) Glava 15. članak 41. Zakonika SAD-a.

([93]) Prilog IV.

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

([95]) Vidjeti odjeljak „Ishođenje i praćenje naloga" Priloga IV.

([96]) Nalozima FTC-a ili sudskim nalozima može se zahtijevati od poduzeća da provode programe zaštite privatnosti i redovito FTC-u omogućuju uvid u izvješća o usklađenosti ili neovisne ocjene tih programa koje provodi treća strana.

([97]) Odjeljak „Ishođenje i praćenje naloga" Priloga IV.

([98]) Radni dokument službi Komisije SWD(2019) 495 final, str. 11.

([99]) Vidjeti slučajeve navedene na internetskim stranicama FTC-a, dostupno na https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Vidjeti i radni dokument službi Komisije SWD(2017) 344 final, str. 17., radni dokument službi Komisije SWD(2018) 497 final, str. 12., i radni dokument službi Komisije SWD(2019) 495 final, str. 11.

([100]) Vidjeti npr. Pripremljene napomene predsjednika Josepha Simonsa na drugom godišnjem preispitivanju sustava zaštite privatnosti (ftc.gov).

(63) Općenitije, FTC je posljednjih godina poduzeo provedbene mjere u nizu predmeta koji su se odnosili na usklađenost s posebnim zahtjevima zaštite podataka koji su predviđeni i okvirom EU-a i SAD-a za privatnost podataka, na primjer u pogledu načela ograničavanja svrhe i čuvanja podataka ([101]), smanjenja količine podataka ([102]), sigurnosti podataka ([103]) i točnosti podataka ([104]).

(64) Ministarstvo prometa ima isključivu ovlast regulirati praksu zaštite privatnosti zračnih prijevoznika te s FTC-om dijeli nadležnost za praksu zaštite privatnosti posrednika u prodaji karata za usluge zračnog prijevoza. Službenici Ministarstva prometa prvo pokušavaju postići nagodbu, a ako to nije moguće, mogu pokrenuti provedbeni postupak koji uključuje izvođenje dokaza pred upravnim sucem Ministarstva prometa koji ima ovlast izdavati naloge za obustavu i građanskopravne sankcije ([105]). Neovisnost i nepristranost upravnih sudaca na razne je načine zaštićena Zakonom o upravnom postupku (Administrative Procedure Act – APA). Na primjer, može ih se razriješiti samo iz valjanih razloga, rotiraju se pri dodjeli predmeta, ne mogu obavljati dužnosti koje nisu u skladu s njihovim dužnostima i odgovornostima u svojstvu upravnog suca, ne može ih nadzirati istražni tim tijela koje ih zapošljava (u ovom slučaju Ministarstvo prometa) i moraju nepristrano izvršavati svoju pravosudnu/provedbenu funkciju ([106]). Ministarstvo prometa obvezalo se da će pratiti izvršenje provedbenih naloga i pobrinuti se za to da su nalozi doneseni u predmetima povezanima s okvirom EU-a i SAD-a za privatnost podataka dostupni na njegovim internetskim stranicama ([107]).

2.4. **Pravna zaštita**

(65) Kako bi se osigurala primjerena zaštita, a naročito ostvarivanje prava pojedinca, ispitaniku bi trebalo pružiti djelotvornu upravnu i sudsku zaštitu.

(66) Odbor za *pravne zaštite, provedbe i odgovornosti* iz okvira EU-a i SAD-a za privatnost podataka organizacije moraju osigurati pravnu zaštitu pojedinaca na koje utječe neusklađenost, a time i omogućiti ispitanicima iz Unije da podnose pritužbe zbog neusklađenosti organizacija uključenih u okvir EU-a i SAD-a za zaštitu podataka i da se te pritužbe rješavaju, prema potrebi odlukom o djelotvornom pravnom lijeku ([108]). U okviru certificiranja organizacije moraju ispuniti zahtjeve tog načela uspostavom djelotvornih i lako dostupnih neovisnih mehanizama pravne zaštite u okviru kojih se pritužbe i sporovi svakog pojedinca mogu istražiti i brzo riješiti bez naknade ([109]).

([101]) Vidjeti npr. nalog FTC-a u predmetu Drizly, LLC. kojim se od poduzeća zahtijevalo, među ostalim, 1. da uništi sve osobne podatke koje je prikupilo, a koji mu nisu potrebni za pružanje proizvoda ili usluga potrošačima, 2. da ne prikuplja niti pohranjuje osobne informacije osim ako je to potrebno za konkretne svrhe navedene u rasporedu čuvanja.

([102]) Vidjeti npr. nalog FTC-a u predmetu CafePress (24. ožujka 2022.) kojim se zahtijevalo, među ostalim, da se što više smanji količina prikupljanih podataka.

([103]) Vidjeti npr. FTC-ove provedbene mjere u predmetima Drizly, LLC i CafePress kojima se od predmetnih poduzeća zahtijevalo da uspostave namjenski sigurnosni program ili posebne sigurnosne mjere. Osim toga, kad je riječ o povredama podataka, vidjeti i nalog FTC-a od 27. siječnja 2023. u predmetu Chegg, nagodbu postignutu s društvom Equifax 2019. (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Vidjeti npr. predmet RealPage, Inc (16. listopada 2018.), u kojem je FTC u skladu sa Zakonom o poštenom izvješćivanju o kreditnoj sposobnosti poduzeo provedbene mjere protiv poduzeća za provjeru najmoprimaca koje je vlasnicima nekretnina i poduzećima za upravljanje nekretninama dostavljalo izvješća o pojedincima koja su pripremljena na temelju informacija iz izvješćâ o dosadašnjem najmoprimstvu i javnih evidencija (uključujući povijest kaznenih djela i deložacija) te kreditnih informacija i koja su uzeta u obzir pri donošenju odluke o tome jesu li ispunjeni uvjeti za najmoprimstvo. FTC je utvrdio da poduzeće nije poduzelo razumne mjere kako bi osiguralo točnost informacija koje je dostavilo služeći se svojim alatom za automatizirano donošenje odluka.

([105]) Vidjeti odjeljak „Provedbena praksa” Priloga V.

([106]) Vidjeti glavu 5. članak 3105., članak 7521. točku (a), članak 554. točku (d) i članak 556. točku (b)(3) Zakonika SAD-a.

([107]) Vidjeti odjeljak „Praćenje i objava provedbenih naloga koji se odnose na povrede okvira EU-a i SAD-a za privatnost podataka” Priloga V.

([108]) Odjeljak II.7 Priloga I.

([109]) Odjeljak III.11 Priloga I.

(67) Organizacije mogu odabrati neovisne mehanizme pravne zaštite u Uniji ili u SAD-u. Kako je detaljnije objašnjeno u uvodnoj izjavi 73., to uključuje mogućnost da se dobrovoljno obvežu na suradnju s tijelima za zaštitu podataka iz EU-a. Ako organizacije obrađuju podatke o ljudskim resursima, obvezne su surađivati s tijelima za zaštitu podataka iz EU-a. 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 sadržavati djelotvorne provedbene mehanizme u skladu sa zahtjevima *načela pravne zaštite, provedbe i odgovornosti*.

(68) Stoga su u okviru EU-a i SAD-a za privatnost podataka ispitanicima dostupne razne mogućnosti za ostvarenje njihovih prava, podnošenje pritužbi zbog neusklađenosti organizacija uključenih u okvir i rješavanje njihovih pritužbi, prema potrebi odlukom o djelotvornom pravnom lijeku. Pojedinci mogu podnijeti pritužbu izravno organizaciji, neovisnom tijelu za rješavanje sporova koje odredi organizacija, nacionalnim tijelima za zaštitu podataka, Ministarstvu trgovine ili FTC-u. Ako se njihove pritužbe ne riješe nijednim od tih mehanizama pravne zaštite ili provedbenih mehanizama, pojedinci imaju pravo zatražiti i obvezujuću arbitražu (Prilog I. uz Prilog I. ovoj Odluci). Osim arbitražnog odbora, čija se intervencija može zatražiti tek nakon što se iscrpe određena pravna sredstva, pojedinci se mogu poslužiti bilo kojim ili svim mehanizmima pravne zaštite po svojem izboru i ne moraju odabrati samo jedan ili pratiti poseban redoslijed.

(69) Prvo, ispitanici iz Unije mogu tražiti rješavanje slučajeva neusklađenosti s Načelima izravnim obraćanjem organizacijama uključenima u okvir EU-a i SAD-a za privatnost podataka ([110]). Kako bi olakšala rješavanje, organizacija mora uspostaviti djelotvoran 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 odabranom neovisnom tijelu za rješavanje sporova (vidjeti uvodnu izjavu 70.). Organizacija mora odgovoriti ispitaniku iz Unije u roku od 45 dana od primitka pritužbe izravno od pojedinca ili preko Ministarstva trgovine kojem je pritužbu uputilo tijelo za zaštitu podataka ([111]). Slično tomu, organizacije moraju brzo odgovoriti na upite i druge zahtjeve za informacije Ministarstva trgovine ili tijela za zaštitu podataka ([112]) (ako se organizacija obvezala surađivati s tijelom za zaštitu podataka) koji se odnose njihovo pridržavanje Načela.

(70) Drugo, pojedinci mogu podnijeti pritužbu izravno neovisnom tijelu za rješavanje sporova (u SAD-u ili Uniji) koje organizacija odredi za istragu i rješavanje pojedinačnih pritužbi (osim ako su očito neutemeljene ili neosnovane) te za pružanje odgovarajuće besplatne pravne zaštite pojedincu ([113]). Sankcije i pravna sredstva koje odredi takvo tijelo moraju biti dovoljno strogi da se njima osigura usklađenost organizacija s Načelima te bi trebali dovesti do toga da organizacija poništi ili ispravi učinke neusklađenosti i, ovisno o okolnostima, prekine daljnju obradu predmetnih osobnih podataka i/ili ih izbriše te objavi informacije o utvrđenoj neusklađenosti ([114]). Neovisna tijela za rješavanje sporova koje odredi organizacija moraju na svojim javnim internetskim stranicama navesti informacije o okviru EU-a i SAD-a za privatnost podataka i usluge koje pružaju na temelju njega ([115]). Svake godine moraju objaviti godišnje izvješće s agregiranim statističkim podacima o tim uslugama ([116]).

([110]) Odjeljak III.11.d.i Priloga I.
([111]) Odjeljak III.11.d.i Priloga I.
([112]) To je tijelo za rješavanje pritužbi koje je odredio odbor tijela za zaštitu podataka u skladu s dodatnim načelom o ulozi tijela za zaštitu podataka (odjeljak III.5 Priloga I.).
([113]) Odjeljak III.11.d Priloga I.
([114]) Odjeljci II.7 i III.11.e Priloga I.
([115]) Odjeljak III.11.d.ii Priloga I.
([116]) Godišnje izvješće mora sadržavati sljedeće informacije: 1. ukupan broj pritužbi koje se odnose na okvir EU-a i SAD-a za privatnost podataka zaprimljenih u izvještajnoj godini, 2. vrste zaprimljenih pritužbi, 3. mjere za osiguranje kvalitete rješavanja sporova, kao što je trajanje obrade pritužbi, i 4. ishode zaprimljenih pritužbi, posebno broj i vrstu pravnih sredstava ili izrečenih sankcija.

(71) U okviru preispitivanja usklađenosti Ministarstvo trgovine može provjeriti jesu li organizacije uključene u okvir EU-a i SAD-a za privatnost podataka doista registrirane u okviru neovisnih mehanizama pravne zaštite u skladu sa svojim izjavama ([117]). Organizacije i odgovorni neovisni mehanizmi pravne zaštite moraju brzo odgovoriti na upite i zahtjeve Ministarstva trgovine za informacije povezane s tim okvirom. Ministarstvo trgovine surađivat će s neovisnim mehanizmima pravne zaštite kako bi provjerilo jesu li ti mehanizmi na svojim internetskim stranicama naveli informacije o Načelima i uslugama koje pružaju u skladu s okvirom te objavljuju li godišnja izvješća ([118]).

(72) Ako organizacija ne postupi u skladu s odlukom tijela za rješavanje sporova ili samoregulatornog tijela, to tijelo mora o tome obavijestiti Ministarstvo trgovine i FTC (ili drugo američko tijelo nadležno za istragu neusklađenosti organizacije) ili nadležni sud ([119]). Ako organizacija odbije postupiti u skladu s konačnom odlukom samoregulatornog tijela za zaštitu privatnosti, neovisnog tijela za rješavanje sporova ili vladina tijela ili ako takvo tijelo utvrdi da organizacija često ne postupa u skladu s Načelima, to se može smatrati ustrajnom neusklađenosti, u kojem će slučaju Ministarstvo trgovine, nakon što joj da rok od 30 dana i priliku za odgovor, organizaciju koja ne postupa u skladu s Načelima ukloniti s popisa organizacija uključenih u okvir za privatnost podataka ([120]). Ako, nakon što je se ukloni s popisa, organizacija i dalje izjavljuje da je certificirana u skladu s okvirom EU-a i SAD-a za privatnost podataka, Ministarstvo trgovine uputit će je FTC-u ili drugoj provedbenoj agenciji ([121]).

(73) Treće, pojedinci mogu podnijeti pritužbe i nacionalnom tijelu za zaštitu podataka u Uniji, koje može iskoristiti svoje istražne i korektivne ovlasti na temelju Uredbe (EU) 2016/679. Organizacije su dužne surađivati s tijelima za zaštitu podataka pri istrazi i rješavanju pritužbi ako se one odnose na obradu podataka o ljudskim resursima prikupljenih u kontekstu radnog odnosa ili ako se predmetna organizacija dobrovoljno podvrgnula nadzoru tijela za zaštitu podataka ([122]). Organizacije prije svega moraju odgovarati na upite, postupati u skladu sa savjetima tijela za zaštitu podataka, među ostalim o korektivnim ili kompenzacijskim mjerama, i dostaviti tijelu za zaštitu podataka pisanu potvrdu da su te mjere poduzete ([123]). Slučajeve nepostupanja u skladu s njegovim savjetom tijelo za zaštitu podataka upućuje Ministarstvu trgovine (koje može organizacije ukloniti s popisa organizacija uključenih u okvir EU-a i SAD-a za privatnost podataka) odnosno FTC-u ili Ministarstvu prometa, koji mogu naložiti provedbene mjere (nesuradnja s tijelima za zaštitu podataka i neusklađenost s Načelima kažnjivi su u američkom pravu) ([124]).

(74) Kako bi se olakšala suradnja radi djelotvornog rješavanja pritužbi, i Ministarstvo trgovine i FTC uspostavili su posebnu kontaktnu točku koja je odgovorna za izravnu komunikaciju s tijelima za zaštitu podataka ([125]). Te kontaktne točke pomažu tijelima za zaštitu podataka s upitima o usklađenosti organizacije s Načelima.

(75) Tijelo za zaštitu podataka izdaje savjet ([126]) nakon što su obje stranke u sporu imale razumnu mogućnost iznijeti primjedbe i dostaviti dokaze. Odbor može dati savjet čim to bude moguće u skladu s propisanim postupkom, u pravilu u roku od 60 dana od primitka pritužbe ([127]). Ako organizacija ne postupi u skladu sa savjetom u roku od 25 dana od njegova primitka i ne ponudi prihvatljivo objašnjenje za kašnjenje, odbor može poslati obavijest o svojoj namjeri da proslijedi predmet FTC-u (ili drugom nadležnom američkom provedbenom tijelu) ili da zaključi da je došlo do teškog kršenja obveze suradnje. U prvom slučaju to može dovesti do izricanja provedbene mjere u

([117]) Odjeljak „Provjera zahtjeva za samocertificiranje” Priloga I.

([118]) Vidjeti odjeljak „Olakšavanje suradnje s tijelima za alternativno rješavanje sporova koja pružaju usluge povezane s Načelima” Priloga III. Vidjeti i odjeljak III.11.d.ii–iii Priloga I.

([119]) Vidjeti odjeljak III.11.e Priloga I.

([120]) Vidjeti odjeljak III.11.g Priloga I., posebno točke ii. i iii.

([121]) Vidjeti odjeljak „Traženje i suzbijanje lažnih izjava o sudjelovanju” Priloga III.

([122]) Odjeljak II.7.b Priloga I.

([123]) Odjeljak III.5 Priloga I.

([124]) Odjeljak III.5.c.ii Priloga I.

([125]) Prilog III. (vidjeti odjeljak „Olakšavanje suradnje s tijelima za zaštitu podataka”) i Prilog IV. (vidjeti odjeljke „Davanje prednosti upućenim predmetima i istrage” i „Suradnja u području provedbe s tijelima za zaštitu podataka iz EU-a”).

([126]) Tijela za zaštitu podataka trebala bi na temelju svoje nadležnosti za organizaciju svojeg rada i međusobnu suradnju izraditi poslovnik svojeg neslužbenog odbora.

([127]) Odjeljak III.5.c.i Priloga I.

skladu s člankom 5. Zakona o FTC-u (ili sličnim zakonom) ([128]). U drugom slučaju odbor će obavijestiti Ministarstvo trgovine, koje će odbijanje organizacije da postupi u skladu sa savjetom odbora tijela za zaštitu podataka smatrati ustrajnom neusklađenosti, što će dovesti do uklanjanja organizacije s popisa organizacija uključenih u okvir za privatnost podataka.

(76) Ako tijelo za zaštitu podataka kojem je upućena pritužba nije poduzelo mjere za njezino rješavanje ili te mjere nisu dovoljne, podnositelj pritužbe može zbog takvog (ne)postupanja pokrenuti postupak pred nacionalnim sudovima nadležne države članice EU-a.

(77) Pojedinci mogu podnijeti pritužbe tijelima za zaštitu podataka čak i ako organizacija nije odredila njihov odbor kao tijelo za rješavanje sporova. U tim slučajevima tijelo za zaštitu podataka takve pritužbe može uputiti Ministarstvu trgovine ili FTC-u. Radi lakše i bolje suradnje na pitanjima povezanima s pojedinačnim pritužbama i neusklađenosti organizacija uključenih u okvir EU-a i SAD-a za privatnost podataka Ministarstvo trgovine uspostavit će posebnu kontaktnu točku za komunikaciju koja će pomagati s upitima tijela za zaštitu podataka o usklađenosti organizacije s Načelima ([129]). Slično tomu, FTC se obvezao na uspostavljanje posebne kontaktne točke ([130]).

(78) Četvrto, Ministarstvo trgovine obvezalo se da će primati i preispitivati pritužbe zbog neusklađenosti organizacija s Načelima te učiniti sve što može da ih riješi ([131]). U tu svrhu Ministarstvo trgovine ima uspostavljene posebne postupke kojima tijela za zaštitu podataka upućuju pritužbe posebnoj kontaktnoj točki, prate ih i dodatno komuniciraju s organizacijama radi lakšeg rješavanja pritužbi ([132]). Kako bi se ubrzala obrada pojedinačnih pritužbi, kontaktna točka izravno komunicira s nadležnim tijelom za zaštitu podataka o problemima zbog neusklađenosti, a posebno ga informira o statusu pritužbi u roku od najviše 90 dana od upućivanja ([133]). To ispitanicima omogućuje da pritužbe zbog neusklađenosti organizacija uključenih u okvir EU-a i SAD-a za privatnost podataka podnesu izravno svojim nacionalnim tijelima za zaštitu podataka i da ih se proslijedi Ministarstvu trgovine kao američkom tijelu koje upravlja

(79) Ako na temelju provjera po službenoj dužnosti, pritužbi ili bilo kojih drugih informacija Ministarstvo trgovine zaključi da organizacija ustrajno ne postupa u skladu s Načelima, može je ukloniti s popisa organizacija uključenih u okvir za privatnost podataka ([134]). Odbijanje postupanja u skladu s konačnom odlukom samoregulatornog tijela za zaštitu privatnosti, neovisnog tijela za rješavanje sporova ili vladina tijela, uključujući tijelo za zaštitu privatnosti, smatrat će se ustrajnom neusklađenosti ([135]).

(80) Peto, organizacija uključena u okvir EU-a i SAD-a za privatnost podataka mora biti u nadležnosti američkih tijela, osobito FTC-a ([136]), koja imaju istražne i provedbene ovlasti potrebne da bi se stvarno osigurala usklađenost s Načelima. FTC daje prednost razmatranju predmeta o neusklađenosti s Načelima koje su mu uputila neovisna tijela za rješavanje sporova ili samoregulatorna tijela, Ministarstvo trgovine i tijela za zaštitu podataka (na vlastitu inicijativu ili na temelju pritužbi) kako bi utvrdio je li došlo do povrede članka 5. Zakona o FTC-u ([137]). FTC se obvezao uspostaviti standardizirani postupak upućivanja predmeta, odrediti kontaktnu točku kojoj tijela za zaštitu podataka mogu upućivati predmete i razmjenjivati informacije o upućenim predmetima. Osim toga, pritužbe može prihvaćati izravno od pojedinaca i na vlastitu inicijativu pokretati istrage povezane s okvirom EU-a i SAD-a za privatnost podataka, osobito u okviru svojih istraga problema povezanih sa zaštitom privatnosti

([128]) Odjeljak III.5.c.ii Priloga I.
([129]) Vidjeti odjeljak „Olakšavanje suradnje s tijelima za zaštitu podataka” Priloga III.
([130]) Vidjeti odjeljke „Davanje prednosti upućenim predmetima i istrage” i „Suradnja u području provedbe s tijelima za zaštitu podataka iz EU-a” Priloga IV.
([131]) Vidjeti npr. odjeljak „Olakšavanje suradnje s tijelima za zaštitu podataka” Priloga III.
([132]) Odjeljak II.7.e Priloga I. i odjeljak „Olakšavanje suradnje s tijelima za zaštitu podataka” Priloga III.
([133]) Vidjeti prethodnu bilješku.
([134]) Odjeljak III.11.g Priloga I.
([135]) Odjeljak III.11.g Priloga I.
([136]) Organizacija uključena u okvir EU-a i SAD-a za privatnost podataka mora javno izjaviti da se obvezala postupati u skladu s Načelima, objaviti svoje politike zaštite privatnosti u skladu s Načelima i u cijelosti ih provoditi. Neusklađenost je kažnjiva u skladu s člankom 5. Zakona o FTC-u, kojim se zabranjuje nepošteno i prijevarno postupanje u trgovini ili koje utječe na trgovinu.
([137]) Vidjeti i slične obveze Ministarstva prometa, Prilog V.

(81) Šesto, kao posljednji mehanizam pravne zaštite koji se upotrebljava samo ako se drugim dostupnim oblicima pravne zaštite pritužba pojedinca ne riješi na zadovoljavajući način, ispitanik iz Unije može zatražiti obvezujuću arbitražu pred Odborom za okvir EU-a i SAD-a za privatnost podataka ([138]). Organizacija mora obavijestiti pojedince o mogućnosti da zatraže obvezujuću arbitražu te su, odabere li pojedinac tu mogućnost, dužne odgovoriti slanjem obavijesti predmetnoj organizaciji ([139]).

(82) Odbor za okvir EU-a i SAD-a za privatnost podataka sastoji se od najmanje deset arbitara koje će imenovati Ministarstvo trgovine i Komisija na temelju njihove neovisnosti, integriteta i iskustva u području američkog prava o zaštiti privatnosti i Unijina prava o zaštiti podataka. Za svaki pojedini spor stranke biraju jednog ili tri ([140]) arbitra iz te skupine.

(83) Ministarstvo trgovine odabralo je Međunarodni centar za rješavanje sporova (ICDR), međunarodni odjel Američkog udruženja za arbitražu (AAA), za vođenje arbitraža. Postupci pred Odborom za okvir EU-a i SAD-a za privatnost podataka bit će uređeni nizom usuglašenih pravila arbitraže i kodeksom ponašanja imenovanih arbitara. Na internetskim stranicama Međunarodnog centra za rješavanje sporova Američkog udruženja za arbitražu navedene su jasne i sažete informacije za pojedince o mehanizmu arbitraže i postupku za pokretanje arbitraže.

(84) Pravila arbitraže koja usuglase Ministarstvo prometa i Komisija dopunjuju okvir EU-a i SAD-a za privatnost podataka čijih nekoliko značajki povećava dostupnost tog mehanizma ispitanicima iz Unije: i. pri pripremi zahtjeva za odbor ispitaniku smije pomoći njegovo nacionalno tijelo za zaštitu podataka, ii. arbitraža će se odvijati u SAD-u, ali ispitanici iz Unije mogu odlučiti sudjelovati videokonferencijom ili telefonskom konferencijom, što će im se besplatno omogućiti, iii. jezik na kojem će se odvijati arbitraža u pravilu će biti engleski, ali će se pri arbitražnom saslušanju ispitaniku na obrazložen zahtjev u načelu pružiti besplatna usluga prevođenja, iv. naposljetku, iako svaka stranka mora snositi vlastite odvjetničke troškove, ako stranku pred odborom zastupa odvjetnik, Ministarstvo trgovine vodit će fond u koji organizacije uključene u okvir EU-a i SAD-a za privatnost podataka svake godine uplaćuju doprinose i iz kojeg se pokrivaju troškovi arbitražnog postupka do najvećeg iznosa koji odrede američka tijela u dogovoru s Komisijom ([141]).

(85) Odbor za okvir EU-a i SAD-a za privatnost podataka ima ovlasti odrediti pojedinačnu nenovčanu pravičnu naknadu ([142]) potrebnu da bi se ispravila neusklađenost s Načelima. Iako odbor pri donošenju odluke uzima u obzir druga pravna sredstva već iskorištena u okviru drugih mehanizama uključenih u okvir EU-a i SAD-a za privatnost podataka, pojedinci ipak mogu pokrenuti arbitražu ako smatraju da ta druga pravna sredstva nisu dostatna. To ispitanicima iz Unije omogućuje da zatraže arbitražu svaki put kad postupanjem ili nepostupanjem organizacija uključenih u okvir EU-a i SAD-a za privatnost podataka, neovisnih mehanizama pravne zaštite ili nadležnih američkih tijela (npr. FTC) nisu na zadovoljavajući način riješene njihove pritužbe. Arbitraža se ne može zatražiti ako tijelo za zaštitu podataka ima pravne ovlasti riješiti predmetnu pritužbu na rad organizacije uključene u okvir EU-a i SAD-a za privatnost podataka, odnosno u slučajevima u kojima je organizacija obvezna ili se dobrovoljno obvezala surađivati i postupati u skladu sa savjetima tijela za zaštitu podataka o obradi podataka o ljudskim resursima prikupljenih u kontekstu radnog odnosa. Pojedinci mogu zatražiti provedbu arbitražne odluke pred američkim sudovima u skladu sa Saveznim zakonom o arbitraži (Federal Arbitration Act), čime im je osigurano pravno sredstvo ako organizacija ne postupi u skladu sa savjetima.

([138]) Vidjeti Prilog I. „Model arbitraže" uz Prilog I.
([139]) Vidjeti odjeljke II.1.a.xi i II.7.c Priloga I.
([140]) Stranke se dogovaraju i o broju arbitara u Odboru.
([141]) Odjeljak G.6 Priloga I. uz Prilog I.
([142]) Pojedinci ne mogu u arbitražnom postupku tražiti naknadu štete, ali pokretanjem tog postupka ne gubi se mogućnost traženja naknade štete na redovnim američkim sudovima.

(86) Sedmo, ako organizacija ne ispunjava svoju obvezu da poštuje Načela i objavljenu politiku zaštite privatnosti, u američkom pravu predviđeni su dodatni oblici sudske zaštite, među ostalim za naknadu štete. Na primjer, pojedinci u određenim okolnostima mogu ostvariti sudsku zaštitu (uključujući naknadu štete) u skladu s državnim potrošačkim zakonima u slučaju lažnog prikazivanja, nepoštenog ili prijevarnog postupanja ili prakse ([143]) i u skladu s odštetnim pravom (osobito u slučaju štetnih radnji zadiranja u privatni život ([144]), prisvajanja imena ili lika ([145]) i javnog objavljivanja privatnih činjenica ([146])).

(87) Opisanim oblicima pravne zaštite osigurava se učinkovito rješavanje svih pritužbi na neusklađenost certificiranih organizacija s okvirom EU-a i SAD-a za privatnost podataka, kao i učinkovito ispravljanje te neusklađenosti.

3. PRISTUP JAVNIH TIJELA U SAD-u OSOBNIM PODACIMA PRENESENIMA IZ EUROPSKE UNIJE I NJIHOVA UPORABA

(88) Komisija je ocijenila i ograničenja i zaštitne mjere, uključujući mehanizme za nadzor i pravnu zaštitu pojedinaca dostupne u pravu SAD-a u vezi s osobnim podacima prenesenima voditeljima i izvršiteljima obrade u SAD-u koje američka javna tijela prikupljaju i naknadno upotrebljavaju zbog javnog interesa, osobito u svrhe kaznenog progona i nacionalne sigurnosti (vladin pristup) ([147]). Pri ocjenjivanju ispunjavaju li uvjeti pod kojima je vladi omogućen pristup podacima prenesenima u SAD u skladu s ovom Odlukom test „načelne istovjetnosti" u skladu s člankom 45. stavkom 1. Uredbe (EU) 2016/679, kako je tumači Sud s obzirom na Povelju o temeljnim pravima, Komisija je uzela u obzir nekoliko kriterija.

(89) Svako ograničenje prava na zaštitu osobnih podataka mora biti predviđeno zakonom, a u samoj se pravnoj osnovi kojom se dopušta zadiranje u takvo pravo mora utvrditi doseg ograničenja ostvarivanja predmetnog prava ([148]). Nadalje, da bi se ispunio zahtjev proporcionalnosti, prema kojem se odstupanja od zaštite osobnih podataka i ograničenja te zaštite u demokratskom društvu moraju primjenjivati samo ako je to nužno za ostvarenje specifičnih ciljeva od općeg interesa koji su jednakovrijedni onima koje priznaje Unija, u toj pravnoj osnovi moraju biti utvrđena jasna i precizna pravila o dosegu i primjeni predmetnih mjera i moraju se uvesti minimalne zaštitne mjere tako da osobe čiji su podaci preneseni raspolažu dostatnim jamstvima koja omogućuju djelotvornu zaštitu njihovih osobnih podataka od rizika zlouporabe ([149]). Osim toga, ta pravila i zaštitne mjere moraju biti pravno obvezujući i

([143]) Vidjeti npr. zakone o zaštiti potrošača Kalifornije (članci od 1750. do 1785. Građanskog zakonika Kalifornije (West) – Zakon o pravnim sredstvima za potrošače), Okruga Columbije (članak 28-3901. Zakonika Okruga Columbije), Floride (članci od 501.201. do 501.213. Zakonika Floride – Zakon o prijevarnoj i nepoštenoj trgovinskoj praksi), Illinoisa (glava 815. članci od 505/1 do 505/12 Zakonika Illinoisa – Zakon o prijevari potrošača i prijevarnoj poslovnoj praksi), Pennsylvanije (glava 73. članci od 201-1 do 201-9.3 Zakonika Pennsylvanije s komentarima (West) – Zakon o nepoštenoj trgovinskoj praksi i zaštiti potrošača).

([144]) Tj. u slučaju namjernog uplitanja u privatne poslove ili interese pojedinca na način koji bi razumna osoba smatrala izrazito uvredljivim (članak 652.(b) u 2. izdanju Kodifikacije odštetnog prava).

([145]) Ta štetna radnja obično se odnosi na prisvajanje i uporabu imena ili lika nekog pojedinca u svrhe oglašavanja poduzeća ili proizvoda ili u sličnu komercijalnu svrhu (vidjeti članak 652.C u 2. izdanju Kodifikacije odštetnog prava).

([146]) Tj. objavljivanje informacija o privatnom životu pojedinca, pri čemu razumna osoba to smatra izrazito uvredljivim, a informacije nisu od legitimnog interesa za javnost (članak 652.D u 2. izdanju Kodifikacije odštetnog prava).

([147]) To je bitno i s obzirom na odjeljak I.5 Priloga I. U skladu s tim odjeljkom i slično kao u Općoj uredbi o zaštiti podataka postupanje u skladu sa zahtjevima zaštite podataka i pravima na zaštitu podataka koja su dio Načela zaštite privatnosti može podlijegati ograničenjima. No takva ograničenja nisu apsolutna, nego se na njih može pozvati samo pod nekoliko uvjeta, na primjer u mjeri koja je nužna da se postupi u skladu sa sudskim nalogom ili ispune zahtjevi u pogledu javnog interesa, kaznenog progona ili nacionalne sigurnosti. U tom kontekstu i radi jasnoće u tom se odjeljku upućuje i na uvjete utvrđene u Izvršnom nalogu br. 14086 koji su ocijenjeni među ostalim u uvodnim izjavama 127.–141.

([148]) Vidjeti predmet *Schrems II*, t. 174. i 175. te navedenu sudsku praksu. Kad je riječ o pristupu javnih tijela država članica, vidjeti i predmet C-623/17 *Privacy International*, ECLI:EU:C:2020:790, t. 65., i spojene predmete C-511/18, C-512/18 i C-520/18, *La Quadrature du Net i dr.*, ECLI:EU:C:2020:791, t. 175.

([149]) Vidjeti predmet *Schrems II*, t. 176. i 181. te navedenu sudsku praksu. Kad je riječ o pristupu javnih tijela država članica, vidjeti i predmete *Privacy International*, t. 68., i *La Quadrature du Net i dr.*, t. 132.

pojedinci moraju moći tražiti ostvarenje svojeg prava na njih ([150]). Točnije, ispitanici moraju imati mogućnost pokretanja postupka pred neovisnim i nepristranim sudom radi pristupa svojim osobnim podacima ili njihova ispravka ili brisanja ([151]).

3.1. **Pristup američkih javnih tijela podacima i njihova uporaba u svrhe kaznenog progona**

(90) Kad je riječ o zadiranju u osobne podatke koji se u skladu s okvirom EU-a i SAD-a za privatnost podataka prenose u svrhe kaznenog progona, pravom SAD-a propisan je niz ograničenja pristupa osobnim podacima i njihove uporabe te su predviđeni mehanizmi nadzora i pravne zaštite koji su u skladu sa zahtjevima iz uvodne izjave 89. ove Odluke. Uvjeti pod kojima je takav pristup moguć i zaštitne mjere koje se primjenjuju na upotrebu tih ovlasti detaljno se ocjenjuju u odjeljcima u nastavku. U tom je pogledu američka vlada (odnosno Ministarstvo pravosuđa) dala jamstva o primjenjivim ograničenjima i zaštitnim mjerama (Prilog VI. ovoj Odluci).

3.1.1. ***Pravne osnove, ograničenja i zaštitne mjere***

3.1.1.1. *Ograničenja i zaštitne mjere pri prikupljanju osobnih podataka u svrhe kaznenog progona*

(91) Da bi u svrhe kaznenog progona pristupili osobnim podacima koje obrađuju certificirane američke organizacije, a koji bi se prenosili iz Unije na temelju okvira EU-a i SAD-a za privatnost podataka, američki savezni tužitelji i savezni agenti provode drukčije postupke, kako je detaljnije objašnjeno u uvodnim izjavama od 92. do 99. Isti se postupci provode i kad se informacije prikupljaju od bilo koje američke organizacije neovisno o državljanstvu ili boravištu dotičnih ispitanika ([152]).

(92) Prvo, na zahtjev službenika saveznog tijela kaznenog progona ili odvjetnika u ime vlade sudac može izdati nalog za pretragu ili zapljenu (među ostalim i elektronički pohranjenih podataka) ([153]). Takav nalog može se izdati samo ako postoji „osnovana sumnja" ([154]) da se „zapljenjivi predmeti" (dokazi o kaznenom djelu, predmeti u nezakonitom posjedu ili imovina koja je osmišljena, predviđena ili se upotrebljava za počinjenje kaznenog djela) vjerojatno nalaze na mjestu navedenom u nalogu. U nalogu mora biti navedena imovina ili predmet koji će se zaplijeniti te sudac kojem se nalog mora vratiti. Osoba koja je predmet pretrage ili čija je imovina predmet pretrage može podnijeti

([150]) Vidjeti predmet *Schrems II*, t. 181. i 182.

([151]) Vidjeti predmete *Schrems I*, t. 95., i *Schrems II*, t. 194. Sud je u tom pogledu posebno istaknuo da poštovanje članka 47. Povelje o temeljnim pravima, u kojem se jamči pravo na djelotvoran pravni lijek pred neovisnim i nepristranim sudom, „pridonosi razini zaštite koja se zahtijeva u okviru Unije [i to poštovanje] mora utvrditi Komisija prije nego što donese odluku o primjerenosti na temelju članka 45. stavka 1. [Uredbe (EU) 2016/679]" (*Schrems II*, t. 186.).

([152]) Vidjeti Prilog VI. Kad je riječ o Zakonu o prisluškivanju (Wiretap Act), Zakonu o pohranjenoj komunikaciji (Stored Communications Act) i Zakonu o uređajima za bilježenje izlaznih poziva (Pen Register Act) (detaljnije opisani u uvodnim izjavama od 95. do 98.), vidjeti npr. predmet *Suzlon Energy Ltd protiv Microsoft Corp., 671 F.3d 726, 729* (9. okrug, 2011.).

([153]) Savezni propisi o kaznenom postupku, Propis br. 41. Vrhovni sud potvrdio je u presudi iz 2018. da se nalog za pretragu odnosno izuzeće od izdavanja naloga mora izdati kako bi tijela kaznenog progona mogla pristupiti povijesnim podacima o lokaciji baznih stanica, koji omogućuju potpun pregled korisnikova kretanja, i da korisnik može razumno očekivati da su takve informacije privatne (*Timothy Ivory Carpenter protiv Sjedinjenih Američkih Država*, br. predmeta: 16-402, 585 U.S. Zbog toga se ti podaci u pravilu ne mogu dobiti od mobilnih operatera na temelju sudskog naloga koji je izdan na osnovi opravdane pretpostavke da su te informacije relevantne i bitne za istragu u kaznenom postupku koja je u tijeku, već je za uporabu naloga potrebno dokazati postojanje osnovane sumnje.

([154]) Prema Vrhovnom sudu „osnovana sumnja" je „praktičan, netehnički" standard koji se temelji na „činjeničnim i praktičnim razmatranjima svakodnevnog života na temelju kojih postupaju razumne i razborite osobe […]" (*Illinois protiv Gatesa*, 462 U.S. 213, 232 (1983.)). Osnovana sumnja za nalog za pretragu postoji ako postoji velika vjerojatnost da će se pretragom otkriti dokazi o kaznenom djelu (vidjeti prethodno upućivanje).

prijedlog za odbijanje izvođenja dokaza pribavljenih nezakonitom pretragom ili izvedenih na temelju takve pretrage ako se ti dokazi iznesu protiv te osobe u kaznenom postupku ([155]). Kad je dužan otkriti podatke na temelju naloga, nositelj podataka (npr. poduzeće) obvezu otkrivanja ponajprije može osporavati kao prekomjerno opterećenje ([156]).

(93) Drugo, u slučaju istraga određenih teških kaznenih djela ([157]), najčešće na zahtjev saveznog tužitelja, velika porota (istražni ogranak suda koji sastavlja sudac ili pomoćni sudac) može izdati sudski poziv kako bi se osobu obvezalo da dostavi ili da na uvid poslovne evidencije, elektronički pohranjene informacije ili druge fizičke predmete. Nadalje, određenim propisima ovlašćuju se upravni sudski pozivi na dostavu ili davanje na uvid poslovnih evidencija, elektronički pohranjenih informacija ili drugih fizičkih predmeta u istragama povezanima s prijevarom u zdravstvu, zlostavljanjem djece, zaštitom koju pruža Tajna služba i kontroliranim tvarima te istragama glavnog inspektora ([158]). U oba slučaja informacije moraju biti relevantne za istragu, a sudski poziv ne smije biti nerazuman, odnosno preopsežan, opresivan ni opterećujući (te ga primatelj može osporavati na temelju tih razloga) ([159]).

(94) Upravni sudski pozivi jedan su od glavnih alata za pristup civilnih ili regulatornih tijela (pristup zbog „javnog interesa") podacima poduzeća u SAD-u, a na njega se primjenjuju vrlo slični uvjeti. Ovlasti agencija s civilnim i regulatornim odgovornostima za izdavanje takvih upravnih sudskih poziva moraju se utvrditi zakonom. Uporaba upravnog sudskog poziva podliježe „provjeri opravdanosti", u kojoj se ispituje provodi li se istraga u legitimnu svrhu, jesu li informacije zatražene u sudskom pozivu relevantne za tu svrhu, raspolaže li agencija već informacijama koje traži u sudskom pozivu te jesu li poduzeti potrebni administrativni koraci za izdavanje sudskog poziva ([160]). U sudskoj praksi Vrhovnog suda pojašnjena je i potreba za postizanjem ravnoteže između važnosti javnog interesa u pogledu traženih informacija i važnosti interesa pojedinaca i organizacija u pogledu privatnosti ([161]). Iako za uporabu upravnog sudskog poziva nije potrebno prethodno sudsko odobrenje, ona podliježe sudskom preispitivanju ako je primatelj osporava na temelju prethodno navedenih razloga ili ako agencija koja ga je izdala želi provesti sudski poziv na sudu ([162]). Uz ta opća glavna ograničenja posebni (stroži) zahtjevi mogu proizlaziti iz pojedinačnih zakona ([163]).

([155]) *Mapp protiv Ohija*, 367 U.S. 643 (1961.).

([156]) Vidjeti predmete *In re Application of United States*, 610 F.2d 1148, 1157 (3. okrug, 1979.) (utvrđeno je da je „postupanje […] zakonito samo ako se saslušanje o pitanju opterećenja održi prije nego što se telefonskog operatera obveže da pomogne" u izvršenju naloga za pretragu) i *In re Application of United States*, 616 F.2d 1122 (9. okrug, 1980.).

([157]) Petim amandmanom na američki Ustav propisano je da optužnicu za „kazneno djelo kažnjivo smrtnom kaznom ili osobito teško kazneno djelo" mora potvrditi velika porota. Velika porota ima od 16 do 23 člana i utvrđuje postoji li osnovana sumnja da je počinjeno kazneno djelo. Radi toga ima istražne ovlasti koje joj omogućuju izdavanje sudskih poziva.

([158]) Vidjeti Prilog VI.

([159]) Savezni propisi o kaznenom postupku, Propis br. 17.

([160]) *Sjedinjene Američke Države protiv Powella*, 379 U.S. 48 (1964.).

([161]) *Oklahoma Press Publishing Co. protiv Wallinga*, 327 U.S. 186 (1946.).

([162]) Vrhovni sud pojasnio je da u slučaju osporavanja upravnog sudskog poziva sud mora razmotriti 1. provodi li se istraga u zakonski dopuštenu svrhu, 2. je li predmetna ovlast za izdavanje sudskih poziva jedna od ovlasti koje Kongres može naložiti i 3. jesu li „zatraženi dokumenti relevantni za istragu". Sud je ujedno napomenuo da zahtjev iz upravnog sudskog poziva mora biti „razuman", odnosno da „specifikacija dokumenata koje treba dostaviti mora biti primjerena svrhama predmetne istrage i ne smije biti pretjerana" te da mora sadržavati „točan ‚opis mjesta koje će se pretraživati i osoba ili stvari koje će se zaplijeniti'".

([163]) Na primjer, Zakonom o pravu na privatnost financijskih podataka (Right to Financial Privacy Act) vladino tijelo ovlašteno je pribaviti financijske evidencije financijske institucije na temelju upravnog sudskog poziva 1. samo ako postoji razlog za pretpostavku da su zatražene evidencije relevantne za legitimnu istragu tijela kaznenog progona i 2. samo ako je klijentu dostavljen primjerak sudskog poziva ili poziva na davanje iskaza zajedno s obavijesti u kojoj se odgovarajućom preciznošću navodi priroda istrage (glava 12. . članak 3405. Zakonika SAD-a). Drugi je primjer Zakon o poštenom izvješćivanju o kreditnoj sposobnosti, kojim se agencijama za izvješćivanje o potrošačima zabranjuje objavljivanje izvješća o potrošačima na temelju zahtjevâ iz upravnih sudskih poziva (te im se dopušta da odgovore samo na zahtjeve iz sudskih poziva koje je izdala velika porota i sudskih naloga; glava 15. članak 1681. i dalje Zakonika SAD-a). Kad je riječ o pristupu informacijama o komunikaciji, primjenjuju se posebni zahtjevi iz Zakona o pohranjenoj komunikaciji, među ostalim u pogledu mogućnosti uporabe upravnih sudskih poziva (vidjeti detaljan pregled u uvodnim izjavama 96. i 97.).

(95) Treće, tijela kaznenog progona mogu dobiti pristup podacima o komunikaciji na temelju nekoliko pravnih osnova. Sud može izdati nalog kojim odobrava prikupljanje informacija o biranim brojevima, preusmjeravanju, adresiranju i signaliziranju bez sadržaja u stvarnom vremenu za telefonski broj ili e-adresu (uređajima za bilježenje ulaznih i izlaznih poziva) ako utvrdi da je tijelo potvrdilo da su informacije koje će se vjerojatno dobiti relevantne za istragu u kaznenom postupku koja je u tijeku ([164]). U nalogu moraju biti navedeni, među ostalim, identitet osumnjičenika ako je poznat, obilježja komunikacije na koju se nalog odnosi i pravna kvalifikacija kaznenog djela na koje se odnose informacije koje se prikupljaju. Uporaba uređaja za bilježenje ulaznih i izlaznih poziva može se odobriti na najviše 60 dana, a to se razdoblje može produljiti isključivo novim sudskim nalogom.

(96) Pristup u svrhe kaznenog progona informacijama o pretplatnicima, podacima o prometu i pohranjenom sadržaju komunikacije u posjedu pružatelja internetskih usluga, telefonskih operatera i pružatelja usluga koji su treća strana može se dobiti na temelju Zakona o pohranjenoj komunikaciji ([165]). Kako bi mogla dobiti pohranjeni sadržaj elektroničke komunikacije, tijela kaznenog progona u načelu moraju od suca ishoditi nalog na temelju osnovane sumnje da predmetni račun sadržava dokaze o kaznenom djelu ([166]). Informacije o registraciji pretplatnika, IP adrese i povezane vremenske oznake te informacije o naplati ta tijela mogu dobiti na temelju sudskog poziva. Za većinu drugih pohranjenih informacija bez sadržaja, kao što su zaglavlja e-poruka bez predmeta, tijela kaznenog progona moraju ishoditi sudski nalog koji će sudac izdati ako postoji opravdana pretpostavka da su tražene informacije relevantne i bitne za istragu u kaznenom postupku koja je u tijeku.

(97) Pružatelji koji prime zahtjeve na temelju Zakona o pohranjenoj komunikaciji mogu dobrovoljno obavijestiti klijenta ili pretplatnika čije se informacije traže, osim ako nadležno tijelo kaznenog progona ishodi nalog za zaštitu kojim se zabranjuje obavješćivanje ([167]). Nalog za zaštitu je sudski nalog kojim se pružatelju usluga elektroničke komunikacije ili računalnih usluga na daljinu kojem je upućen nalog, sudski poziv ili sudski nalog zabranjuje obavješćivanje drugih osoba o postojanju naloga, sudskog poziva ili sudskog naloga na razdoblje koje sud smatra primjerenim. Nalozi za zaštitu izdaju se ako sud utvrdi da postoji razlog za pretpostavku da bi se obavješćivanjem znatno ugrozila istraga ili neopravdano odgodilo suđenje, na primjer jer bi se time ugrozio život ili fizička sigurnost pojedinca, omogućio bijeg od kaznenog progona ili zastrašili mogući svjedoci. Na temelju memoranduma zamjenika glavnog državnog odvjetnika (koji je obvezujući za sve odvjetnike i agente Ministarstva pravosuđa) tužitelji moraju detaljno obrazložiti zašto je nalog o zaštiti potreban i sudu obrazložiti na koji su način u određenom predmetu ispunjeni zakonski kriteriji za ishođenje naloga za zaštitu ([168]). Njime je ujedno propisano da se u zahtjevu za nalog za zaštitu u pravilu ne smije tražiti odgoda obavješćivanja dulja od godine dana. Ako je u izvanrednim okolnostima potreban nalog duljeg trajanja, njega se može zatražiti samo uz pisanu suglasnost nadzornika kojeg određuje američki glavni državni odvjetnik ili nadležni pomoćnik glavnog državnog odvjetnika. Nadalje, kad zatvara istragu, tužitelj mora odmah procijeniti postoji li osnova za daljnju primjenu važećih naloga za zaštitu te, ako ne postoji, ukinuti nalog za zaštitu i pobrinuti se da se o tome obavijesti pružatelj usluga ([169]).

([164]) Glava 18. članak 3123. Zakonika SAD-a.

([165]) Glava 18. članci od 2701. do 2713. Zakonika SAD-a.

([166]) Glava 18. članak 2701. točke (a)–(b)(1)(A) Zakonika SAD-a. Ako se o tome obavijesti dotičnog pretplatnika ili klijenta (unaprijed ili u određenim okolnostima uz odgodu), informacije o sadržaju pohranjene dulje od 180 dana mogu se isto tako dobiti na temelju upravnog sudskog poziva ili sudskog poziva kojeg je izdala velika porota (članak 2701. točka (b)(1)(B) glava 18. Zakonika SAD-a) ili sudskog naloga (ako postoji opravdana pretpostavka da su informacije relevantne i bitne za istragu u kaznenom postupku koja je u tijeku (glava 18. članak 2701. točka (d) Zakonika SAD-a). No, u skladu s presudom saveznog žalbenog suda državni istražitelji obično od sudaca ishode nalog za pretragu kako bi od pružatelja komercijalnih komunikacijskih usluga prikupili sadržaj privatne komunikacije ili pohranjene podatke. *Sjedinjene Američke Države protiv Warshaka*, 631 F.3d 266 (6. okrug, 2010.).

([167]) Glava 18. članak 2705. točka (b) Zakonika SAD-a.

([168]) Vidjeti Memorandum zamjenika glavnog državnog odvjetnika Roda Rosensteina od 19. listopada 2017. o strožoj politici za zahtjeve za naloge za zaštitu (ili neotkrivanje), dostupan na https://www.justice.gov/criminal-ccips/page/file/1005791/download

([169]) Memorandum zamjenice glavnog državnog odvjetnika Lise Monaco od 27. svibnja 2022. o dopunskoj politici za zahtjeve za nalog za zaštitu u skladu s glavom 18. člankom 2705. stavkom (b) Zakonika SAD-a.

(98) Tijela kaznenog progona isto tako mogu u stvarnom vremenu presretati telefonsku, usmenu ili elektroničku komunikaciju na temelju sudskog naloga u kojem sudac utvrdi, među ostalim, da postoji osnovana sumnja da će se prisluškivanjem ili elektroničkim presretanjem pronaći dokazi o saveznom kaznenom dijelu ili o lokaciji bjegunca od kaznenog progona ([170]).

(99) Dodatna zaštita osigurana je politikama i smjernicama Ministarstva pravosuđa, uključujući Smjernice glavnog državnog odvjetnika za domaće operacije FBI-ja (AGG-DOM), kojima je među ostalim propisano da Savezni istražni ured (FBI) mora upotrebljavati istražne metode kojima se najmanje zadire u privatnost, uzimajući u obzir utjecaj na privatnost i građanske slobode ([171]).

(100) Prema izjavama američke vlade prethodno opisana, jednaka ili viša razina zaštite primjenjuje se na istrage tijela kaznenog progona na državnoj razini (u pogledu istraga koje se provode u skladu s državnim zakonima) ([172]). Točnije, ustavne odredbe te zakoni i sudska praksa na državnoj razini potvrđuju prethodno navedenu zaštitu od nerazumnih pretraga i zapljena jer je njima propisano izdavanje naloga za pretragu ([173]). Slično zaštiti koja se pruža na saveznoj razini, nalozi za pretragu mogu se izdati samo ako se dokaže osnovana sumnja i u njima se mora opisati mjesto koje će se pretraživati i osoba ili stvar koja će se zaplijeniti ([174]).

([170]) Glava 18. članci od 2510. do 2522. Zakonika SAD-a.

([171]) Smjernice glavnog državnog odvjetnika za domaće operacije Saveznog istražnog ureda (FBI) (rujan 2008.), dostupne na http://www.justice.gov/archive/opa/docs/guidelines.pdf. Dodatna pravila i politike u kojima su propisana ograničenja istražnih aktivnosti saveznih tužitelja navedeni su u Priručniku za državne tužitelje SAD-a, koji je dostupan na http://www.justice.gov/usam/united-states-attorneys-manual. Od tih se Smjernica može odstupiti samo ako to prethodno odobri ravnatelj FBI-ja, njegov zamjenik ili izvršni pomoćnik ravnatelja kojeg određuje ravnatelj, osim ako je prijetnja sigurnosti osoba ili imovine ili nacionalnoj sigurnosti toliko izravna ili velika da se to odobrenje ne može ishoditi (u tom slučaju treba što prije obavijestiti ravnatelja ili drugu ovlaštenu osobu). O nepridržavanju Smjernica FBI mora obavijestiti Ministarstvo pravosuđa, koje potom obavješćuje glavnog državnog odvjetnika i njegova zamjenika.

([172]) Bilješka 2. Priloga VI. Vidjeti i npr. *Arnold protiv Grada Clevelanda*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993.) („U području prava pojedinaca i građanskih sloboda Ustavom Sjedinjenih Američkih Država, u dijelu primjenjivom na države, predviđa se minimalna razina zaštite koju moraju pružiti sudske odluke na državnoj razini."), *Cooper protiv Kalifornije*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L. Ed.2d 730 (1967.) („Naše utvrđenje ni na koji način ne utječe na ovlast države da, ako to odluči, odredi više standarde u pogledu pretraga i zapljena od onih koji su propisani Saveznim ustavom."), *Petersen protiv Grada Mese*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003.) („Iako su Ustavom Arizone predviđeni stroži standardi u pogledu pretraga i zapljena nego u Saveznom ustavu, sudovi u Arizoni ne smiju pružiti nižu razinu zaštite od one predviđene četvrtim amandmanom.").

([173]) Većina država u svoje je ustave prenijela formulaciju o zaštiti iz četvrtog amandmana. Vidjeti članak I. stavak 5. Ustava Alabame, članak I. stavak 14. Ustava Aljaske, 1, članak II. stavak 15. Ustava Arkansasa, članak I. stavak 13. Ustava Kalifornije, članak II. stavak 7. Ustava Colorada, članak I. stavak 7. Ustava Connecticuta, članak I. stavak 6. Ustava Delawarea, članak I. stavak 12. Ustava Floride, članak I. stavak I. podstavak XIII. Ustava Georgije, članak I. stavak 7. Ustava Hawaija, članak I. stavak 17. Ustava Idahoa, članak I. stavak 6. Ustava Illinoisa, članak I. stavak 11. Ustava Indiane, članak I. stavak 8. Ustava Iowe, Povelja o pravima članak 15. Ustava Kansasa; članak 10. Ustava Kentuckyja, članak I. stavak 5. Ustava Louisiane, članak I. stavak 5. Ustava Mainea, Deklaracija o pravima članak 14. Ustava Massachusettsa, članak I. stavak 11. Ustava Michigana, članak I. stavak 10. Ustava Minnesote, članak III. stavak 23. Ustava Mississippija, članak I. stavak 15. Ustava Missourija, članak II. stavak 11. Ustava Montane, članak I. stavak 7. Ustava Nebraske, članak I. stavak 18. Ustava Nevade, dio 1. članak 19. Ustava New Hampshirea, članak II. stavak 7. Ustava New Jerseyja, članak II. stavak 10. Ustava New Mexica, članak I. stavak 12. Ustava New Yorka, članak I. stavak 8. Sjeverne Dakote, članak I. stavak 14. Ohija, članak II. stavak 30. Ustava Oklahome, članak I. stavak 9. Ustava Oregona, članak I. stavak 8. Ustava Pennsylvanije, članak I. stavak 6. Ustava Rhode Islanda, članak I. stavak 10. Ustava Južne Karoline, članak VI. stavak 11. Ustava Južne Dakote, članak I. stavak 7. Ustava Tennesseeja, članak I. stavak 9. Ustava Teksasa, članak I. stavak 14. Ustava Ute, poglavlje I. članak 11. Ustava Vermonta, članak III. stavak 6. Zapadne Virginije, članak I. stavak 11. Ustava Wisconsina, članak I. stavak 4. Ustava Wyominga. Ustavi ostalih država (npr. Maryland, Sjeverna Karolina i Virginia) sadržavaju drukčije formulacije o nalozima za koje je sud utvrdio da pružaju razinu zaštite sličnu kao četvrti amandman ili višu (vidjeti članak 26. Deklaracije o pravima Marylanda, članak I. stavak 20. Ustava Sjeverne Karoline, članak I. stavak 10. Ustava Virginije i relevantnu sudsku praksu, npr. *Hamel protiv Države*, 943 A.2d 686, 701. (Md. Ct. Spec. App. 2008., *Država protiv Johnsona*, 861 S.E.2d 474, 483 (N.C. 2021.) i *Lowe protiv Commonwealtha*, 337 S.E.2d 273, 274 (Va. 1985.)). Naposljetku, Arizona i Washington imaju ustavne odredbe kojima se općenito štiti privatnost (članak 2. stavak 8. Ustava Arizone, članak I. stavak 7. Ustava Washingtona), za koje je sud utvrdio da pružaju višu razinu zaštite od četvrtog amandmana (vidjeti npr. *Država protiv Bolta*, 689 P.2d 519, 523 (Ariz. 1984.), *Država protiv Aulta*, 759 P.2d 1320, 1324 (Ariz. 1988.), *Država protiv Myricka*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984)., *Država protiv Younga*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994.)).

([174]) Vidjeti npr. članak 1524,3(b) Kaznenog zakona Kalifornije, pravila od 3.6 do 3.13 Pravila kaznenog postupka Alabame, članak 10.79.035 Revidiranog zakonika Washingtona, glava 19.2. „Kazneni postupak" poglavlje 5. članak 19.2-59. Zakonika Virginije.

3.1.1.2. *Daljnja uporaba prikupljenih informacija*

(101) Raznim zakonima, smjernicama i standardima propisane su posebne zaštitne mjere za daljnju uporabu podataka koje su prikupila savezna tijela kaznenog progona. Uz iznimku posebnih instrumenata koji se primjenjuju na aktivnosti FBI-ja (Smjernice glavnog državnog odvjetnika za domaće operacije FBI-ja i Vodič FBI-ja za domaće istrage i operacije), zahtjevi opisani u ovom odjeljku općenito se primjenjuju na sva savezna tijela, odnosno njihovu daljnju uporabu podataka, uključujući podatke kojima se pristupa u civilne ili regulatorne svrhe. To uključuje zahtjeve koji proizlaze iz memoranduma/propisa Ureda za upravljanje i proračun, Zakona o modernizaciji savezne informacijske sigurnosti (Federal Information Security Management Modernization Act), Zakona o e-vladi (E-Government Act) i Zakona o saveznim evidencijama (Federal Records Act – FRA).

(102) U skladu s ovlastima iz Zakona Clinger–Cohen (dio E Javnog zakona br. 104–106) i Zakona o računalnoj sigurnosti iz 1987. (Computer Security Act) (Javni zakon br. 100–235) Ured za upravljanje i proračun (OMB) izdao je Okružnicu br. A-130 o uspostavljanju općih obvezujućih smjernica za sve savezne agencije (uključujući tijela kaznenog progona) pri rukovanju informacijama na temelju kojih se može utvrditi identitet pojedinca ([175]). Njome je propisano da sve savezne agencije moraju „ograničiti stvaranje, prikupljanje, uporabu, obradu, pohranu, održavanje, širenje i otkrivanje informacija na temelju kojih se može utvrditi identitet pojedinca na mjeru u kojoj su zakonski ovlaštene za te aktivnosti i u kojoj su te aktivnosti relevantne i opravdano se smatraju nužnima za pravilno izvršavanje funkcija za koje je agencija ovlaštena” ([176]). Nadalje, u mjeri u kojoj je to razumno izvedivo savezne agencije moraju osigurati točnost, relevantnost, pravodobnost i potpunost informacija na temelju kojih se može utvrditi identitet pojedinca te smanjiti njihovu količinu na onu koja je nužna za pravilno izvršavanje njihovih funkcija. Općenitije govoreći, savezne agencije moraju uspostaviti sveobuhvatan program zaštite privatnosti radi usklađivanja s primjenjivim zahtjevima zaštite privatnosti, izraditi i ocjenjivati politike zaštite privatnosti te upravljati rizicima za privatnost, provoditi postupke za otkrivanje i dokumentiranje slučajeva neusklađenosti s propisima o privatnosti i izvješćivanje o njima, izraditi programe za informiranje i osposobljavanje zaposlenika i izvođača o privatnosti te uspostaviti politike i postupke kojima se osigurava odgovornost osoblja za usklađenost sa zahtjevima i politikama zaštite privatnosti ([177]).

(103) Nadalje, Zakonom o e-vladi ([178]) propisano je da sve savezne agencije (uključujući tijela kaznenog progona) trebaju uvesti oblike zaštite u području informacijske sigurnosti koji su razmjerni riziku od i razini štete koja bi nastala neovlaštenim pristupom, uporabom, otkrivanjem, presretanjem, izmjenom ili uništavanjem, imati glavnog službenika za informacije koji osigurava usklađenost sa zahtjevima informacijske sigurnosti i provesti godišnju neovisnu evaluaciju (npr. može je provesti glavni inspektor, vidjeti uvodnu izjavu 109.) svojeg programa i prakse u području informacijske sigurnosti ([179]). Slično tomu, u skladu sa Zakonom o saveznim evidencijama ([180]) i dopunskim propisima ([181]) na informacije u posjedu saveznih agencija moraju se primjenjivati zaštitne mjere za očuvanje fizičke cjelovitosti informacija i zaštitu od neovlaštenog pristupa njima.

(104) U skladu s ovlastima iz saveznih zakona, uključujući Zakon o modernizaciji savezne informacijske sigurnosti iz 2014., Ured za upravljanje i proračun i Nacionalni institut za standarde i tehnologiju (NIST) izradili su standarde koji su obvezujući za sve savezne agencije (uključujući tijela kaznenog progona) i u kojima se dodatno preciziraju minimalni zahtjevi informacijske sigurnosti koje treba uspostaviti, uključujući kontrole pristupa, informiranje i osposobljavanje, planiranje djelovanja u nepredvidivim okolnostima, odgovaranje na incidente, alate za reviziju i odgovornost, jamčenje cjelovitosti sustava i informacija te procjene sigurnosnog rizika ([182]). Nadalje, sve savezne

([175]) „Informacije koje se mogu upotrijebiti da bi se razabrao ili pratio identitet pojedinca bilo samostalno ili u kombinaciji s drugim informacijama koje su povezane ili se mogu povezati s određenim pojedincem”, vidjeti Okružnicu Ureda za upravljanje i proračun br. A-130, str. 33. (definicija „informacija na temelju kojih se može utvrditi identitet pojedinca”).

([176]) Okružnica Ureda za upravljanje i proračun br. A-130, *Managing Information as a Strategic Resource* (Upravljanje informacijama kao strateškim resursom), Dodatak II. Odgovornosti za upravljanje informacijama na temelju kojih se može utvrditi identitet pojedinca, Savezni registar, sv. 81, str. 49689. (28. srpnja 2016.), str. 17.

([177]) Točke 5(a)–(h) Dodatka II.

([178]) Glava 44. poglavlje 36. Zakonika SAD-a.

([179]) Glava 44. članci od 3544. do 3545. Zakonika SAD-a.

([180]) Zakon o saveznim evidencijama – glava 44. članak 3105. Zakonika SAD-a.

([181]) Glava 36. članak 1228,150 i dalje, članak 1228,228 i Dodatak A Kodeksa saveznih propisa.

([182]) Vidjeti npr. Okružnicu Ureda za upravljanje i proračun br. A-130, Nacionalni institut za standarde i tehnologiju, SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (10. prosinca 2020.) i Nacionalni institut za standarde i tehnologiju, *Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.*

agencije (uključujući tijela kaznenog progona) moraju u skladu sa smjernicama Ureda za upravljanje i proračun imati i provoditi plan postupanja u slučaju povreda podataka, koji uključuje i odgovaranje na takve povrede i procjenu rizika od štete ([183]).

(105) Kad je riječ o čuvanju podataka, Zakonom o saveznim evidencijama ([184]) propisano je da američke savezne agencije (uključujući tijela kaznenog progona) moraju utvrditi razdoblje čuvanja svojih evidencija (nakon kojeg ih treba ukloniti), koje mora odobriti Uprava za nacionalne arhive i evidencije ([185]). Razdoblje čuvanja utvrđuje se ovisno o raznim čimbenicima, na primjer vrsti istrage ili daljnjoj relevantnosti dokaza za istragu. U Smjernicama glavnog državnog odvjetnika za domaće operacije FBI-ja propisano je da FBI mora imati plan čuvanja evidencija i održavati sustav iz kojeg se odmah može dohvatiti status istraga i osnova po kojoj se provode.

(106) Naposljetku, u Okružnici Ureda za upravljanje i proračun br. A-130 navedeni su određeni zahtjevi za širenje informacija na temelju kojih se može utvrditi identitet pojedinca. Širenje i otkrivanje informacija na temelju kojih se može utvrditi identitet pojedinca u načelu mora biti ograničeno na mjeru u kojoj je agencija zakonski ovlaštena za te aktivnosti i u kojoj su te aktivnosti relevantne i opravdano se smatraju nužnima za pravilno izvršavanje funkcija agencije ([186]). Pri dijeljenju informacija na temelju kojih se može utvrditi identitet pojedinca s drugim vladinim tijelima američke savezne agencije prema potrebi moraju u okviru pisanih sporazuma (uključujući ugovore, sporazume o uporabi podataka, sporazume o razmjeni informacija i memorandume o razumijevanju) odrediti uvjete (uključujući provedbu određenih kontrola sigurnosti i privatnosti) za obradu informacija ([187]). Smjernicama glavnog državnog odvjetnika za domaće operacije FBI-ja i Vodičem FBI-ja za domaće istrage i operacije ([188]) propisane su osnove za širenje podataka, pa tako FBI može imati pravnu obvezu širiti podatke (npr. na temelju međunarodnog sporazuma) ili mu je dopušteno širiti podatke u određenim okolnostima, na primjer drugim američkim agencijama ako je otkrivanje u skladu sa svrhom u koju su informacije prikupljene i ako je povezano s njihovim odgovornostima, kongresnim odborima, stranim agencijama ako su informacije povezane s njihovim odgovornostima i ako je širenje u skladu s interesima SAD-a, ako je širenje prvenstveno potrebno radi sigurnosti ili zaštite osoba ili imovine odnosno radi zaštite od ili sprečavanja kaznenog djela ili prijetnje nacionalnoj sigurnosti i ako je otkrivanje u skladu sa svrhom u koju su informacije prikupljene ([189]).

3.1.2. ***Nadzor***

(107) Aktivnosti saveznih agencija kaznenog progona nadziru razna tijela ([190]). Kako je objašnjeno u uvodnim izjavama 92.–99., to većinom uključuje prethodni nadzor koji obavljaju pravosudna tijela, koja moraju odobriti pojedinačne mjere prikupljanja prije njihove primjene. Osim toga, druga tijela nadziru različite faze aktivnosti tijela kaznenog progona, uključujući prikupljanje i obradu osobnih podataka. Ta pravosudna i nepravosudna tijela zajedno osiguravaju neovisni nadzor tijela kaznenog progona.

([183]) Memorandum br. 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Priprema za povrede informacija na temelju kojih se može utvrditi identitet pojedinca i odgovaranje na takve povrede), dostupan na https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, Okružnica Ureda za upravljanje i proračun br. A-130. Npr. postupci Ministarstva pravosuđa za odgovaranje na povrede podataka, vidjeti https://www.justice.gov/file/4336/download

([184]) Zakon o saveznim evidencijama – glava 44. članak 3101. i dalje Zakonika SAD-a.

([185]) Uprava za nacionalne arhive i evidencije ovlaštena je ocjenjivati praksu upravljanja agencijskim evidencijama i može utvrditi je li daljnje čuvanje određenih evidencija potrebno (glava 44. članak 2904. točka (c) i članak 2906. Zakonika SAD-a).

([186]) Odjeljak 5.f.1.(d) Okružnice Ureda za upravljanje i proračun br. A-130.

([187]) Točka 3(d) Dodatka I. Okružnici Ureda za upravljanje i proračun br. A-130.

([188]) Vidjeti i odjeljak 14. Vodiča FBI-ja za domaće istrage i operacije (DIOG).

([189]) Odjeljci VI., B i C Smjernica glavnog državnog odvjetnika za domaće operacije FBI-ja, odjeljak 14. Vodiča FBI-ja za domaće istrage i operacije (DIOG).

([190]) Mehanizmi navedeni u ovom odjeljku primjenjuju se i na savezna tijela, odnosno njihovo prikupljanje i uporabu podataka u civilne i regulatorne svrhe. Savezne civilne i regulatorne agencije podliježu nadzoru nadležnih glavnih inspektora i Kongresa, uključujući revizijsku i istražnu agenciju Kongresa Ured za utvrđivanje odgovornosti Vlade. Osim ako agencija ima imenovanog službenika za privatnost i građanske slobode, što je uobičajeno u tijelima kao što su Ministarstvo pravosuđa i Ministarstvo domovinske sigurnosti zbog njihovih odgovornosti za kazneni progon i nacionalnu sigurnost, te su dužnosti u nadležnosti višeg službenika agencije za zaštitu privatnosti (SAOP). Sve savezne agencije zakonski su obvezne imenovati SAOP-a, koji snosi odgovornost za usklađenost agencije s propisima o privatnosti i nadzor povezanih pitanja. Vidjeti npr. Memorandum Ureda za upravljanje i proračun br. M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (2016.).

(108) Prvo, u raznim ministarstvima koja su, među ostalim, odgovorna za kazneni progon rade službenici za privatnost i građanske slobode ([191]). Iako se konkretne ovlasti tih službenika mogu donekle razlikovati ovisno o zakonu kojim su propisane, one obično obuhvaćaju nadzor postupaka kako bi se osiguralo da predmetno ministarstvo/agencija na primjereni način štiti privatnost i građanske slobode te da je uspostavilo primjerene postupke za rješavanje pritužbi pojedinaca koji smatraju da su im ugrožene privatnost ili građanske slobode. Ministri ili ravnatelji agencija moraju službenicima za privatnost i građanske slobode osigurati materijale i resurse za izvršavanje mandata, kao i pristup svim materijalima i osoblju nužnima za izvršavanje njihovih funkcija, te ih informirati i savjetovati se s njima o predloženim izmjenama politika ([192]). Službenici za privatnost i građanske slobode periodično izvješćuju Kongres, među ostalim o broju i prirodi pritužbi koje je zaprimilo ministarstvo/agencija, uz navođenje sažetka odgovora na te pritužbe, o provedenim preispitivanjima i istragama te o učinku aktivnosti koje je službenik proveo ([193]).

(109) Drugo, aktivnosti Ministarstva pravosuđa, uključujući aktivnosti FBI-ja, nadzire i neovisni glavni inspektor ([194]). Glavni inspektori zakonski su neovisni ([195]) i odgovorni za provedbu neovisnih istraga, revizija i inspekcija programa i operacija ministarstva. Imaju pristup svim evidencijama, izvješćima, revizijama, preispitivanjima, dokumentima, spisima, preporukama ili drugim relevantnim materijalima, prema potrebi na temelju sudskog naloga, i mogu uzimati iskaze ([196]). Iako glavni inspektori izdaju neobvezujuće preporuke korektivnih mjera, njihova izvješća, uključujući ona o daljnjim mjerama (ili nepostojanju takvih mjera) ([197]), u pravilu se objavljuju i šalju Kongresu, koji na osnovi toga može vršiti svoju nadzornu funkciju (vidjeti uvodnu izjavu 111.) ([198]).

([191]) Vidjeti glavu 42. članak 2000ee-1. Zakonika SAD-a. To su npr. Ministarstvo pravosuđa, Ministarstvo domovinske sigurnosti i FBI. Osim toga, u Ministarstvu domovinske sigurnosti postoji glavni službenik za privatnost koji je odgovoran za očuvanje i poboljšanje zaštite privatnosti i promicanje transparentnosti u ministarstvu (glava 6. članak 142. Zakonika SAD-a, članak 222.). Sve sustave, tehnologije, obrasce i programe Ministarstva domovinske sigurnosti u okviru kojih se prikupljaju osobni podaci ili koji utječu na privatnost nadzire glavni službenik za privatnost koji ima pristup svim evidencijama, izvješćima, revizijama, preispitivanjima, dokumentima, spisima, preporukama i drugim materijalima dostupnima ministarstvu, prema potrebi na temelju sudskog poziva. Službenik za privatnost svake godine mora izvješćivati Kongres o aktivnostima ministarstva koje utječu na privatnost, među ostalim o pritužbama zbog povreda privatnosti.

([192]) Glava 42. članak 2000ee-1. točka (d) Zakonika SAD-a.

([193]) Vidjeti glavu 42. članak 2000ee-1. točke (f)(1)–(2) Zakonika SAD-a. Na primjer, izvješće glavnog službenika za privatnost i građanske slobode Ministarstva pravosuđa te Ureda za privatnost i građanske slobode za razdoblje od listopada 2020. do ožujka 2021. pokazuje da je provedeno 389 revizija privatnosti, uključujući informacijske sustave i druge programe (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) Slično tomu, Zakonom o domovinskoj sigurnosti (Homeland Security Act) iz 2002. osnovan je Ured glavnog inspektora pri Ministarstvu domovinske sigurnosti.

([195]) Glavni inspektori imaju osiguran mandat i može ih razriješiti jedino predsjednik, koji mora pisanim putem obavijestiti Kongres o razlozima za razrješenje.

([196]) Vidjeti članak 6. Zakona o glavnom inspektoru (Inspector General Act) iz 1978.

([197]) U tom pogledu vidjeti npr. pregled koji je Ured glavnog inspektora pri Ministarstva pravosuđa izradio o izdanim preporukama i mjeri u kojoj su provedene u okviru daljnjih mjera ministarstva i agencija, https://oig.justice.gov/sites/default/files/reports/22-043.pdf

([198]) Vidjeti članak 4. točku 5. i članak 5. Zakona o glavnom inspektoru iz 1978. Na primjer, Ured glavnog inspektora pri Ministarstvu pravosuđa nedavno je objavio svoje polugodišnje izvješće Kongresu (1. listopada 2021.–31. ožujka 2022., https://oig.justice.gov/node/23596), u kojem se nalazi pregled njegovih revizija, evaluacija, inspekcija, posebnih preispitivanja i istraga programa i operacija Ministarstva pravosuđa. Jedna od tih aktivnosti bila je istraga nekadašnjeg izvođača zbog nezakonitog otkrivanja elektroničkog nadzora (prisluškivanje jednog pojedinca) dok je istraga bila u tijeku, što je dovelo do izricanja kazne izvođaču. Ured glavnog inspektora istražio je i programe i praksu agencija Ministarstva pravosuđa u području informacijske sigurnosti, što je uključivalo ispitivanje djelotvornosti politika, postupaka i prakse u području informacijske sigurnosti na temelju reprezentativnog podskupa agencijskih sustava.

(110) Treće, u mjeri u kojoj provode protuterorističke aktivnosti, ministarstva odgovorna za kazneni progon podliježu nadzoru Odbora za nadzor privatnosti i građanskih sloboda (PCLOB), neovisne agencije u okviru izvršne vlasti sastavljene od dvostranačkog peteročlanog odbora koji imenuje predsjednik na fiksni šestogodišnji mandat uz odobrenje Senata ([199]). U skladu sa zakonom na temelju kojeg je osnovan PCLOB je odgovoran za politike za borbu protiv terorizma i njihovu provedbu u cilju zaštite privatnosti i građanskih sloboda. Za potrebe preispitivanja taj odbor može pristupiti svim relevantnim evidencijama, izvješćima, revizijama, preispitivanjima, dokumentima, spisima i preporukama agencije, uključujući klasificirane podatke, te obavljati razgovore i uzimati iskaze ([200]). Prima izvješća službenika za građanske slobode i privatnost nekoliko saveznih ministarstava/agencija ([201]), može davati preporuke državnim tijelima i tijelima kaznenog progona te redovito izvješćuje kongresne odbore i predsjednika ([202]). Izvješća tog odbora, uključujući ona Kongresu, moraju biti što dostupnija javnosti ([203]).

(111) Naposljetku, aktivnosti kaznenog progona nadziru posebni odbori američkog Kongresa (odbori za pravosuđe Zastupničkog doma i Senata). Odbori za pravosuđe provode redoviti nadzor na razne načine, osobito u okviru saslušanja, istraga, preispitivanja i izvješća ([204]).

3.1.3. ***Pravna zaštita***

(112) Kako je već navedeno, tijela kaznenog progona većinom moraju ishoditi prethodno sudsko odobrenje za prikupljanje osobnih podataka. Iako to nije obavezno u slučaju upravnih sudskih poziva, ti se pozivi izdaju samo u posebnim situacijama i podliježu neovisnom sudskom preispitivanju barem u slučajevima kad vlada traži provedbu sudskim putem. Naime, primatelji upravnih sudskih poziva mogu ih osporiti na sudu na osnovi toga da su nerazumni, odnosno preopsežni, opresivni ili opterećujući ([205]).

(113) Pojedinci mogu najprije podnijeti zahtjeve ili pritužbe tijelima kaznenog progona u vezi s obradom njihovih osobnih podataka. To uključuje mogućnost traženja pristupa osobnim podacima i njihova ispravka ([206]). Kad je riječ o protuterorističkim aktivnostima, pojedinci mogu podnijeti pritužbu i službenicima za privatnost i građanske slobode (ili drugim službenicima za privatnost) u tijelima kaznenog progona ([207]).

(114) Nadalje, u američkom pravu predviđen je niz oblika sudske zaštite pojedinaca protiv javnih tijela ili njihovih službenika ako ta tijela obrađuju osobne podatke ([208]). Ti oblici zaštite, koji prije svega uključuju Zakon o upravnom postupku (APA), Zakon o pravu na pristup informacijama (Freedom of Information Act – FOIA) i Zakon o zaštiti privatnosti elektroničke komunikacije (Electronic Communications Privacy Act – ECPA), dostupni su svim pojedincima neovisno o državljanstvu u skladu sa svim primjenjivim uvjetima.

([199]) Članovi odbora moraju se birati isključivo na temelju njihovih stručnih kvalifikacija, postignuća, javnog statusa, stručnosti u području građanskih sloboda i privatnosti te relevantnog iskustva, ne uzimajući u obzir političku pripadnost. Više od tri člana ni u kojem slučaju ne smiju pripadati istoj političkoj stranci. Pojedinac koji je imenovan članom odbora ne smije tijekom svojeg mandata biti izabrani dužnosnik, službenik ni zaposlenik savezne vlade, osim u svojstvu člana odbora. Vidjeti glavu 42. članak 2000ee. točku (h) Zakonika SAD-a.

([200]) Glava 42. članak 2000ee. točka (g) Zakonika SAD-a.

([201]) Vidjeti glavu 42. članak 2000ee-1. točku (f)(1)(A)(iii) Zakonika SAD-a. Oni uključuju, u najmanju ruku, Ministarstvo pravosuđa, Ministarstvo obrane, Ministarstvo domovinske sigurnosti te sva druga ministarstva, agencije ili subjekte izvršne vlasti koje PCLOB smatra relevantnima.

([202]) Glava 42. članak 2000ee. točka (e) Zakonika SAD-a.

([203]) Glava 42. članak 2000ee. točka (f) Zakonika SAD-a.

([204]) Na primjer, odbori organiziraju tematska saslušanja (vidjeti npr. nedavno saslušanje Odbora za pravosuđe Zastupničkog doma o „digitalnim mrežama za hvatanje kriminalaca", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983) i saslušanja o redovitom nadzoru, npr. FBI-ja i Ministarstva pravosuđa, vidjeti https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 i https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899

([205]) Vidjeti Prilog VI.

([206]) Odjeljak 3. točke (a) i (f) Dodatka II. Okružnice Ureda za upravljanje i proračun br. A-130, kojim se od saveznih agencija zahtijeva da osiguraju odgovarajući pristup i ispravak na zahtjev pojedinaca te da uspostave postupke za primanje i rješavanje pritužbi i zahtjeva povezanih s privatnošću.

([207]) Vidjeti glavu 42. članak 2000ee-1. Zakonika SAD-a u pogledu npr. Ministarstva pravosuđa i Ministarstva domovinske sigurnosti. Vidjeti i Memorandum Ureda za upravljanje i proračun br. M-16-24, *Role and Designation of Senior Agency Officials for Privacy*.

([208]) Mehanizmi pravne zaštite navedeni u ovom odjeljku primjenjuju se i na savezna tijela, odnosno njihovo prikupljanje i uporabu podataka u civilne i regulatorne svrhe.

(115) Općenito, u skladu s odredbama Zakona o upravnom postupku ([209]) koje se odnose na sudsko preispitivanje, „svaka osoba koja je pretrpjela štetu zbog mjere agencije protivne zakonu ili na koju je mjera agencije štetno djelovala odnosno kojoj su mjerom agencije povrijeđena prava" ima pravo tražiti sudsko preispitivanje ([210]). To uključuje mogućnost da od suda zatraži da „proglasi nezakonitima i ukine mjere, nalaze i zaključke agencija za koje se utvrdi da su […] samovoljni i doneseni iz inata, da čine zlouporabu diskrecijskih prava ili da na drugi način nisu u skladu sa zakonom" ([211]).

(116) Točnije, u glavi II. Zakona o zaštiti privatnosti elektroničke komunikacije ([212]) utvrđuje se sustav zakonskih prava na privatnost i uređuje pristup radi kaznenog progona telefonskoj, usmenoj ili elektroničkoj komunikaciji koju pohranjuju pružatelji usluga koji su treća strana ([213]). Njome se kriminalizira nezakonit pristup takvoj komunikaciji (tj. koji nije sudski odobren ili inače dopušten) te se oštećenom pojedincu pruža mogućnost da pokrene građanski postupak pred američkim saveznim sudom radi stvarne i kaznene odštete te pravične ili deklarativne naknade protiv vladina dužnosnika koji je samovoljno počinio takve nezakonite radnje ili protiv SAD-a.

(117) Nadalje, pravo da se podnese tužba protiv američkog javnog tijela ili dužnosnika zbog obrade osobnih podataka dodijeljeno je pojedincima nizom drugih zakona, na primjer Zakonom o prisluškivanju ([214]), Zakonom o računalnoj prijevari i zlouporabi ([215]), Saveznim zakonom o tužbi za naknadu građanske štete ([216]), Zakonom o pravu na privatnost financijskih podataka ([217]) i Zakonom o poštenom izvješćivanju o kreditnoj sposobnosti ([218]).

([209]) Glava 5. članak 702. Zakonika SAD-a.

([210]) Sudskom preispitivanju obično podliježe samo „krajnja", a ne „prethodna, postupovna ili privremena" mjera agencije. Vidjeti glavu 5. članak 704. Zakonika SAD-a.

([211]) Glava 5. članak 706. točka (2)(A) Zakonika SAD-a.

([212]) Glava 18. članci od 2701. do 2712. Zakonika SAD-a.

([213]) Zakonom o zaštiti privatnosti elektroničke komunikacije štiti se komunikacija u posjedu dviju vrsta pružatelja mrežnih usluga, odnosno pružatelja: i. usluga elektroničke komunikacije, npr. telefonija ili e-pošta, ii. računalnih usluga na daljinu kao što su usluge računalne pohrane ili obrade.

([214]) Glava 18. članak 2510. i dalje Zakonika SAD-a. U skladu sa Zakonom o prisluškivanju (glava 18. članak 2520. Zakonika SAD-a) osoba čija se telefonska, usmena ili elektronička komunikacija presreće, otkriva ili namjerno upotrebljava može pokrenuti građanski postupak zbog povrede Zakona o prisluškivanju, a u određenim okolnostima i protiv vladina dužnosnika ili SAD-a. Za prikupljanje informacija bez sadržaja (npr. IP adresa, e-adresa primatelja/pošiljatelja) vidjeti poglavlje „Uređaji za bilježenje ulaznih i izlaznih poziva" glave 18. (glava 18. članci od 3121. do 3127. i, za građanski postupak, članak 2707. Zakonika SAD-a).

([215]) Glava 18. članak 1030. Zakonika SAD-a. U skladu sa Zakonom o računalnoj prijevari i zlouporabi (Computer Fraud and Abuse Act) osoba može podnijeti tužbu protiv bilo koje osobe zbog namjernog neovlaštenog pristupa (ili prekoračenja ovlaštenog pristupa) radi prikupljanja informacija od financijske ustanove, računalnog sustava američke vlade ili drugog određenog računala, a u određenim okolnostima i protiv vladina dužnosnika.

([216]) Glava 28. članak 2671. i dalje Zakonika SAD-a. U skladu sa Saveznim zakonom o tužbi za naknadu građanske štete (Federal Tort Claims Act) osoba u određenim okolnostima može podnijeti tužbu protiv SAD-a zbog „nemara, protupravne radnje ili propusta bilo kojeg zaposlenika vlade dok djeluje u okviru svojeg mandata ili radnog odnosa".

([217]) Glava 12. članak 3401. i dalje Zakonika SAD-a. U skladu sa Zakonom o pravu na privatnost financijskih podataka osoba u određenim okolnostima može podnijeti tužbu protiv SAD-a zbog prikupljanja ili otkrivanja zaštićenih financijskih evidencija kojima se krši taj zakon. Pristup vlade zaštićenim financijskim evidencijama općenito je zabranjen osim ako vlada podnese zahtjev koji podliježe zakonitom sudskom pozivu ili nalogu za pretragu ili, uz primjenu određenih ograničenja, službeni pisani zahtjev te pojedinac čije se informacije traže primi obavijest o takvom zahtjevu.

([218]) Glava 15. članci od 1681. do 1681.x Zakonika SAD-a. 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) koji se odnose na prikupljanje, širenje i uporabu izvješća o kreditnoj sposobnosti potrošača ili, pod određenim uvjetima, protiv vladine agencije.

(118) Nadalje, u skladu sa Zakonom o pravu na pristup informacijama ([219]) (glava 5. članak 552. Zakonika SAD-a) svaka osoba ima pravo pristupiti evidencijama saveznih agencija, među ostalim ako one sadržavaju osobne podatke pojedinca. Nakon što iscrpi upravnopravna sredstva, pojedinac se može pozvati na takvo pravo na pristup pred sudom, osim ako su takve evidencije zaštićene od javnog objavljivanja izuzećem ili posebnim izuzećem od kaznenog progona ([220]). U tom će slučaju sud ocijeniti primjenjuje li se izuzeće ili se na njega zakonito poziva relevantno javno tijelo.

3.2. **Pristup američkih javnih tijela podacima i njihova uporaba u svrhe nacionalne sigurnosti**

(119) Pravo SAD-a sadržava brojna ograničenja i zaštitne mjere za pristup osobnim podacima i njihovu uporabu u svrhe nacionalne sigurnosti te su njime predviđeni mehanizmi nadzora i pravne zaštite koji su u skladu sa zahtjevima iz uvodne izjave 89. ove Odluke. Uvjeti pod kojima je takav pristup moguć i zaštitne mjere koje se primjenjuju na upotrebu tih ovlasti detaljno se ocjenjuju u odjeljcima u nastavku.

3.2.1. ***Pravne osnove, ograničenja i zaštitne mjere***

3.2.1.1. *Primjenjivi pravni okvir*

(120) Osobne podatke koji se prenose iz Unije u organizacije uključene u okvir EU-a i SAD-a za privatnost podataka mogu u svrhe nacionalne sigurnosti prikupljati američka tijela na osnovi raznih pravnih instrumenata uz određene uvjete i zaštitne mjere.

(121) Nakon što organizacije koje se nalaze u SAD-u prime osobne podatke, američke obavještajne agencije mogu u svrhe nacionalne sigurnosti zatražiti pristup takvim podacima samo ako je to dopušteno zakonom, posebno Zakonom o nadzoru stranih obavještajnih aktivnosti (FISA) i/ili zakonskim odredbama kojima se dopušta pristup uporabom dopisa o nacionalnoj sigurnosti ([221]). U Zakonu o nadzoru stranih obavještajnih aktivnosti navedeno je nekoliko pravnih osnova koje se mogu upotrijebiti za prikupljanje (i daljnju obradu) osobnih podataka ispitanika iz Unije prenesenih u skladu s okvirom EU-a i SAD-a za privatnost podataka (članci 105. ([222]), 302. ([223]), 402. ([224]), 501. ([225]) i 702. ([226]) Zakona o nadzoru stranih obavještajnih aktivnosti), kako je detaljnije opisano u uvodnim izjavama od 142. do 152.

([219]) Glava 5. članak 552. Zakonika SAD-a.

([220]) Ta su izuzeća, međutim, ograničena. Na primjer, u skladu s glavom 5. člankom 552. točkom (b)(7) Zakonika SAD-a prava zajamčena Zakonom o pravu na pristup informacijama ne primjenjuju se u slučaju „evidencija ili informacija prikupljenih u svrhe kaznenog progona, ali samo (A) ako se za dostavu takvih evidencija ili informacija može u razumnoj mjeri očekivati da će omesti provedbeni postupak, (B) ako bi se njome osobi uskratilo pravo na pošteno suđenje ili nepristrano donošenje presude, (C) ako se u razumnoj mjeri može očekivati da će predstavljati neopravdano uplitanje u čiju privatnost, (D) ako bi se u razumnoj mjeri moglo očekivati da će se otkriti identitet povjerljivog izvora, uključujući državnu, lokalnu ili stranu agenciju ili tijelo ili bilo koju privatnu ustanovu od kojih su informacije pribavljene na povjerljivoj osnovi, te informacije iz povjerljivih izvora u slučaju evidencija ili informacija koje je prikupilo tijelo kaznenog progona tijekom istrage u kaznenom postupku ili agencija pri provedbi zakonite obavještajne istrage u području nacionalne sigurnosti, (E) ako bi se 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 (F) da će ugroziti nečiji život ili fizičku sigurnost”. Osim toga, „pri svakom podnošenju zahtjeva koji uključuje pristup evidencijama [za čiju bi se dostavu moglo razumno očekivati da će omesti provedbeni postupak], a (A) istraga ili postupak uključuje moguću povredu kaznenog prava i (B) postoji vjerojatnost da i. pojedinac koji je predmet istrage ili postupka nije upoznat s tim da su u tijeku te ii. bi se moglo u razumnoj mjeri očekivati da će otkrivanje postojanja evidencija ometati provedbeni postupak, agencija smije, samo dok su te okolnosti primjenjive, smatrati da se na evidencije ne primjenjuju zahtjevi iz ovog članka” (glava 5. članak 552. točka (c)(1) Zakonika SAD-a).

([221]) Glava 12. članak 3414. Zakonika SAD-a, glava 15. članci od 1681.u do 1681.v Zakonika SAD-a i glava 18. članak 2709. Zakonika SAD-a. Vidjeti uvodnu izjavu 153.

([222]) Glava 50. članak 1804. Zakonika SAD-a koji se odnosi na tradicionalan pojedinačan elektronički nadzor.

([223]) Glava 50. članak 1822. Zakonika SAD-a koji se odnosi na fizičke pretrage u svrhe stranih obavještajnih aktivnosti.

([224]) Glava 50. članak 1842. u vezi s člankom 1841. točkom 2. i glava 18. članak 3127. Zakonika SAD-a koji se odnose na postavljanje uređaja za bilježenje ulaznih i izlaznih poziva.

([225]) Glava 50. članak 1861. Zakonika SAD-a kojim se FBI-ju dopušta da podnese „zahtjev za nalog kojim se ovlašćuje javnog prijevoznika, javni smještajni objekt, subjekt za fizičko skladištenje ili subjekt za iznajmljivanje vozila da omogući pristup evidencijama u njihovu posjedu za potrebe istrage u kojoj se prikupljaju strane obavještajne informacije ili istrage međunarodnog terorizma”.

([226]) Glava 50. članak 1881.a Zakonika SAD-a, kojim se subjektima američke obavještajne zajednice dopušta da od američkih poduzeća zatraže pristup informacijama, uključujući sadržaj internetske komunikacije, radi ciljanog praćenja određenih osoba koje nisu američki državljani izvan SAD-a uz zakonski obveznu pomoć pružatelja elektroničke komunikacije.

(122) Američke obavještajne agencije mogu prikupljati osobne podatke i izvan SAD-a, među ostalim osobne podatke u tranzitu između Unije i SAD-a. Prikupljanje podataka izvan SAD-a temelji se na Izvršnom nalogu br. 12333 ([227]), koji je izdao predsjednik ([228]).

(123) Prikupljanje podataka elektroničkim izviđanjem najbitniji je način prikupljanja obavještajnih informacija za utvrđivanje primjerenosti u ovoj Odluci jer podrazumijeva prikupljanje elektroničke komunikacije i podataka iz informacijskih sustava. Američke obavještajne agencije mogu prikupljati podatke na taj način i u SAD-u (na temelju Zakona o nadzoru stranih obavještajnih aktivnosti) i dok su podaci u tranzitu prema SAD-u (na temelju Izvršnog naloga br. 12333).

(124) Američki predsjednik izdao je 7. listopada 2022. Izvršni nalog br. 14086 o poboljšanju zaštitnih mjera u američkim aktivnostima elektroničkog izviđanja, u kojem se utvrđuju ograničenja i zaštitne mjere za sve takve aktivnosti. Tim izvršnim nalogom uvelike je zamijenjen Predsjednički ukaz o politici br. 28 (PPD-28) ([229]), postrožuju se uvjeti, ograničenja i zaštitne mjere za sve aktivnosti elektroničkog izviđanja (tj. na temelju Zakona o nadzoru stranih obavještajnih aktivnosti i Izvršnog naloga br. 12333) neovisno o lokaciji na kojoj se provode ([230]) te se uvodi novi mehanizam pravne zaštite u okviru kojeg pojedinci mogu zatražiti provedbu tih zaštitnih mjera i tražiti ostvarenje svojeg prava na njih ([231]) (vidjeti detaljnije u uvodnim izjavama od 176. do 194.). Time se u američko pravo prenose ishodi pregovora EU-a i SAD-a održanih nakon što je Sud utvrdio da Komisijina odluka o primjerenosti sustava zaštite privatnosti nije valjana (vidjeti uvodnu izjavu 6.) Stoga je taj nalog posebno važan element pravnog okvira koji se ocjenjuje u ovoj Odluci.

(125) Ograničenja i zaštitne mjere uvedene Izvršnim nalogom br. 14086 dopunjuju ograničenja i zaštitne mjere iz članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti i Izvršnog naloga br. 12333. Obavještajne agencije moraju primjenjivati zahtjeve opisane u nastavku (u odjeljcima 3.2.1.2. i 3.2.1.3.) kad provode aktivnosti elektroničkog izviđanja u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti i Izvršnim nalogom br. 12333, na primjer pri odabiru/utvrđivanju kategorija stranih obavještajnih informacija koje će se prikupljati u skladu s člankom 702. tog zakona, prikupljanju stranih obavještajnih ili protuobavještajnih informacija u skladu s tim izvršnim nalogom te donošenju pojedinačnih odluka o ciljanom praćenju u skladu s člankom 702. tog zakona i tim izvršnim nalogom.

(126) Zahtjevi utvrđeni u tom izvršnom nalogu predsjednika obvezujući su za cijelu obavještajnu zajednicu. Mora ih se provesti u okviru agencijskih politika i postupaka kojima se prenose u konkretne upute za svakodnevni rad. U tom je pogledu Izvršnim nalogom br. 14086 predviđeno da američke obavještajne agencije imaju najviše godinu dana da ažuriraju svoje postojeće politike i postupke (tj. do 7. listopada 2023.) kako bi ih uskladile sa zahtjevima iz naloga. Pri ažuriranju politika i postupaka treba se savjetovati s glavnim državnim odvjetnikom, službenikom za zaštitu građanskih sloboda Ureda direktora za nacionalna obavještajna pitanja (ODNI) i PCLOB-om, koji je neovisno nadzorno tijelo ovlašteno za preispitivanje politika izvršne vlasti i njihove provedbe u cilju zaštite privatnosti i građanskih sloboda (za ulogu i status PCLOB-a vidjeti uvodnu izjavu 110.), te ih treba objaviti ([232]). Nadalje, nakon što se uvedu ažurirane politike i postupci, PCLOB će preispitati njihovu usklađenost s izvršnim nalogom. Nakon što PCLOB završi preispitivanje, svaka obavještajna agencija morat će u roku od 180 dana pažljivo razmotriti i provesti

([227]) *Executive Order 12333: United States Intelligence Activities* (Izvršni nalog br. 12333: Američke obavještajne aktivnosti) (Savezni registar, sv. 40, br. 235 (8. prosinca 1981. kako je izmijenjen 30. srpnja 2008.). U Izvršnom nalogu br. 12333 općenitije se određuju ciljevi, upute, dužnosti i odgovornosti američkih obavještajnih službi (uključujući ulogu raznih subjekata obavještajne zajednice) te su utvrđeni opći parametri za provedbu obavještajnih aktivnosti.

([228]) U skladu s člankom II. američkog Ustava za nacionalnu sigurnost, osobito za prikupljanje stranih obavještajnih informacija, odgovoran je predsjednik kao vrhovni zapovjednik oružanih snaga.

([229]) Izvršni nalog br. 14086 zamjenjuje prethodni predsjednički ukaz, Predsjednički ukaz o politici br. 28, osim njegova članka 3. i dopunskog Priloga (kojim je propisano da obavještajne agencije svake godine moraju preispitati svoje prioritete i zahtjeve za elektroničko izviđanje uzimajući u obzir prednosti aktivnosti elektroničkog izviđanja za nacionalne interese SAD-a i rizik koji one donose) te članka 6. (koji sadržava opće odredbe), vidjeti Memorandum o nacionalnoj sigurnosti o djelomičnom stavljanju izvan snage Predsjedničkog ukaza o politici br. 28, dostupan na https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/

([230]) Vidjeti članak 5. točku (f) Izvršnog naloga br. 14086, u kojem je objašnjeno da taj izvršni nalog ima isto područje primjene kao Predsjednički ukaz o politici br. 28, koji se prema bilješci 3. ukaza primjenjuje na aktivnosti elektroničkog izviđanja koje se provode radi prikupljanja komunikacije ili informacija o komunikaciji, osim kad se provode radi ispitivanja ili razvoja kapaciteta za te aktivnosti.

([231]) U tom pogledu vidjeti npr. članak 5. točku (h) Izvršnog naloga br. 14086, u kojem je pojašnjeno da su zaštitne mjere iz naloga zakonsko pravo čije ostvarenje pojedinci mogu tražiti u okviru mehanizma pravne zaštite.

([232]) Vidjeti članak 2. točku (c)(iv)(C) Izvršnog naloga br. 14086.

sve preporuke PCLOB-a ili ih na drugi način uzeti u obzir. Američka vlada objavila je 3. srpnja 2023. ažurirane politike i postupke ([233]).

3.2.1.2. *Ograničenja i zaštitne mjere pri prikupljanju osobnih podataka u svrhe nacionalne sigurnosti*

(127) Izvršnim nalogom br. 14086 utvrđuje se niz glavnih zahtjeva za sve aktivnosti elektroničkog izviđanja (prikupljanje, uporaba, širenje itd. osobnih podataka).

(128) Prvo, te aktivnosti moraju se provoditi na temelju zakona ili predsjedničkog odobrenja te u skladu s američkim pravom, uključujući Ustav ([234]).

(129) Drugo, moraju se uspostaviti odgovarajuće zaštitne mjere kojima se jamči da se pri planiranju tih aktivnosti vodi računa o privatnosti i građanskim slobodama ([235]).

(130) Točnije, aktivnosti elektroničkog izviđanja mogu se provoditi tek „nakon što se, na temelju razumne procjene svih relevantnih čimbenika, utvrdi da su te aktivnosti nužne za ostvarenje potvrđenog obavještajnog prioriteta" (kad je riječ o „potvrđenom obavještajnom prioritetu", vidjeti uvodnu izjavu 135.) ([236]).

(131) Nadalje, te aktivnosti mogu se provoditi samo „u mjeri i na način koji su proporcionalni potvrđenom obavještajnom prioritetu za čije su ostvarenje odobrene" ([237]). Drugim riječima, mora se postići dobra ravnoteža „između važnosti predviđenog obavještajnog prioriteta te utjecaja na privatnost i građanske slobode pojedinaca u vezi s kojima se provode aktivnosti, neovisno o njihovu državljanstvu ili boravištu" ([238]).

(132) Naposljetku, kako bi se zajamčila usklađenost s tim općim zahtjevima, koji se temelje na načelima zakonitosti, nužnosti i proporcionalnosti, aktivnosti elektroničkog izviđanja podliježu nadzoru (vidjeti detaljnije u odjeljku 3.2.2.) ([239]).

(133) Te glavne zahtjeve u pogledu prikupljanja podataka elektroničkim izviđanjem dodatno dopunjuje niz uvjeta i ograničenja kojima se osigurava da je zadiranje u prava pojedinaca ograničeno na ono što je nužno i proporcionalno za ostvarenje legitimnog cilja.

(134) Prvo, razlozi na temelju kojih se podaci mogu prikupljati elektroničkim izviđanjem na dva su načina ograničeni u Izvršnim nalogom. S jedne strane, Izvršnim nalogom utvrđuju se legitimni ciljevi koji se mogu ostvarivati prikupljanjem podataka elektroničkim izviđanjem, na primjer utvrđivanje ili procjena kapaciteta, namjera ili aktivnosti stranih organizacija, uključujući međunarodne terorističke organizacije, koje su prijetnja ili bi mogle biti prijetnja nacionalnoj sigurnosti SAD-a, zaštita od stranih vojnih kapaciteta i aktivnosti, utvrđivanje ili procjena transnacionalnih prijetnji globalnoj sigurnosti, kao što su klimatske i druge ekološke promjene, rizici za javno zdravlje i humanitarne prijetnje ([240]). S druge strane Izvršni nalog sadržava popis određenih ciljeva koji se nikad ne smiju nastojati ostvariti aktivnostima elektroničkog izviđanja, na primjer suzbijanje kritike, neslaganja ili slobodnog

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

([234]) Članak 2. točka (a)(i) Izvršnog naloga br. 14086.

([235]) Članak 2. točka (a)(ii) Izvršnog naloga br. 14086.

([236]) Članak 2. točka (a)(ii)(A) Izvršnog naloga br. 14086. Pritom elektroničko izviđanje ne mora uvijek biti jedino sredstvo ostvarenja aspekata potvrđenog obavještajnog prioriteta. Na primjer, prikupljanje podataka elektroničkim izviđanjem može se upotrijebiti kako bi se uspostavili alternativni načini potvrđivanja (npr. kako bi se potvrdile informacije iz drugog obavještajnog izvora) ili zadržao pouzdan pristup istim informacijama (članak 2. točka (c)(i)(A) Izvršnog naloga br. 14086).

([237]) Članak 2. točka (a)(ii)(B) Izvršnog naloga br. 14086.

([238]) Članak 2. točka (a)(ii)(B) Izvršnog naloga br. 14086.

([239]) Članak 2. točka (a)(iii) u vezi s člankom 2. točkom (d) Izvršnog naloga br. 14086.

([240]) Članak 2. točka (b)(i) Izvršnog naloga br. 14086. Budući da sadržava ograničen popis legitimnih ciljeva, koji ne obuhvaća moguće buduće prijetnje, izvršnim nalogom predviđa se mogućnost da predsjednik ažurira taj popis ako se pojave nove potrebe u području nacionalne sigurnosti, kao što su nove prijetnje nacionalnoj sigurnosti. Ta se ažuriranja u načelu moraju objaviti, osim ako predsjednik utvrdi da bi to stvorilo rizik za nacionalnu sigurnost SAD-a (članak 2. točka (b)(i)(B) Izvršnog naloga br. 14086).

izražavanja ideja ili političkih stajališta pojedinaca ili medija, stavljanje u nepovoljniji položaj osoba na temelju njihova etničkog podrijetla, rase, roda, rodnog identiteta, spolne orijentacije odnosno vjere ili osiguravanje konkurentske prednosti američkim poduzećima ([241]).

(135) Osim toga, obavještajne agencije ne mogu se pozvati samo na legitimne ciljeve iz Izvršnog naloga br. 14086 kako bi opravdale prikupljanje podataka elektroničkim izviđanjem, nego ih za operativne potrebe moraju dodatno potkrijepiti konkretnijim prioritetima zbog kojih se podaci prikupljaju elektroničkim izviđanjem. Drugim riječima, podaci se mogu prikupljati samo za ostvarenje konkretnijeg prioriteta. Ti se prioriteti utvrđuju posebnim postupkom kako bi bili usklađeni s primjenjivim pravnim zahtjevima, uključujući zahtjeve u pogledu privatnosti i građanskih sloboda. Točnije, obavještajne prioritete prvo sastavlja direktor za nacionalna obavještajna pitanja (kao dio Okvira za nacionalne obavještajne prioritete) i podnosi ih na odobrenje predsjedniku ([242]). Prema Izvršnom nalogu br. 14086, prije nego što predsjedniku predloži obavještajne prioritete, direktor mora za svaki prioritet od službenika za zaštitu građanskih sloboda ODNI-ja ishoditi procjenu 1. da se prioritetom nastoji ostvariti jedan ili više legitimnih ciljeva iz Izvršnog naloga, 2. da prioritet nije osmišljen da dovede niti se očekuje da će dovesti do prikupljanja podataka elektroničkim izviđanjem za cilj zabranjen Izvršnim nalogom i 3. da je prioritet postavljen nakon što su se u odgovarajućoj mjeri uzele u obzir privatnost i građanske slobode svih osoba neovisno o njihovu državljanstvu ili boravištu ([243]). Ako se direktor ne slaže s procjenom službenika za zaštitu građanskih sloboda, oba stajališta moraju se podnijeti predsjedniku ([244]).

(136) Stoga se tim postupkom prvenstveno osigurava da se privatnost uzima u obzir već na početku, pri utvrđivanju obavještajnih prioriteta.

(137) Drugo, nakon utvrđivanja obavještajnog prioriteta mora se ispuniti niz zahtjeva kako bi se odlučilo mogu li se i u kojoj mjeri podaci prikupljati elektroničkim izviđanjem da bi se ostvario taj prioritet. Ti zahtjevi služe provedbi glavnih standarda nužnosti i proporcionalnosti iz članka 2. točke (a) Izvršnog naloga.

(138) Naime, podaci se mogu prikupljati elektroničkim izviđanjem tek „nakon što se, na temelju razumne procjene svih relevantnih čimbenika, utvrdi da je prikupljanje nužno za ostvarenje određenog obavještajnog prioriteta” ([245]). Kad utvrđuju je li određena aktivnost prikupljanja podataka elektroničkim izviđanjem nužna za ostvarenje potvrđenog obavještajnog prioriteta, američke obavještajne agencije moraju razmotriti jesu li drugi manje izvori i metode kojima se manje zadire u privatnost, uključujući diplomatske i javne izvore, dostupni, izvedivi i primjereni ([246]). Ako su dostupni, mora se dati prednost tim alternativnim izvorima i metodama kojima se manje zadire u privatnost ([247]).

(139) Ako se primjenom tih kriterija utvrdi da je prikupljanje podataka elektroničkim izviđanjem nužno, prikupljanje podataka mora biti „što usmjerenije” i „ne smij[e] nerazmjerno utjecati na privatnost i građanske slobode” ([248]). Kako bi se izbjegao nerazmjeran utjecaj na privatnost i građanske slobode, tj. kako bi se postigla dobra ravnoteža između potreba u području nacionalne sigurnosti te zaštite privatnosti i građanskih sloboda, u obzir se moraju uzeti svi relevantni čimbenici, kao što su priroda postavljenog cilja, mjera u kojoj se aktivnostima prikupljanja zadire u privatnost, uključujući njihovo trajanje, vjerojatan doprinos prikupljanja ostvarenju postavljenog cilja, razumno predvidive posljedice za pojedince te priroda i osjetljivost podataka koji će se prikupljati ([249]).

([241]) Članak 2. točka (b)(ii) Izvršnog naloga br. 14086.
([242]) Članak 102A Zakona o nacionalnoj sigurnosti i članak 2. točka (b)(iii) Izvršnog naloga br. 14086.
([243]) U iznimnim slučajevima (posebno kad se taj postupak ne može provesti jer treba ispuniti novi ili promjenjiv obavještajni zahtjev) te prioritete može utvrditi izravno predsjednik ili čelnik subjekta obavještajne zajednice, koji u načelu treba primjenjivati iste kriterije kao one iz članka 2. točki (b)(iii)(A)(1)–(3), vidjeti članak 4. točku (n) Izvršnog naloga br. 14086.
([244]) Članak 2. točka (b)(iii)(C) Izvršnog naloga br. 14086.
([245]) Članak 2. točke (b) i (c)(i)(A) Izvršnog naloga br. 14086.
([246]) Članak 2. točka (c)(i)(A) Izvršnog naloga br. 14086.
([247]) Članak 2. točka (c)(i)(A) Izvršnog naloga br. 14086.
([248]) Članak 2. točka (c)(i)(B) Izvršnog naloga br. 14086.
([249]) Članak 2. točka (c)(i)(B) Izvršnog naloga br. 14086.

(140) Prikupljanje podataka u SAD-u, kao najbitnija vrsta prikupljanja podataka elektroničkim izviđanjem za utvrđivanje primjerenosti u ovoj Odluci jer se odnosi na podatke koji su preneseni u organizacije u SAD-u, uvijek mora biti ciljano, kako je detaljnije objašnjeno u uvodnim izjavama od 142. do 153.

(141) U skladu s Izvršnim nalogom br. 12333 podaci se mogu „skupno prikupljati" ([250]) samo izvan SAD-a. U tom se slučaju u skladu s Izvršnim nalogom br. 14086 prednost mora dati ciljanom prikupljanju ([251]). Stoga je skupno prikupljanje dopušteno samo ako se informacije nužne za ostvarenje potvrđenog obavještajnog prioriteta iz opravdanih razloga ne mogu dobiti ciljanim prikupljanjem ([252]). Kad je nužno skupno prikupiti podatke izvan SAD-a, primjenjuju se posebne zaštitne mjere iz Izvršnog naloga br. 14086 ([253]). Prvo, moraju se provesti metode i tehničke mjere za ograničavanje prikupljanja samo na one podatke koji su nužni za ostvarenje potvrđenog obavještajnog prioriteta i na što manju količinu nerelevantnih informacija ([254]). Drugo, uporaba skupno prikupljenih informacija (uključujući pretraživanje) ograničena je Izvršnim nalogom na šest konkretnih ciljeva, koji uključuju zaštitu od terorizma, uzimanja taoca i zatočeništva u kojem pojedince drži strana vlada, organizacija ili osoba ili u kojem ih se drži u ime strane vlade, organizacije ili osobe, zaštitu od strane špijunaže, sabotaže ili atentata te zaštitu od prijetnji od razvoja, posjedovanja ili širenja oružja za masovno uništenje ili povezanih tehnologija i prijetnji ([255]). Naposljetku, podaci skupno prikupljeni elektroničkim izviđanjem mogu se pretraživati samo ako je to nužno za ostvarenje potvrđenog obavještajnog prioriteta, ako se time nastoji ostvariti tih šest ciljeva i ako je u skladu s politikama i postupcima kojima se u odgovarajućoj mjeri uzima u obzir utjecaj pretraživanja na privatnost i građanske slobode svih osoba neovisno o njihovu državljanstvu ili boravištu ([256]).

(142) Osim zahtjevima iz Izvršnog naloga br. 14086, prikupljanje elektroničkim izviđanjem podataka koji su preneseni u organizaciju u SAD-u podliježe određenim ograničenjima i zaštitnim mjerama iz članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti ([257]). U skladu s tim člankom strane obavještajne informacije mogu se, uz zakonski obveznu pomoć američkih pružatelja usluga elektroničke komunikacije, prikupljati ciljanim praćenjem osoba koje nisu američki državljani, a za koje se iz opravdanih razloga vjeruje da se nalaze izvan SAD-a ([258]). Kako bi se strane

([250]) Tj. prikupljanje velike količine podataka elektroničkim izviđanjem koji su iz tehničkih ili operativnih razloga prikupljeni bez primjene razlikovnih čimbenika (npr. bez uporabe posebnih identifikatora ili čimbenika za odabir), vidjeti članak 4. točku (b) Izvršnog naloga br. 14086. Kako je dodatno objašnjeno u uvodnoj izjavi 141., u skladu s Izvršnim nalogom br. 14086 podaci se skupno prikupljaju na temelju Izvršnog naloga br. 12333 samo ako je to nužno za ostvarivanje određenih potvrđenih obavještajnih prioriteta i pritom se primjenjuje niz ograničenja i zaštitnih mjera za sprečavanje neselektivnog pristupa podacima. Skupno prikupljanje stoga se razlikuje od generaliziranog i neselektivnog prikupljanja („masovni nadzor") bez ograničenja i zaštitnih mjera.

([251]) Članak 2. točka (c)(ii)(A) Izvršnog naloga br. 14086.

([252]) Članak 2. točka (c)(ii)(A) Izvršnog naloga br. 14086.

([253]) Posebna pravila o skupnom prikupljanju iz Izvršnog naloga br. 14086 primjenjuju se i na ciljane aktivnosti prikupljanja podataka elektroničkim izviđanjem u kojima se privremeno upotrebljavaju podaci prikupljeni bez razlikovnih čimbenika (npr. posebni čimbenici za odabir ili identifikatori), tj. skupno prikupljeni podaci (što je moguće samo izvan državnog područja SAD-a). To nije slučaj ako se takvi podaci upotrebljavaju samo za potporu početnoj tehničkoj fazi ciljanih aktivnosti prikupljanja podataka elektroničkim izviđanjem, čuvaju samo kratko razdoblje potrebno za dovršetak te faze i odmah nakon toga brišu (članak 2. točka (c)(ii)(D) Izvršnog naloga br. 14086). U tom je slučaju jedina svrha početnog prikupljanja bez razlikovnih čimbenika omogućiti ciljano prikupljanje informacija primjenom posebnog identifikatora ili čimbenika za odabir. U tom se slučaju samo podaci dohvaćeni primjenom određenog razlikovnog čimbenika unose u vladine baze podataka, a ostali se podaci uništavaju. Stoga je takvo ciljano prikupljanje i dalje uređeno općim pravilima za prikupljanje podataka elektroničkim izviđanjem, među ostalim člankom 2. točkama od (a) do (b) i (c)(i) Izvršnog naloga br. 14086.

([254]) Članak 2. točka (c)(ii)(A) Izvršnog naloga br. 14086.

([255]) Članak 2. točka (c)(ii)(B) Izvršnog naloga br. 14086. Ako se pojave nove potrebe u području nacionalne sigurnosti, kao što su nove prijetnje nacionalnoj sigurnosti, predsjednik može ažurirati taj popis. Ta se ažuriranja u načelu moraju objaviti, osim ako predsjednik utvrdi da bi to stvorilo rizik za nacionalnu sigurnost SAD-a (članak 2. točka (c)(ii)(C) Izvršnog naloga br. 14086). Kad je riječ o pretraživanju skupno prikupljenih podataka, vidjeti članak 2. točku (c)(iii)(D) Izvršnog naloga br. 14086.

([256]) Članak 2. točka (a)(iii)(A) u vezi s člankom 2. točkom (c)(iii)(D) Izvršnog naloga br. 14086. Vidjeti i Prilog VII.

([257]) Glava 50. članak 1881. Zakonika SAD-a.

([258]) Glava 50. članak 1881.a točka (a) Zakonika SAD-a. Točnije, kao što navodi PCLOB, nadzor na temelju članka 702. „u cijelosti se sastoji od ciljanog praćenja određenih osoba [koje nisu američki državljani i] za koje je utvrđeno da ih se treba ciljano pratiti" (Odbor za nadzor privatnosti i građanskih sloboda, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2. srpnja 2014., Izvješće o članku 702., str. 111.). Vidjeti i izvješće Službenika za zaštitu građanskih sloboda Nacionalne sigurnosne agencije, *NSA's Implementation of Foreign Intelligence Act Section 702*, 16. travnja 2014. Pojam „pružatelj usluga elektroničke komunikacije" definiran je u glavi 50. članku 1881. točki (a)(4) Zakonika SAD-a.

obavještajne informacije prikupljale u skladu s člankom 702., glavni državni odvjetnik i direktor za nacionalna obavještajna pitanja podnose Sudu za nadzor stranih obavještajnih aktivnosti (FISC) godišnje potvrde o kategorijama stranih obavještajnih informacija koje će se prikupljati ([259]). Potvrde moraju biti popraćene postupcima ciljanog praćenja, smanjenja količine i pretraživanja, koje također odobrava taj sud i koji su pravno obvezujući za američke obavještajne agencije.

(143) FISC je neovisni sud ([260]) osnovan saveznim zakonom na čije se odluke može žaliti Žalbenom sudu za nadzor stranih obavještajnih aktivnosti (FISCR) ([261]) i, na najvišem stupnju, Vrhovnom sudu SAD-a ([262]). FISC-u (i FISCR-u) pomaže stalni odbor od pet odvjetnika i pet tehničkih stručnjaka specijaliziranih za pitanja nacionalne sigurnosti i građanskih sloboda ([263]). 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 ([264]). Time se prije svega osigurava da su pitanja privatnosti primjereno uključena u procjenu suda. Sud može kad god to smatra primjerenim imenovati i pojedinca ili organizaciju kao *amicus curiae* koji, među ostalim, pruža tehničke savjete, ili na zahtjev dopustiti pojedincu ili organizaciji da podnesu sažetak *amicus curiae* ([265]).

(144) FISC preispituje jesu li potvrde i povezani postupci (osobito ciljano praćenje i smanjenje količine podataka) usklađeni sa zahtjevima Zakona o nadzoru stranih obavještajnih aktivnosti. Ako smatra da zahtjevi nisu ispunjeni, može odbiti potvrdu u cijelosti ili djelomično te zahtijevati izmjenu postupaka ([266]). FISC je u tom pogledu u više navrata potvrdio da njegovo preispitivanje postupaka ciljanog praćenja i smanjenja količine podataka u skladu s člankom 702. nije ograničeno na pisani opis postupaka nego obuhvaća i način na koji ih vlada provodi ([267]).

(145) Nacionalna sigurnosna agencija (NSA) (obavještajna agencija odgovorna za ciljano praćenje u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti) utvrđuje treba li određenog pojedinca ciljano pratiti u skladu s postupcima za ciljano praćenje koje je odobrio FISC, prema kojima agencija mora na temelju svih okolnosti procijeniti je li vjerojatno da će se ciljanim praćenjem određene osobe prikupiti strane obavještajne informacije navedene u potvrdi ([268]). Ta procjena mora biti detaljna i temeljiti se na činjenicama te u njoj treba uzeti u obzir

([259]) Glava 50. članak 1881a. točka (g) Zakonika SAD-a.

([260]) FISC čine suci koje predsjednik Vrhovnog suda SAD-a imenuje iz redova sudaca američkih okružnih sudova, koje je prethodno imenovao predsjednik i potvrdio Senat. Suci, koji imaju doživotni mandat i koje je moguće razriješiti samo iz valjanog razloga, imenuju se u FISC na sedmogodišnje mandate koji se ne preklapaju. U skladu sa Zakonom o nadzoru stranih obavještajnih aktivnosti suci se imenuju iz najmanje sedam različitih sudačkih okruga SAD-a. Vidjeti glavu 50. članak 1803. točku (a) Zakonika SAD-a. Sucima pomažu iskusni sudski službenici koji su pravni stručnjaci suda i izrađuju pravnu analizu zahtjeva za prikupljanje podataka. Vidjeti Dopis časnog suca Reggieja B. Waltona, predsjedavajućeg suca Suda za nadzor stranih obavještajnih aktivnosti, časnom sucu Patricku J. Leahyju, predsjedniku Odbora za pravosuđe Senata SAD-a (29. srpnja 2013.) (Waltonov dopis), str. 2., dostupan na https://fas.org/irp/news/2013/07/fisc-leahy.pdf

([261]) FISCR čine suci koje predsjednik Vrhovnog suda SAD-a imenuje iz redova sudaca okružnih ili žalbenih sudova SAD-a na sedmogodišnje mandate koji se ne preklapaju. Vidjeti glavu 50. članak 1803. točku (b) Zakonika SAD-a.

([262]) Vidjeti glavu 50. članak 1803. točku (b), članak 1861a. točku (f) te članak 1881a. točke (h) i (i)(4) Zakonika SAD-a.

([263]) Glava 50. članak 1803. točke (i)(1) i (i)(3)(A) Zakonika SAD-a.

([264]) Glava 50. članak 1803. točka (i)(2)(A) Zakonika SAD-a.

([265]) Glava 50. članak 1803. točka (i)(2)(B) Zakonika SAD-a.

([266]) Vidjeti npr. Mišljenje FISC-a od 18. listopada 2018., dostupno na: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, kako ga je potvrdio Žalbeni sud za nadzor stranih obavještajnih aktivnosti u svojem Mišljenju od 12. srpnja 2019., dostupno na: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf

([267]) Vidjeti npr. FISC, Sažeta sudska odluka i nalog (18. studenoga 2020.) (odobreno za objavu 26. travnja 2021.), str. 35., (Prilog D).

([268]) Glava 50. članak 1881.a točka (a) Zakonika SAD-a, Postupci koje Nacionalna sigurnosna agencija upotrebljava za ciljano praćenje osoba koje nisu američki državljani, a za koje je iz opravdanih razloga vjerojatno da se nalaze izvan SAD-a, kako bi prikupila strane obavještajne informacije u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti iz 1978., kako je izmijenjen, iz ožujka 2018. (NSA-ovi postupci ciljanog praćenja), dostupno na https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, str. 1.–4., dodatno objašnjeno u Izvješću PCLOB-a, str. 41.–42.

analitičko prosuđivanje, specijalizirano osposobljavanje i iskustvo analitičara te prirodu stranih obavještajnih informacija koje će se dobiti ([269]). Ciljano praćenje provodi se tako da se odrede selektori kojima se označuju određena komunikacijska sredstva, kao što su e-adresa ili telefonski broj ciljane osobe, ali nikada ključne riječi ni imena pojedinaca ([270]).

(146) NSA-ovi analitičari prvo će identificirati osobe u inozemstvu koje nisu američki državljani i čijim nadzorom će se, na temelju procjene analitičara, prikupiti relevantni strani obavještajni podaci navedeni u potvrdi ([271]). Kako je navedeno u NSA-ovim postupcima ciljanog praćenja, NSA može nadzoru podvrgnuti određenu ciljanu osobu tek kad već ima neke informacije o njoj ([272]). Te informacije mogu potjecati iz raznih izvora, na primjer ljudskih izvora. Analitičar mora iz njih saznati i koji konkretni selektor (tj. komunikacijski račun) upotrebljava potencijalna ciljana osoba. Kad se te izdvojene osobe identificiraju te se ciljano praćenje odobri opsežnim mehanizmom preispitivanja u okviru NSA-a ([273]), „zadat" će se (odnosno izraditi i primijeniti) selektori kojima se utvrđuju komunikacijska sredstva (kao što su e-adrese) kojima se koriste ciljane osobe ([274]).

(147) NSA mora evidentirati činjeničnu osnovu za odabir ciljane osobe ([275]) i nakon početnog ciljanog praćenja redovito potvrđivati je li i dalje ispunjen standard za ciljano praćenje ([276]). Kad on više nije ispunjen, prikupljanje podataka mora prestati ([277]). Svaka dva mjeseca službenici uredâ za nadzor obavještajnih aktivnosti pri Ministarstvu pravosuđa, koji o povredi propisa moraju obavijestiti FISC i Kongres, preispituju jesu li način na koji je NSA odabrao ciljane osobe i njegova evidencija o svakoj evidentiranoj procjeni i obrazloženju za ciljano praćenje u skladu s postupcima ciljanog praćenja ([278]). NSA-ova pisana dokumentacija olakšava FISC-u da nadzire jesu li pojedinci pravilno ciljano praćeni na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti u skladu sa svojim nadzornim ovlastima opisanima u uvodnim izjavama od 173. do 174. ([279]) Naposljetku, direktor za nacionalna obavještajna pitanja dužan je svake godine za javna godišnja statistička izvješća o transparentnosti podnijeti izvješće o ukupnom broju ciljanih osoba praćenih na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti. Poduzeća kojima su upućeni nalozi na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti mogu (u izvješćima o transparentnosti) objaviti agregirane podatke o zaprimljenim zahtjevima ([280]).

([269]) NSA-ovi postupci ciljanog praćenja, str. 4.

([270]) Vidjeti PCLOB, Izvješće o članku 702., str. 32.–33. i 45. s daljnjim upućivanjima. Vidjeti i Polugodišnju ocjenu usklađenosti s postupcima i smjernicama izdanima u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti, koju su podnijeli glavni državni odvjetnik i direktor za nacionalna obavještajna pitanja, Izvještajno razdoblje: 1. prosinca 2016.–31. svibnja 2017., str. 41. (listopad 2018.), dostupno na: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) PCLOB, Izvješće o članku 702., str. 42.–43.

([272]) NSA-ovi postupci ciljanog praćenja, str. 2.

([273]) PCLOB, Izvješće o članku 702., str. 46. Na primjer, NSA mora provjeriti postoji li veza između ciljane osobe i selektora, 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 i izvješće Službenika za zaštitu građanskih sloboda Nacionalne sigurnosne agencije, *NSA's Implementation of Foreign Intelligence Act Section 702*, 16. travnja 2014.

([274]) Glava 50. članak 1881a. točka (h) Zakonika SAD-a.

([275]) NSA-ovi postupci ciljanog praćenja, str. 8. Vidjeti i PCLOB, Izvješće o članku 702., str. 46. Nedostavljanje pisanog obrazloženja predstavlja slučaj neusklađenosti s propisima o dokumentaciji o kojem se moraju obavijestiti FISC i Kongres. Vidjeti Polugodišnju ocjenu usklađenosti s postupcima i smjernicama izdanima u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti, koju su podnijeli glavni državni odvjetnik i direktor za nacionalna obavještajna pitanja, Izvještajno razdoblje: 1. prosinca 2016.–31. svibnja 2017., str. 41. (listopad 2018.), Izvješće Ministarstva pravosuđa i ODNI-ja FISC-u o usklađenosti za razdoblje od prosinca 2016. do svibnja 2017., str. A-6, dostupno na: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

([276]) Vidjeti podnesak američke vlade Sudu za nadzor stranih obavještajnih aktivnosti, *2015 Summary of Notable Section 702 Requirements* (Sažetak iz 2015. o najvažnijim zahtjevima iz članka 702.), str. 2.–3. (15. srpnja 2015.) i informacije iz Priloga VII.

([277]) Vidjeti podnesak američke vlade Sudu za nadzor stranih obavještajnih aktivnosti, *2015 Summary of Notable Section 702 Requirements* (Sažetak iz 2015. o najvažnijim zahtjevima iz članka 702.), str. 2.–3. (15. srpnja 2015.), u kojem je navedeno da „ako Vlada naknadno ocijeni da se ne očekuje da će daljnje zadavanje selektora ciljane osobe dovesti do prikupljanja stranih obavještajnih informacija, potrebno je odmah poništiti zadavanje, a njegova odgoda može predstavljati slučaj neusklađenosti o kojem se može obavijestiti nadležno tijelo". Vidjeti i informacije u Prilogu VII.

([278]) PCLOB, Izvješće o članku 702., str. 70.–72. Pravilo 13. točka (b) Poslovnika Suda SAD-a za nadzor obavještajnih aktivnosti, dostupno na: https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf

([279]) Vidjeti i Izvješće Ministarstva pravosuđa i ODNI-ja FISC-u o usklađenosti za razdoblje od prosinca 2016. do svibnja 2017., str. A-6.

([280]) Glava 50. članak 1874. Zakonika SAD-a.

(148) Kad je riječ o drugim pravnim osnovama za prikupljanje osobnih podataka koji su preneseni u organizacije u SAD-u, primjenjuju se razna ograničenja i zaštitne mjere. Skupno prikupljanje podataka općenito je izričito zabranjeno na temelju članka 402. Zakona o nadzoru stranih obavještajnih aktivnosti (ovlast za bilježenje ulaznih i izlaznih poziva) i dopisa o nacionalnoj sigurnosti te se umjesto toga moraju upotrebljavati posebni „čimbenici za odabir” ([281]).

(149) Za potrebe tradicionalnog individualiziranog elektroničkog nadzora (u skladu s člankom 105. Zakona o nadzoru stranih obavještajnih aktivnosti) obavještajne agencije moraju FISC-u podnijeti zahtjev koji uključuje izjavu o činjenicama i okolnostima na temelju kojih se vjeruje da postoji osnovana sumnja da se sredstvom koristi ili će se njime koristiti strana sila ili agent strane sile ([282]). FISC će ocijeniti, među ostalim, postoji li na temelju podnesenih činjenica osnovana sumnja da je to doista tako ([283]).

(150) Za potrebe pretrage prostora ili imovine koja bi trebala dovesti do pregleda, zapljene itd. informacija, dokumenata ili imovine (npr. računalni uređaj) u skladu s člankom 301. Zakona o nadzoru stranih obavještajnih aktivnosti FISC-u se mora podnijeti zahtjev za nalog ([284]). U tom se zahtjevu mora među ostalim dokazati da postoji osnovana sumnja da je osoba koja je predmet pretrage strana sila ili agent strane sile, da se u prostoru ili imovini koja će se pretraživati nalaze strane obavještajne informacije i da je strana sila (ili njezin agent) vlasnik prostora koji će se pretraživati, koristi se njime, uživa posjed tog prostora ili se prenosi s nje ili na nju ([285]).

(151) Slično tomu, za postavljanje uređaja za bilježenje ulaznih ili izlaznih poziva (na temelju članka 402. Zakona o nadzoru stranih obavještajnih aktivnosti) potrebni su zahtjev za nalog FISC-a (ili američkog pomoćnog suca) i primjena konkretnog čimbenika za odabir, tj. pojma kojim se točno određuje osoba, račun itd. i koji služi da bi se u najvećoj razumno mogućoj mjeri ograničio opseg traženih informacija ([286]) Ta se ovlast ne odnosi na sadržaj komunikacije, već joj je svrha informiranje o klijentu ili pretplatniku koji se koristi uslugom (kao što su ime, adresa, pretplatnički broj, trajanje/vrsta primljene usluge, izvor/mehanizam plaćanja).

(152) U skladu s člankom 501. Zakona o nadzoru stranih obavještajnih aktivnosti ([287]) za prikupljanje poslovnih evidencija javnog prijevoznika (svaka osoba ili subjekt koji za naknadu prevozi osobe ili imovinu kopnom, zrakom, prugom, vodom ili zrakom), javnog smještajnog objekta (npr. hotel, motel ili prenoćište), subjekta za iznajmljivanje vozila ili subjekta za fizičko skladištenje (koji pruža prostor za skladištenje robe i materijala ili s tim povezane usluge) ([288]) potrebno je podnijeti zahtjev FISC-u ili pomoćnom sucu. U njemu se moraju navesti tražene evidencije te konkretne i razumljive činjenice zbog kojih se vjeruje da je osoba kojoj evidencije pripadaju strana sila ili agent strane sile ([289]).

(153) Naposljetku, dopisi o nacionalnoj sigurnosti temelje se na raznim zakonima, a istražnim agencijama omogućuju da od određenih subjekata (npr. financijske ustanove, agencije za izvješćivanje o kreditnoj sposobnosti, pružatelji elektroničke komunikacije) prikupe određene informacije (isključujući sadržaj komunikacije) koje se nalaze u izvješćima o kreditnoj sposobnosti, financijskim evidencijama i elektroničkim evidencijama o pretplatnicima i transakcijama ([290]). Propisom o dopisima o nacionalnoj sigurnosti pristup elektroničkoj komunikaciji dopušta se samo FBI-ju te je u njemu utvrđeno da se u zahtjevu mora navesti izraz koji točno određuje osobu, subjekt, telefonski broj ili račun i potvrditi da je informacija relevantna za ovlaštenu istragu u području nacionalne sigurnosti radi zaštite od međunarodnog terorizma ili tajnih obavještajnih aktivnosti ([291]). Primatelji dopisa o nacionalnoj sigurnosti imaju pravo osporavati ga pred sudom ([292]).

([281]) Glava 50. članak 1842. točka (c)(3) Zakonika SAD-a i, kad je riječ o dopisima o nacionalnoj sigurnosti, glava 12. članak 3414. točka (a)(2) Zakonika SAD-a, glava 15. članak 1681.u Zakonika SAD-a, glava 15. članak 1681.v točka (a) Zakonika SAD-a i glava 18. članak 2709. točka (a) Zakonika SAD-a.

([282]) „Agent strane sile” može biti osoba koja nije američki državljanin i koja sudjeluje u međunarodnom terorizmu ili međunarodnom širenju oružja za masovno uništenje (uključujući pripremne radnje) (glava 50. članak 1801. točka (b)(1) Zakonika SAD-a).

([283]) Glava 50. članak 1804. Zakonika SAD-a. Vidjeti i članak 1841. točku 4. za izbor čimbenika za odabir.

([284]) Glava 50. članak 1821. točka (5) Zakonika SAD-a.

([285]) Glava 50. članak 1823. točka (a) Zakonika SAD-a.

([286]) Glava 50. članak 1842. u vezi s člankom 1841. točkom (2) i glava 18. članak 3127. Zakonika SAD-a.

([287]) Glava 50. članak 1862. Zakonika SAD-a.

([288]) Glava 50. članci od 1861. do 1862. Zakonika SAD-a.

([289]) Glava 50. članak 1862. točka (b) Zakonika SAD-a.

([290]) Glava 12. članak 3414. Zakonika SAD-a, glava 15. članci od 1681.u do 1681.v Zakonika SAD-a i glava 18. članak 2709. Zakonika SAD-a.

([291]) Glava 18. članak 2709. točka (b) Zakonika SAD-a.

([292]) Npr. glava 18. članak 2709. točka (d) Zakonika SAD-a.

3.2.1.3. *Daljnja uporaba prikupljenih informacija*

(154) Za obradu osobnih podataka koje su američke obavještajne agencije prikupile elektroničkim izviđanjem postoji niz zaštitnih mjera.

(155) Prvo, svaka obavještajna agencija mora osigurati odgovarajuću sigurnost podataka i spriječiti pristup neovlaštenih osoba osobnim podacima prikupljenima elektroničkim izviđanjem. U tom se pogledu u brojnim instrumentima, uključujući zakone, smjernice i standarde, dodatno preciziraju minimalni zahtjevi informacijske sigurnosti koje treba provesti (npr. višerazinska autentifikacija ili šifriranje) ([293]). Pristup prikupljenim podacima mora se ograničiti na ovlašteno, osposobljeno osoblje koje mora biti upoznato s informacijama da bi obavilo svoju dužnost ([294]). Općenitije, obavještajne agencije moraju na odgovarajući način osposobiti svoje zaposlenike, među ostalim za provedbu postupaka za izvješćivanje o povredama zakona i njihovo rješavanje (uključujući Izvršni nalog br. 14086) ([295]).

(156) Drugo, obavještajne agencije moraju se pridržavati standarda obavještajne zajednice za točnost i objektivnost, posebno u vezi s jamčenjem kvalitete i pouzdanosti podataka, razmatranjem alternativnih izvora informacija i objektivnosti u izvršavanju analiza ([296]).

(157) Treće, u Izvršnom nalogu br. 14086 pojašnjeno je da se na osobne podatke osoba koje nisu američki građani primjenjuju ista razdoblja čuvanja kao i na podatke američkih građana ([297]). Obavještajne agencije dužne su utvrditi posebna razdoblja čuvanja i/ili čimbenike koji se moraju uzeti u obzir kako bi se utvrdila duljina primjenjivih razdoblja čuvanja (npr. jesu li informacije dokazi o kaznenom djelu, jesu li informacije strane obavještajne informacije, jesu li informacije potrebne za zaštitu sigurnosti osoba ili organizacija, uključujući žrtve ili mete međunarodnog terorizma), koji su utvrđeni u raznim pravnim instrumentima ([298]).

(158) Četvrto, na širenje osobnih podataka prikupljenih elektroničkim izviđanjem primjenjuju se posebna pravila. Osobni podaci o osobama koje nisu američki državljani u pravilu se mogu širiti samo ako se iste vrste informacija mogu širiti o američkim državljanima, na primjer informacije potrebne za zaštitu sigurnosti osoba ili organizacija (kao što su mete, žrtve ili taoci međunarodnih terorističkih organizacija) ([299]). Nadalje, osobni podaci ne smiju se širiti samo na temelju državljanstva ili države boravišta osobe ili u svrhu izbjegavanja zahtjeva iz Izvršnog naloga br. 14086 ([300]). Podaci se mogu širiti unutar američke vlade samo ako ovlašten i osposobljen pojedinac iz opravdanih razloga

([293]) Članak 2. točka (c)(iii)(B)(1) Izvršnog naloga br. 14086. Vidjeti i glavu VIII. Zakona o nacionalnoj sigurnosti (u kojoj su detaljno navedeni zahtjevi za pristup klasificiranim podacima), članak 1.5. Izvršnog naloga br. 12333 (prema kojem se ravnatelji agencija iz obavještajne zajednice moraju pridržavati smjernica za dijeljenje i zaštitu informacija, privatnosti informacija i drugih pravnih zahtjeva), Direktivu o nacionalnoj sigurnosti br. 42 „Nacionalna politika za zaštitu telekomunikacija i informacijskih sustava u području nacionalne sigurnosti" (prema kojoj Odbor za sustave nacionalne sigurnosti mora izraditi smjernice o zaštiti sustava nacionalne sigurnosti za ministarstva i agencije) i Memorandum o nacionalnoj sigurnosti br. 8 „Poboljšanje kibernetičke sigurnosti sustava nacionalne sigurnosti, Ministarstva obrane i obavještajne zajednice" (u kojem su utvrđeni rokovi i smjernice za provedbu zahtjeva u pogledu kibernetičke sigurnosti sustava nacionalne sigurnosti, koji uključuju višerazinsku autentifikaciju, šifriranje, tehnologije u oblaku i usluge prepoznavanja krajnjih točaka).

([294]) Članak 2. točka (c)(iii)(B)(2) Izvršnog naloga br. 14086. Osim toga, osobnim podacima za koje nije konačno utvrđeno trebaju li se čuvati može se pristupiti samo kako bi se to utvrdilo ili potkrijepilo to utvrđenje ili kako bi se mogle izvršiti ovlaštene administrativne, ispitivačke, razvojne, sigurnosne ili nadzorne funkcije (članak 2. točka (c)(iii)(B)(3) Izvršnog naloga br. 14086).

([295]) Članak 2. točka (d)(ii) Izvršnog naloga br. 14086.

([296]) Članak 2. točka (c)(iii)(C) Izvršnog naloga br. 14086.

([297]) Članak 2. točke (c)(iii)(A)(2)(a)–(c) Izvršnog naloga br. 14086. Općenitije, svaka agencija mora uvesti politike i postupke za smanjenje širenja i čuvanja osobnih podataka prikupljenih elektroničkim izviđanjem (članak 2. točka (c)(iii)(A) Izvršnog naloga br. 14086).

([298]) Vidjeti npr. članak 309. Zakona o odobrenju prikupljanja obavještajnih podataka za fiskalnu godinu 2015., postupke smanjenja količine podataka koje su donijele pojedinačne obavještajne agencije u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti i koje je odobrio FISC, postupke koje je odobrio glavni državni odvjetnik u skladu sa Zakonom o saveznim evidencijama (kojima se od američkih saveznih agencija, uključujući nacionalne sigurnosne agencije, zahtijeva da utvrde razdoblja čuvanja svojih evidencija koja mora odobriti Uprava za nacionalne arhive i evidencije).

([299]) Članak 2. točka (c)(iii)(A)(1)(a) i članak 5. točka (d) Izvršnog naloga br. 14086 u vezi s člankom 2.3. Izvršnog naloga br. 12333.

([300]) Članak 2. točke (c)(iii)(A)(1)(b) i (e) Izvršnog naloga br. 14086.

vjeruje da primatelj podataka mora biti upoznat s informacijama ([301]) i da će ih na odgovarajući način zaštititi ([302]). Kako bi se utvrdilo mogu li se osobni podaci širiti primateljima izvan američke vlade (među ostalim stranim vladama ili međunarodnim organizacijama), moraju se uzeti u obzir svrha širenja, priroda i opseg podataka koji se šire i mogući štetni učinak na dotične osobe ([303]).

(159) Naposljetku, kako bi se među ostalim olakšali nadzor usklađenosti s primjenjivim pravnim zahtjevima i djelotvorna pravna zaštita, svaka obavještajna agencija mora u skladu s Izvršnim nalogom br. 14086 voditi odgovarajuću dokumentaciju o prikupljanju podataka elektroničkim izviđanjem. Dokumentacijski zahtjevi obuhvaćaju elemente kao što su činjenična osnova na temelju koje se procjenjuje je li određena aktivnost prikupljanja potrebna za ostvarenje potvrđenog obavještajnog prioriteta ([304]).

(160) Osim prethodno navedenih zaštitnih mjera iz Izvršnog naloga br. 14086 za uporabu informacija prikupljenih elektroničkim izviđanjem, sve obavještajne agencije SAD-a podliježu općenitijim zahtjevima u pogledu ograničenja svrhe, smanjenja količine podataka, točnosti, sigurnosti, čuvanja i širenja, posebno na temelju Okružnice Ureda za upravljanje i proračun br. A-130, Zakona o e-upravi, Zakona o saveznim evidencijama (vidjeti uvodne izjave 101.–106.) i smjernica Odbora za sustave nacionalne sigurnosti (CNSS) ([305]).

3.2.2. ***Nadzor***

(161) Aktivnosti američkih obavještajnih agencija nadzire nekoliko tijela.

(162) Prvo, Izvršnim nalogom br. 14086 propisano je da svaka obavještajna agencija mora imati više službenike za pravna pitanja, nadzor i usklađenost kako bi se osigurala usklađenost s primjenjivim američkim pravom ([306]). Oni moraju redovito nadzirati aktivnosti elektroničkog izviđanja i pobrinuti se za to da se sve neusklađenosti isprave. Obavještajne agencije moraju tim službenicima dati pristup svim informacijama koje su im bitne za izvršavanje njihovih nadzornih funkcija i ne smiju poduzimati ništa što bi ih spriječilo u provedbi nadzornih aktivnosti ili neprimjereno utjecalo na nju ([307]). Nadalje, o svakom većem slučaju neusklađenosti ([308]) koji je utvrdio službenik za nadzor ili neki drugi zaposlenik mora se odmah obavijestiti ravnatelja obavještajne agencije i direktora za nacionalna obavještajna pitanja, koji vodi računa o tome da se poduzme sve što je potrebno da se ispravi ta neusklađenost i spriječi njezino ponavljanje ([309]).

(163) Tu nadzornu funkciju obavljaju službenici nadležni za usklađenost, ali i službenici za privatnost i građanske slobode te glavni inspektori ([310]).

([301]) Vidjeti npr. Smjernice glavnog državnog odvjetnika za domaće operacije FBI-ja, kojima se predviđa da FBI može širiti informacije samo ako primatelj podataka mora biti upoznat s njima da bi ispunio svoju misiju ili zaštitio javnost.

([302]) Članak 2. točka (c)(iii)(A)(1)(c) Izvršnog naloga br. 14086. Obavještajne agencije mogu, na primjer, širiti informacije u okolnostima koje su relevantne za kaznenu istragu ili koje se odnose na kazneno djelo, među ostalim širenjem upozorenja o prijetnjama ubojstvom, teškim tjelesnim ozljedama ili otmicom, širenjem informacija o kibernetičkim prijetnjama, incidentima ili odgovoru na neovlašteni ulazak i obavješćivanjem žrtava ili upozoravanjem potencijalnih žrtava kaznenih djela.

([303]) Članak 2. točka (c)(iii)(A)(1)(d) Izvršnog naloga br. 14086.

([304]) Članak 2. točka (c)(iii)(E) Izvršnog naloga br. 14086.

([305]) Vidjeti Politiku CNSS-a br. 22, Cybersecurity Risk Management Policy (Politika upravljanja kibernetičkim rizicima), i Uputu CNSS-a br. 1253, u kojoj se navode detaljne smjernice o sigurnosnim mjerama koje treba uvesti za sustave nacionalne sigurnosti.

([306]) Članak 2. točke (d)(i)(A)–(B) Izvršnog naloga br. 14086.

([307]) Članak 2. točke (d)(i)(B)–(C) Izvršnog naloga br. 14086.

([308]) Tj. sustavna ili namjerna neusklađenost s primjenjivim američkim pravom koja bi mogla narušiti ugled ili integritet subjekta obavještajne zajednice ili na neki drugi način dovesti u pitanje pravilnost aktivnosti obavještajne zajednice, među ostalim s obzirom na eventualan znatan utjecaj na privatnost i građanske slobode dotične osobe ili osoba, vidjeti članak 5. točku (l) Izvršnog naloga br. 14086.

([309]) Članak 2. točka (d)(iii) Izvršnog naloga br. 14086.

([310]) Članak 2. točka (d)(i)(B) Izvršnog naloga br. 14086.

(164) Baš kao i u svim tijelima kaznenog progona, službenici za privatnost i građanske slobode postoje u svim obavještajnim agencijama ([311]). Ovlasti tih službenika obično obuhvaćaju nadzor postupaka kojima se osigurava da predmetno ministarstvo/agencija na primjereni način štite privatnost i građanske slobode te da su uspostavili primjerene postupke za rješavanje pritužbi pojedinaca koji smatraju da su im povrijeđene privatnost ili građanske slobode (a u nekim slučajevima, kao Ured direktora za nacionalna obavještajna pitanja (ODNI), mogu i sami imati ovlasti istraživati pritužbe ([312])). Ravnatelji obavještajnih agencija moraju službenicima za privatnost i građanske slobode osigurati resurse za izvršavanje mandata, kao i pristup svim materijalima i osoblju nužnima za izvršavanje njihovih funkcija, te ih informirati i savjetovati se s njima o predloženim izmjenama politika ([313]). Službenici za privatnost i građanske slobode periodično izvješćuju Kongres i PCLOB, među ostalim o broju i prirodi pritužbi koje je zaprimilo ministarstvo/agencija, uz navođenje sažetka odgovora na te pritužbe, o provedenim preispitivanjima i istragama te o učinku aktivnosti koje je službenik proveo ([314]).

(165) Drugo, svaka obavještajna agencija ima neovisnog glavnog inspektora koji je među ostalim odgovoran za nadzor stranih obavještajnih aktivnosti. U ODNI-ju to je Ured glavnog inspektora obavještajne zajednice koji ima potpunu nadležnost nad cijelom obavještajnom zajednicom i ovlašten je za istrage pritužbi ili informacija o navodnom nezakonitom postupanju ili zlouporabi ovlasti u vezi s ODNI-jem i/ili programima i aktivnostima obavještajne zajednice ([315]). Baš kao i tijela kaznenog progona (vidjeti uvodnu izjavu 109.), glavni inspektori zakonski su neovisni ([316]) i odgovorni za provedbu revizija i istraga povezanih s programima i operacijama koje u nacionalne obavještajne svrhe provodi predmetna agencija, među ostalim zbog zlouporabe ili povrede prava ([317]). Imaju pristup svim evidencijama, izvješćima, revizijama, preispitivanjima, dokumentima, spisima, preporukama ili drugim

([311]) Vidjeti glavu 42. članak 2000ee-1. Zakonika SAD-a. To npr. uključuje Ministarstvo vanjskih poslova, Ministarstvo pravosuđa, Ministarstvo domovinske sigurnosti, Ministarstvo obrane, NSA, Središnju obavještajnu agenciju (CIA), FBI i ODNI.

([312]) Vidjeti članak 3. točku (c) Izvršnog naloga br. 14086.

([313]) Glava 42. članak 2000ee-1. točka (d) Zakonika SAD-a.

([314]) Vidjeti glavu 42. članak 2000ee-1. točke (f)(1)–(2) Zakonika SAD-a. Na primjer, prema izvješću NSA-ova Ureda za građanske slobode, privatnost i transparentnost za razdoblje od siječnja 2021. do lipnja 2021. taj je ured proveo 591 preispitivanje utjecaja na građanske slobode i privatnost u raznim kontekstima, npr. u slučaju aktivnosti prikupljanja, dogovora i odluka o dijeljenju informacija te odluka o čuvanju podataka, pri čemu je uzeo u obzir niz čimbenika kao što su količina i vrsta informacija povezanih s aktivnosti, uključeni pojedinci, svrha i predviđena uporaba podataka ili zaštitne mjere uspostavljene za ublažavanje mogućih rizika za privatnost (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Slično tomu, izvješća CIA-ina Ureda za privatnost i građanske slobode za razdoblje od siječnja do lipnja 2019. sadržavaju informacije o nadzornim aktivnostima tog ureda, npr. o preispitivanju usklađenosti sa Smjernicama glavnog državnog odvjetnika u skladu s Izvršnim nalogom br. 12333 u pogledu čuvanja i širenja informacija, smjernica o provedbi Predsjedničkog ukaza o politici br. 28 i zahtjeva za utvrđivanje i otklanjanje povreda podataka te preispitivanju uporabe osobnih informacija i postupanja s njima (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Glavnog inspektora imenuje predsjednik, potvrđuje Senat i može ga razriješiti samo predsjednik.

([316]) Glavni inspektori imaju osiguran 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 nacionalnih (sigurnosnih) interesa. No Kongres se mora obavijestiti o izvršavanju te ovlasti i na temelju toga može dotičnog direktora pozvati na odgovornost. Vidjeti npr. članak 8. (za Ministarstvo obrane), članak 8.E (za Ministarstvo pravosuđa), članak 8.G točke (d)(2)(A) i (B) (za NSA) Zakona o glavnom inspektoru iz 1978., glavu 50. članak 403.q točku (b) Zakonika SAD-a (za CIA-ju), članak 405. točku (f) (za obavještajnu zajednicu) Zakona o odobrenju prikupljanja obavještajnih podataka za fiskalnu godinu 2010.

([317]) Zakon o glavnom inspektoru iz 1978., kako je izmijenjen, Javni zakon br. 117–108 od 8. travnja 2022. Na primjer, kako je objašnjeno u njegovim polugodišnjim izvješćima Kongresu za razdoblje od 1. travnja 2021. do 31. ožujka 2022., glavni inspektor NSA-a ocijenio je postupanje s informacijama američkih državljana prikupljenima u skladu s Izvršnim nalogom br. 12333, postupak potpunog čišćenja podataka prikupljenih elektroničkim izviđanjem, automatizirani alat za ciljano praćenje kojim se koristi NSA i usklađenost prikupljanja podataka na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti s pravilima o dokumentaciji i pretraživanju te je izdao nekoliko preporuka u tom kontekstu (vidjetihttps://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, str. 5.–8., i https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, str. 10.–13). Vidjeti i novije revizije i istrage glavnog inspektora obavještajne zajednice o informacijskoj sigurnosti i neovlaštenim otkrivanjima klasificiranih informacija u području nacionalne sigurnosti (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, str. 8., 11., i https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, str. 19.–20).

relevantnim materijalima, prema potrebi na temelju sudskog naloga, i mogu uzimati iskaze ([318]). Glavni inspektori upućuju slučajeve navodnih povreda kaznenih propisa u postupak kaznenog progona i ravnateljima agencijama preporučuju korektivne mjere ([319]). Iako su njihove preporuke neobvezujuće, njihova izvješća, uključujući ona o daljnjim mjerama (ili nepostojanju takvih mjera) ([320]) u pravilu se objavljuju i šalju Kongresu, koji na osnovi toga može vršiti svoju nadzornu funkciju (vidjeti uvodne izjave 168. i 169.) ([321]).

(166) Treće, Odbor za nadzor obavještajnih aktivnosti (IOB), koji je uspostavljen u okviru Predsjedničkog savjetodavnog odbora za obavještajne aktivnosti (PIAB), nadzire usklađenost američkih obavještajnih tijela s Ustavom i svim primjenjivim pravilima ([322]). PIAB je savjetodavno tijelo u okviru Izvršnog ureda predsjednika i ima 16 članova koje predsjednik imenuje iz redova osoba koje nisu dio američke vlade. IOB ima najviše pet članova koje predsjednik imenuje iz redova članova PIAB-a. U skladu s Izvršnim nalogom br. 12333 ([323]) ravnatelji svih obavještajnih agencija dužni su obavijestiti IOB o obavještajnim aktivnostima za koje je opravdano vjerovati da bi mogle biti nezakonite ili protivne izvršnom nalogu ili predsjedničkom ukazu. Kako bi IOB imao pristup informacijama nužnima za izvršenje svojih funkcija, u Izvršnom nalogu br. 13462 direktora za nacionalna obavještajna pitanja i ravnatelje agencija obvezuje se da, koliko je to dopušteno zakonom, IOB-u pruže sve informacije i pomoć koje su mu potrebne za izvršenje njegovih funkcija ([324]). IOB je pak dužan obavijestiti predsjednika o obavještajnim aktivnostima kojima se, prema njegovu mišljenju, krše američki zakoni (uključujući izvršne naloge) i u vezi s kojima glavni državni odvjetnik, direktor za nacionalna obavještajna pitanja ili ravnatelj obavještajne agencije ne poduzimaju primjerene mjere ([325]). IOB je usto dužan obavijestiti glavnog državnog odvjetnika o eventualnoj povredi kaznenog prava.

(167) Četvrto, obavještajne agencije podliježu nadzoru PCLOB-a. U skladu sa zakonom na temelju kojeg je osnovan PCLOB je odgovoran za politike za borbu protiv terorizma i njihovu provedbu u cilju zaštite privatnosti i građanskih sloboda. Za potrebe preispitivanja aktivnosti obavještajnih agencija taj odbor može pristupiti svim relevantnim evidencijama, izvješćima, revizijama, preispitivanjima, dokumentima, spisima i preporukama agencije, uključujući klasificirane podatke, te obavljati razgovore i uzimati iskaze ([326]). Prima izvješća službenika za građanske slobode i privatnost nekoliko saveznih ministarstava/agencija ([327]), može davati preporuke državnim i obavještajnim agencijama te redovito izvješćuje kongresne odbore i predsjednika ([328]). Izvješća tog odbora, uključujući ona Kongresu, moraju biti što dostupnija javnosti ([329]). PCLOB je izdao nekoliko izvješća o nadzoru i daljnjim mjerama, uključujući analizu programa koji se provode na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti te analizu zaštite privatnosti u tom kontekstu, provedbe Predsjedničkog ukaza o politici br. 28 i Izvršnog naloga br. 12333 ([330]). PCLOB-u su povjerene i određene nadzorne funkcije povezane s provedbom Izvršnog naloga

([318]) Vidjeti članak 6. Zakona o glavnom inspektoru iz 1978.

([319]) Vidjeti prethodnu bilješku, članak 4., 6–5.

([320]) Kad je riječ o daljnjim mjerama na temelju izvješća i preporuka glavnih inspektora, vidjeti npr. odgovor na izvješće glavnog inspektora Ministarstva pravosuđa u kojem je utvrđeno da FBI od 2014. do 2019. nije podnosio dovoljno transparentne zahtjeve FISC-u, što je potaknulo reforme za poboljšanje usklađenosti, nadzora i snošenja odgovornosti u FBI-ju (npr. ravnatelj je naložio da se provede više od 40 korektivnih mjera, uključujući 12 mjera povezanih s dokumentacijom, nadzorom, održavanjem dokumentacije, osposobljavanjem i revizijama u kontekstu postupka na temelju Zakona o nadzoru stranih obavještajnih aktivnosti) (vidjeti https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance i https://oig.justice.gov/reports/2019/o20012.pdf). Vidjeti npr. i reviziju uloga i odgovornosti Ureda glavnog savjetnika FBI-ja u okviru nadzora usklađenosti s primjenjivim zakonima, politikama i postupcima povezanima s aktivnostima FBI-ja u području nacionalne sigurnosti, koju je proveo glavni inspektor Ministarstva pravosuđa, i Dodatak 2., koji sadržava dopis u kojem FBI prihvaća sve preporuke. U tom se pogledu u Dodatku 3. daje pregled daljnjih mjera i informacija koje je glavni inspektor tražio od FBI-ja kako bi mogao potvrditi da je preporuka provedena (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Vidjeti članak 4. točku 5. i članak 5. Zakona o glavnom inspektoru iz 1978.

([322]) Vidjeti Izvršni nalog br. 13462.

([323]) Članak 1.6. točka (c) Izvršnog naloga br. 12333.

([324]) Članak 8. točka (a) Izvršnog naloga br. 13462.

([325]) Članak 6. točka (b) Izvršnog naloga br. 13462.

([326]) Glava 42. članak 2000ee. točka (g) Zakonika SAD-a.

([327]) Vidjeti glavu 42. članak 2000ee-1. točku (f)(1)(A)(iii) Zakonika SAD-a. Oni uključuju, u najmanju ruku, Ministarstvo pravosuđa, Ministarstvo obrane, Ministarstvo domovinske sigurnosti, direktora za nacionalna obavještajna pitanja i Središnju obavještajnu agenciju te sva druga ministarstva, agencije ili subjekte izvršne vlasti koje PCLOB smatra relevantnima.

([328]) Glava 42. članak 2000ee. točka (e) Zakonika SAD-a.

([329]) Glava 42. članak 2000ee. točka (f) Zakonika SAD-a.

([330]) Dostupno na https://www.pclob.gov/Oversight

br. 14086, koje u prvom redu uključuju preispitivanje jesu li agencijski postupci u skladu s izvršnim nalogom (vidjeti uvodnu izjavu 126.) i ocjenjivanje ispravnosti funkcioniranja mehanizma pravne zaštite (vidjeti uvodnu izjavu 194).

(168) Peto, osim nadzornih mehanizama u okviru izvršne vlasti nadzorne odgovornosti za sve američke strane obavještajne aktivnosti imaju i pojedini odbori u američkom kongresu (odbori za obavještajna pitanja i odbori za pravosuđe Zastupničkog doma i Senata). Članovi tih odbora imaju pristup klasificiranim podacima te obavještajnim metodama i programima ([331]). Odbori izvršavaju svoje nadzorne funkcije na razne načine, osobito saslušanjima, istragama, preispitivanjima i izradom izvješća ([332]).

(169) Kongresni odbori zaprimaju redovita izvješća o obavještajnim aktivnostima, među ostalim od glavnog državnog odvjetnika, direktora za nacionalna obavještajna pitanja, obavještajnih agencija i drugih nadzornih tijela (npr. glavni inspektori), vidjeti uvodne izjave 164. i 165. Prije svega, u skladu sa Zakonom o nacionalnoj sigurnosti „predsjednik osigurava potpuno i ažurno obavješćivanje kongresnih odbora za obavještajna pitanja o obavještajnim aktivnostima SAD-a, među ostalim o svim bitnim očekivanim obavještajnim aktivnostima u skladu s ovim potpoglavljem” ([333]). Nadalje, „predsjednik osigurava žurno obavješćivanje kongresnih odbora za obavještajna pitanja o svim nezakonitim obavještajnim aktivnostima te o korektivnim mjerama koje su poduzete ili se planiraju poduzeti u vezi s takvim nezakonitim aktivnostima” ([334]).

(170) Osim toga, određenim zakonima propisani su dodatni zahtjevi u pogledu izvješćivanja. U skladu s pojedinim člancima Zakona o nadzoru stranih obavještajnih aktivnosti glavni državni odvjetnik mora o vladinim aktivnostima „u potpunosti obavješćivati” odbore za obavještajna pitanja i odbore za pravosuđe Senata i Zastupničkog doma ([335]). Tim je zakonom propisano i da je vlada dužna kongresnim odborima dostaviti preslike svih odluka, naloga ili mišljenja FISC-a ili FISCR-a koji uključuju „znatno oblikovanje ili tumačenje” odredbi tog zakona. Parlamentarni nadzor na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti provodi se podnošenjem zakonski obaveznih izvješća odborima za obavještajna pitanja i odborima za pravosuđe te u okviru čestih informativnih sastanaka i saslušanja. To obuhvaća polugodišnja izvješća glavnog državnog odvjetnika o primjeni članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti popraćena dokumentima, uključujući izvješća Ministarstva pravosuđa i ODNI-ja o usklađenosti i opis svih slučajeva neusklađenosti ([336]), i zasebnu polugodišnju procjenu glavnog državnog odvjetnika i direktora za nacionalna obavještajna pitanja o usklađenosti s postupcima za ciljano praćenje i smanjenje količine podataka ([337]).

([331]) Glava 50. članak 3091. Zakonika SAD-a.

([332]) Na primjer, odbori organiziraju tematska saslušanja (vidjeti npr. nedavno saslušanje Odbora za pravosuđe Zastupničkog doma o „digitalnim mrežama za hvatanje kriminalaca”, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983) i saslušanje Odbora za obavještajna pitanja Zastupničkog doma o umjetnoj inteligenciji u obavještajnoj zajednici (https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), saslušanja o redovitom nadzoru, npr. saslušanja FBI-ja i odjela Ministarstva pravosuđa za nacionalnu sigurnost, vidjeti https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 i https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Kao primjer istrage vidjeti istragu ruskog utjecaja na američke izbore 2016. koju je proveo Odbor za obavještajna pitanja Senata, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. Kad je riječ o izvješćivanju, vidjeti npr. pregled (nadzornih) aktivnosti Odbora za obavještajna pitanja Senata u njegovu izvješću Senatu za razdoblje od 4. siječnja 2019. do 3. siječnja 2021., https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4

([333]) Vidjeti glavu 50. članak 3091. točku (a)(1) Zakonika SAD-a. Ta odredba sadržava opće zahtjeve u pogledu nadzora koji Kongres provodi u području nacionalne sigurnosti.

([334]) Vidjeti glavu 50. članak 3091. točku (b) Zakonika SAD-a.

([335]) Vidjeti glavu 50. članke 1808., 1846., 1862., 1871. i 1881f. Zakonika SAD-a.

([336]) Vidjeti glavu 50. članak 1881f. Zakonika SAD-a.

([337]) Vidjeti glavu 50. članak 1881.a točku (l)(1) Zakonika SAD-a.

(171) Osim toga, u skladu sa Zakonom o nadzoru stranih obavještajnih aktivnosti američka vlada mora svake godine izvijestiti Kongres (i javnost) o, među ostalim, broju naloga traženih i primljenih na temelju tog zakona te o procijenjenom broju američkih državljana i osoba koje nisu američki državljani koje su predmet nadzora ([338]). Tim zakonom propisano je i dodatno izvješćivanje javnosti o broju izdanih dopisa o nacionalnoj sigurnosti za američke državljane i osobe koje nisu američki državljani (no primateljima naloga i potvrda na temelju tog zakona te zahtjeva za dopis o nacionalnoj sigurnosti pod određenim uvjetima dopušteno je izdavanje izvješća o transparentnosti) ([339]).

(172) Općenitije, američka obavještajna zajednica na razne se načine trudi osigurati transparentnost svojih (stranih) obavještajnih aktivnosti. Na primjer, ODNI je 2015. donio Načela transparentnosti obavještajnih aktivnosti i Provedbeni plan za transparentnost te je uputio sve obavještajne agencije da imenuju službenika za transparentnost obavještajnih aktivnosti koji će poticati transparentnost i provoditi inicijative za povećanje transparentnosti ([340]). Obavještajna zajednica usto je deklasificirala dijelove politika, postupaka, izvješća o nadzoru, izvješća o aktivnostima na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti i Izvršnog naloga br. 12333, odluka FISC-a i drugih dokumenata te ih nastavlja objavljivati, među ostalim na internetskoj stranici „IC on the Record” koju ODNI vodi upravo u tu svrhu ([341]).

(173) Naposljetku, prikupljanje osobnih podataka na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti ne nadziru samo nadzorna tijela iz uvodnih izjava od 162. do 168. nego i FISC ([342]). U skladu s pravilom 13. Poslovnika FISC-a službenici za usklađenost u američkim obavještajnim agencijama dužni su o svakoj povredi postupaka za ciljano praćenje na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti, smanjenje količine podataka i pretraživanje obavijestiti Ministarstvo pravosuđa i ODNI, koji o njima potom obavješćuju FISC. Osim toga, Ministarstvo pravosuđa i ODNI podnose FISC-u zajednička polugodišnja izvješća o procjeni nadzora, u kojima se navode kretanja u području usklađenosti s postupcima za ciljano praćenje, iznose statistički podaci, opisuju kategorije slučajeva neusklađenosti, detaljno opisuju razlozi zbog kojih je došlo do određenih slučajeva neusklađenosti s postupcima za ciljano praćenje te se daje pregled mjera koje su obavještajne agencije poduzele da bi spriječile njihovo ponavljanje ([343]).

(174) Prema potrebi (npr. ako se utvrde povrede postupaka za ciljano praćenje) Sud može predmetnoj obavještajnoj agenciji naložiti poduzimanje korektivnih mjera ([344]). Te mjere mogu biti pojedinačne ili strukturne, na primjer prestanak prikupljanja podataka i brisanje nezakonito dobivenih podataka ili promjena prakse prikupljanja podataka, među ostalim kad je riječ o smjernicama i osposobljavanju za osoblje ([345]). Nadalje, u godišnjem preispitivanju potvrda na temelju članka 702. FISC razmatra slučajeve neusklađenosti kako bi utvrdio jesu li

([338]) Glava 50. članak 1873. točka (b) Zakonika SAD-a. Nadalje, u skladu s člankom 402. „direktor za nacionalna obavještajna pitanja u dogovoru s glavnim državnim odvjetnikom provodi deklasifikacijsko preispitivanje svake odluke, naloga ili mišljenja Suda za nadzor stranih obavještajnih aktivnosti ili Žalbenog suda za nadzor stranih obavještajnih aktivnosti (kako su definirani u članku 601. točki (e)) koji uključuju znatno oblikovanje ili tumačenje bilo koje zakonske odredbe, među ostalim novo ili znatno oblikovanje ili tumačenje pojma ‚posebni čimbenik za odabir’ te u skladu s tim preispitivanjem u mjeri u kojoj je to izvedivo objavljuje svaku takvu odluku, nalog ili mišljenje”.

([339]) Glava 50. članak 1873. točka (b)(7) i članak 1874. Zakonika SAD-a.

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

([341]) Vidjeti „IC on the Record”, dostupno na https://icontherecord.tumblr.com/

([342]) FISC je prethodno zaključio da je „Sudu […] jasno da provedbene agencije, kao i [ODNI] i [Odjel Ministarstva pravosuđa za nacionalnu sigurnost], posvećuju znatne resurse izvršavanju svojih odgovornosti za usklađenost i nadzor iz članka 702. Slučajevi neusklađenosti u pravilu se brzo utvrđuju i poduzimaju se primjerene korektivne mjere radi potpunog čišćenja informacija koje su neispravno prikupljene ili na koje se inače primjenjuju zahtjevi za uništenje u skladu s primjenjivim postupcima”. FISC, Sažeta sudska odluka i nalog [slika zacrnjena] (2014.), dostupno na https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf

([343]) Vidjeti npr. Izvješće Ministarstva pravosuđa i ODNI-ja FISC-u o usklađenosti s člankom 702. za razdoblje od lipnja 2018. do studenoga 2018., str. 21.–65.

([344]) Glava 50. članak 1803. točka (h) Zakonika SAD-a. Vidjeti i PCLOB, Izvješće o članku 702., str. 76. Vidjeti i Sažetu sudsku odluku i nalog FISC-a od 3. listopada 2011. kao primjer naloga o nedostacima u kojem je vladi naloženo da otkloni utvrđene nedostatke u roku od 30 dana. Dostupno na https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Vidjeti i Waltonov dopis, 4. dio, str. 10.–11. Vidjeti i Mišljenje FISC-a od 18. listopada 2018., dostupno na https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, kako ga je potvrdio Žalbeni sud za nadzor stranih obavještajnih aktivnosti u svojem Mišljenju od 12. srpnja 2019., dostupno na: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, u kojem je FISC među ostalim naložio vladi da se uskladi s određenim zahtjevima za obavješćivanje, dokumentiranje i izvješćivanje povezanima s FISC-om.

([345]) Vidjeti npr. Sažetu sudsku odluku i nalog FISC-a (6. prosinca 2019.) (odobreno za objavu 4. rujna 2020.), str. 76., u kojem je FISC uputio vladu da do 28. veljače 2020. dostavi pisano izvješće o koracima koje poduzima radi poboljšanja postupaka za utvrđivanje i uklanjanje izvješća izrađenih prema informacijama prikupljenima na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti koja su povučena radi usklađivanja s propisima te o drugim pitanjima. Vidjeti i Prilog VII.

podnesene potvrde u skladu sa zahtjevima iz Zakona o nadzoru stranih obavještajnih aktivnosti. Slično tomu, ako FISC utvrdi da vladine potvrde nisu dostatne, među ostalim zbog određenih slučajeva neusklađenosti, može izdati „nalog o nedostacima" kojim vladu obvezuje da povredu ispravi u roku od 30 dana ili da prestane odnosno ne počinje upotrebljavati potvrde na temelju članka 702. Naposljetku, FISC ocjenjuje uočena kretanja u problemima zbog neusklađenosti i može zahtijevati mijenjanje postupaka ili dodatni nadzor i izvješćivanje kako bi se ublažila ta kretanja ([346]).

3.2.3. ***Pravna zaštita***

(175) Kako je detaljnije objašnjeno u ovom odjeljku, u SAD-u postoje razni oblici zaštite koji ispitanicima iz Unije omogućuju pokretanje postupka pred neovisnim i nepristranim sudom s obvezujućim ovlastima. Zahvaljujući tomu, pojedinci mogu pristupiti svojim osobnim podacima, zakonitost vladina pristupa njihovim podacima može se preispitati, a utvrđena povreda može se ispraviti, među ostalim ispravkom ili brisanjem njihovih osobnih podataka.

(176) Prvo, poseban mehanizam pravne zaštite uspostavljen je Izvršnim nalogom br. 14086 i dopunjen Uredbom glavnog državnog odvjetnika o osnivanju Žalbenog suda za zaštitu podataka te služi za obradu i rješavanje pritužbi pojedinaca zbog američkih aktivnosti elektroničkog izviđanja. U okviru tog mehanizma svi pojedinci u EU-u imaju pravo podnijeti pritužbu zbog navodne povrede američkog prava kojim su uređene aktivnosti elektroničkog izviđanja (npr. Izvršni nalog br. 14086, članak 702. Zakona o nadzoru stranih obavještajnih aktivnosti, Izvršni nalog br. 12333) koja štetno djeluje na njihovu privatnost i građanske slobode ([347]). Taj mehanizam pravne zaštite dostupan je pojedincima iz zemalja ili organizacija za regionalnu gospodarsku integraciju za koje je američki glavni državni odvjetnik odredio da su „države koje ispunjavaju uvjete" ([348]). Glavni državni odvjetnik 30. lipnja 2023. u skladu s člankom 3. točkom (f) Izvršnog naloga br. 14086 odredio je za Europsku uniju i tri zemlje Europskog udruženja slobodne trgovine, koje zajedno čine Europski gospodarski prostor, da su „države koje ispunjavaju uvjete" ([349]). Time se ne dovodi u pitanje članak 4. stavak 2. Ugovora o Europskoj uniji.

(177) Ispitanik iz Unije koji želi podnijeti takvu pritužbu mora je podnijeti nadzornom tijelu u državi članici EU-a nadležnom za nadzor obrade osobnih podataka koju provode javna tijela (tijelo za zaštitu podataka) ([350]). Tako pojedinci mogu lako pristupiti mehanizmu pravne zaštite koji im omogućuje da se obrate tijelu „na kućnom pragu", s kojim mogu komunicirati na vlastitom jeziku. Nakon provjere zahtjeva za ispunjavanje pritužbe iz uvodne izjave 178. nadležno tijelo za zaštitu podataka proslijedit će pritužbu u mehanizam pravne zaštite preko tajništva Europskog odbora za zaštitu podataka.

(178) Zahtjevi za podnošenje pritužbe u mehanizam pravne zaštite jednostavni su s obzirom na to da pojedinci ne moraju dokazati da su njihovi podaci bili predmet američkih aktivnosti elektroničkog izviđanja ([351]). Ipak, kao početnu točku za preispitivanje u okviru mehanizma pravne zaštite, potrebno je dostaviti određene osnovne informacije, na primjer o tome za koje se osobne podatke opravdano vjeruje da su preneseni u SAD i vjerojatno sredstvo njihova prijenosa, o nazivima tijela američke vlade za koja se vjeruje da su sudjelovala u navodnoj povredi (ako je poznato), o osnovi na temelju koje se tvrdi da je došlo do navodne povrede američkog prava (iako se ni za to ne treba dokazati da je neka američka obavještajna agencija doista i prikupila osobne podatke) i o prirodi tražene pravne zaštite.

([346]) Vidjeti Prilog VII.

([347]) Vidjeti članak 4. točku (k)(iv) Izvršnog naloga br. 14086, kojim je propisano da pritužbu u mehanizam pravne zaštite mora podnijeti podnositelj pritužbe u vlastito ime (tj. ne kao predstavnik vlade, nevladine ili međuvladine organizacije). Pojam „štetno djeluje" ne zahtijeva od podnositelja pritužbe da ispuni određeni prag kako bi imao pristup mehanizmu pravne zaštite (vidjeti uvodnu izjavu 178. u tom pogledu). Umjesto toga, u njemu se pojašnjava da službenik za zaštitu građanskih sloboda ODNI-ja i DPRC imaju ovlasti za ispravljanje povreda prava SAD-a kojim se uređuju aktivnosti elektroničkog izviđanja koje štetno djeluju na osobne interese podnositelja pritužbe u pogledu privatnosti i građanskih sloboda. S druge strane, povrede zahtjeva iz primjenjivog prava SAD-a koji nisu namijenjeni zaštiti pojedinaca (npr. proračunski zahtjevi) ne bi bile u nadležnosti službenika za zaštitu građanskih sloboda ODNI-ja i DPRC-a.

([348]) Članak 3. točka (f) Izvršnog naloga br. 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Članak 4. točka (d)(v) Izvršnog naloga br. 14086.

([351]) Vidjeti članak 4. točku (k)(i)–(iv) Izvršnog naloga br. 14086.

(179) Pritužbe u tom mehanizmu pravne zaštite prvo istražuje službenik za zaštitu građanskih sloboda ODNI-ja, kojem su Izvršnim nalogom br. 14086 zakonska uloga i ovlasti proširene upravo na te konkretne aktivnosti ([352]). U obavještajnoj zajednici službenik za zaštitu građanskih sloboda odgovoran je, među ostalim, za ispravno uvrštavanje pitanja građanskih sloboda i privatnosti u politike i postupke ODNI-ja i obavještajnih agencija, nadzor usklađenosti ODNI-ja s primjenjivim zahtjevima zaštite građanskih sloboda i privatnosti te procjene učinka na privatnost ([353]). Službenika za zaštitu građanskih sloboda ODNI-ja može razriješiti samo direktor za nacionalna obavještajna pitanja iz opravdanih razloga, tj. u slučaju povrede dužnosti, zlouporabe položaja, povrede sigurnosti, zanemarivanja dužnosti ili nesposobnosti za rad ([354]).

(180) Službenik za zaštitu građanskih sloboda ODNI-ja pri preispitivanju može pristupiti informacijama za potrebe svoje procjene i može se osloniti na zakonski obaveznu pomoć službenika za privatnost i građanske slobode iz raznih obavještajnih agencija ([355]). Obavještajnim agencijama zabranjeno je sprečavati preispitivanja službenika za zaštitu građanskih sloboda ODNI-ja i neprimjereno utjecati na njih. To uključuje direktora za nacionalna obavještajna pitanja, koji se ne smije uplitati u preispitivanje ([356]). Službenik za zaštitu građanskih sloboda ODNI-ja koji preispituje pritužbu mora „pravo primjenjivati nepristrano” uzimajući u obzir i interese nacionalne sigurnosti u pogledu aktivnosti elektroničkog izviđanja te zaštitu privatnosti ([357]).

(181) U okviru preispitivanja službenik za zaštitu građanskih sloboda ODNI-ja utvrđuje je li došlo do povrede primjenjivog američkog prava i, ako jest, odlučuje o primjerenim korektivnim mjerama ([358]). Riječ je o mjerama koje u potpunosti ispravljaju utvrđenu povredu, kao što su prestanak nezakonitog prikupljanja podataka, brisanje nezakonito prikupljenih podataka, brisanje rezultata neprimjerenih pretraživanja inače zakonito prikupljenih podataka, ograničavanje pristupa zakonito prikupljenim podacima na primjereno osposobljeno osoblje ili povlačenje obavještajnih izvješća s podacima koji su prikupljeni bez zakonitog odobrenja ili su se nezakonito širili ([359]). Odluke službenika za zaštitu građanskih sloboda ODNI-ja (među ostalim o korektivnim mjerama) obvezujuće su za predmetne obavještajne agencije ([360]).

(182) Službenik za zaštitu građanskih sloboda ODNI-ja mora dokumentirati preispitivanje i donijeti klasificiranu odluku u kojoj obrazlaže osnovu za svoja činjenična utvrđenja, kako je utvrdio je li došlo do predmetne povrede i kako je utvrdio koje su korektivne mjere primjerene ([361]). Ako službenik za zaštitu građanskih sloboda ODNI-ja preispitivanjem otkrije povredu koju je počinilo tijelo koje nadzire FISC, službenik mora izraditi i klasificirano izvješće za pomoćnika glavnog državnog odvjetnika za nacionalnu sigurnost, koji je potom obvezan o neusklađenosti obavijestiti FISC koji može poduzeti daljnje provedbene mjere (u skladu s postupkom opisanim u izjavama od 173. do 174.) ([362]).

(183) Nakon što završi preispitivanje, službenik za zaštitu građanskih sloboda ODNI-ja preko nacionalnog tijela obavješćuje podnositelja pritužbe da „preispitivanjem nisu utvrđene predmetne povrede ili je službenik za zaštitu građanskih sloboda ODNI-ja utvrdio koje primjerene korektivne mjere treba provesti” ([363]). Tako se štiti povjerljivost aktivnosti provedenih radi zaštite nacionalne sigurnosti, dok pojedinci dobivaju odluku koja potvrđuje da je njihova pritužba propisno istražena i riješena. Nadalje, pojedinac može osporavati tu odluku. U tu će se svrhu pojedinac obavijestiti da može podnijeti žalbu DPRC-u radi preispitivanja utvrđenja službenika za zaštitu građanskih sloboda (vidjeti uvodnu izjavu 184. i dalje) i da će se odabrati posebni odvjetnik koji će zastupati interese podnositelja pritužbe ako se predmet povjeri tom sudu ([364]).

([352]) Članak 3. točka (c)(iv) Izvršnog naloga br. 14086. Kad je riječ o ulozi službenika za zaštitu građanskih sloboda u okviru ODNI-ja, vidjeti i članak 103D. Zakona o nacionalnoj sigurnosti iz 1947., prenesen glavom 50. člankom 403-3d. Zakonika SAD-a.
([353]) Glava 50. članak 3029. točka (b) Zakonika SAD-a.
([354]) Članak 3. točka (c)(iv) Izvršnog naloga br. 14086.
([355]) Članak 3. točka (c)(iii) Izvršnog naloga br. 14086.
([356]) Članak 3. točka (c)(iv) Izvršnog naloga br. 14086.
([357]) Članak 3. točke (c)(i)(B)(i) i (iii) Izvršnog naloga br. 14086.
([358]) Članak 3. točka (c)(i) Izvršnog naloga br. 14086.
([359]) Članak 4. točka (a) Izvršnog naloga br. 14086.
([360]) Članak 3. točke (c) i (d) Izvršnog naloga br. 14086.
([361]) Članak 3. točke (c)(i)(F)–(G) Izvršnog naloga br. 14086.
([362]) Vidjeti i članak 3. točku (c)(i)(D) Izvršnog naloga br. 14086.
([363]) Članak 3. točka (c)(i)(E)(1) Izvršnog naloga br. 14086.
([364]) Članak 3. točke (c)(i)(E)(2)–(3) Izvršnog naloga br. 14086.

(184) Svi podnositelji pritužbi i svi subjekti obavještajne zajednice mogu zatražiti preispitivanje odluke službenika za zaštitu građanskih sloboda ODNI-ja pred Žalbenim sudom za zaštitu podataka. Zahtjevi za preispitivanje moraju se podnijeti u roku od 60 dana od zaprimanja obavijesti tog službenika o završetku preispitivanja i sadržavati informacije koje pojedinac želi dati DPRC-u (npr. tvrdnje o pravnim pitanjima ili primjeni prava na činjenice predmeta) ([365]). Subjekti iz Unije mogu i taj zahtjev podnijeti nacionalnim tijelima (vidjeti uvodnu izjavu 177.).

(185) DPRC je neovisni sud koji je osnovao glavni državni odvjetnik u skladu s Izvršnim nalogom br. 14086 ([366]). Sastoji se od najmanje šest sudaca koje na četverogodišnji mandat s mogućnošću produljenja imenuje glavni državni odvjetnik u dogovoru s PCLOB-om, ministrom trgovine i direktorom za nacionalna obavještajna pitanja ([367]). Pri imenovanju sudaca glavni državni odvjetnik uzima u obzir kriterije koje izvršna vlast primjenjuje u procjeni kandidata za savezne suce i daje prednost osobama s prethodnim sudačkim iskustvom ([368]). Suci moraju ujedno biti pravni stručnjaci (tj. aktivni članovi koji ispunjavaju sve obveze u komori i propisno su licencirani za obavljanje odvjetničke službe) i imati odgovarajuće iskustvo s propisima o privatnosti i nacionalnoj sigurnosti. Glavni državni odvjetnik nastoji osigurati da u svakom trenutku najmanje polovina odvjetnika ima prethodno sudačko iskustvo, a svi suci moraju proći sigurnosnu provjeru kako bi mogli pristupiti klasificiranim informacijama u području nacionalne sigurnosti ([369]).

(186) Samo pojedinci koji ispunjavaju uvjete iz uvodne izjave 185. i nisu zaposleni u izvršnoj vlasti u trenutku imenovanja ili u prethodne dvije godine mogu se imenovati u DPRC. Slično tomu, tijekom svojeg mandata u DPRC-u suci ne smiju preuzimati nikakve službene dužnosti ili se zaposliti u američkoj vladi (osim kao suci DPRC-a) ([370]).

(187) Neovisnost postupka odlučivanja postiže se nizom jamstava. Izvršnoj vlasti (glavni državni odvjetnik i obavještajne agencije) zabranjeno je uplitanje u preispitivanje DPRC-a ili neprimjereni utjecaj na njega ([371]). DPRC je dužan nepristrano odlučivati o predmetima ([372]) i poslovati u skladu s vlastitim poslovnikom (koji se donosi većinom glasova). Nadalje, suce DPRC-a može razriješiti samo glavni državni odvjetnik, i to samo iz opravdanih razloga (tj. povreda dužnosti, zlouporaba položaja, povreda sigurnosti, zanemarivanje dužnosti ili nesposobnost za rad) nakon što uzme u obzir standarde primjenjive na savezne suce utvrđene u Pravilima za postupke utvrđivanja povrede dužnosti i nesposobnosti za rad sudaca ([373]).

([365]) Članak 201.6. točke (a)–(b) Uredbe glavnog državnog odvjetnika.

([366]) Članak 3. točka (d)(i) i Uredba glavnog državnog odvjetnika. Vrhovni sud SAD-a potvrdio je da glavni državni odvjetnik može osnivati neovisna tijela s ovlastima za donošenje odluka, među ostalim radi odlučivanja u pojedinim predmetima, vidjeti posebno *SAD ex rel. Accardi protiv Shaughnessyja*, 347 U.S. 260 (1954.) i *Sjedinjenje Američke Države protiv Nixona*, 418 U.S. 683, 695 (1974.). Usklađenost s različitim zahtjevima iz Izvršnog naloga br. 14086, na primjer kriterijima i postupkom imenovanja i razrješenja sudaca DPRC-a, posebno podliježe nadzoru glavnog inspektora Ministarstva pravosuđa (vidjeti i uvodnu izjavu 109. o zakonskoj ovlasti glavnih inspektora).

([367]) Članak 3. točka (d)(i)(A) Izvršnog naloga br. 14086 i članak 201.3. točka (a) Uredbe glavnog državnog odvjetnika.

([368]) Članak 201.3. točka (b) Uredbe glavnog državnog odvjetnika.

([369]) Članak 3. točka (d)(i)(B) Izvršnog naloga br. 14086.

([370]) Članak 3. točka (d)(i)(A) Izvršnog naloga br. 14086 i članak 201.3. točke (a) i (c) Uredbe glavnog državnog odvjetnika. Pojedinci imenovani u DPRC mogu sudjelovati u izvansudskim aktivnostima, uključujući poslovne aktivnosti, financijske aktivnosti, neprofitno prikupljanje sredstava i povjereničke djelatnosti, te obavljati odvjetničku službu sve dok te aktivnosti ne utječu na nepristrano izvršavanje njihovih dužnosti odnosno na djelotvornost ili neovisnost DPRC-a (članak 201.7. točka (c) Uredbe glavnog državnog odvjetnika).

([371]) Članak 3. točke (d)(iii)–(iv) Izvršnog naloga br. 14086 i članak 201.7. točka (d) Uredbe glavnog državnog odvjetnika.

([372]) Članak 3. točka (d)(i)(D) Izvršnog naloga br. 14086 i članak 201.9. Uredbe glavnog državnog odvjetnika.

([373]) Članak 3. točka (d)(iv) Izvršnog naloga br. 14086 i članak 201.7. točka (d) Uredbe glavnog državnog odvjetnika. Vidjeti i predmet Bumap protiv SAD-a, 252 U.S. 512, 515 (1920.), u kojem je potvrđeno dugogodišnje načelo u pravu SAD-a da je ovlast za razrješenje povezana s ovlasti za imenovanje (kao što je podsjetio Ured pravnog savjetnika pri Ministarstvu pravosuđa u memorandumu *The Constitutional Separation of Powers Between the President and Congress*, 20 Op. O.L.C. 124, 166 (1996.)).

(188) Zahtjeve podnesene DPRC-u preispituje sudsko vijeće sastavljeno od tri suca, uključujući predsjedavajućeg suca, koji moraju postupati u skladu s Kodeksom ponašanja za suce SAD-a ([374]). Svakom sudskom vijeću u radu pomaže posebni odvjetnik ([375]) koji ima pristup svim informacijama povezanima s predmetom, uključujući klasificirane podatke ([376]). Posebni odvjetnik odgovoran je za zastupanje interesa podnositelja pritužbe te informiranje sudskog vijeća DPRC-a o svim relevantnim pravnim i činjeničnim pitanjima ([377]). Kako bi prikupio dodatne informacije za potrebe oblikovanja stajališta o zahtjevu za preispitivanje koji je pojedinac podnio DPRC-u, posebni odvjetnik može podnositelju pritužbe uputiti pisana pitanja ([378]).

(189) DPRC preispituje utvrđenja službenika za zaštitu građanskih sloboda ODNI-ja (je li došlo do povrede primjenjivog prava SAD-a i koje su korektivne mjere primjerene) na temelju barem evidencije tog službenika o istrazi te svih informacija i podnesaka podnositelja pritužbe, specijalnog odvjetnika ili obavještajne agencije ([379]). Sudsko vijeće DPRC-a može pristupiti svim informacijama koje su mu nužne za preispitivanje i može ih dobiti od službenika za zaštitu građanskih sloboda ODNI-ja (sudsko vijeće može npr. zatražiti od tog službenika da dopuni svoju evidenciju dodatnim informacijama ili činjeničnim utvrđenjima ako je to nužno za preispitivanje) ([380]).

(190) Kad završi preispitivanje, DPRC može 1. odlučiti da nema dokaza koji upućuju na to da su osobni podaci podnositelja pritužbe bili predmet aktivnosti elektroničkog izviđanja, 2. odlučiti da su utvrđenja službenika za zaštitu građanskih sloboda ODNI-ja pravno točna i potkrijepljena zadovoljavajućim dokazima ili 3. ako se DPRC ne slaže s odlukama tog službenika (o tome je li došlo do povrede primjenjivog američkog prava ili koje su korektivne mjere primjerene), može donijeti vlastitu odluku ([381]).

([374]) Članak 3. točka (d)(i)(B) Izvršnog naloga br. 14086 i članak 201.7. točke (a)–(c) Uredbe glavnog državnog odvjetnika. Ured za privatnost i građanske slobode pri Ministarstvu pravosuđa (OPCL), koji pruža administrativnu podršku DPRC-u i posebnim odvjetnicima (vidjeti članak 201.5. Uredbe glavnog državnog odvjetnika), naizmjence odabire tri člana sudskog vijeća kako bi u svakom sudskom vijeću bio najmanje jedan sudac s prethodnim sudačkim iskustvom (ako nijedan od sudaca u sudskom vijeću nema takvo iskustvo, predsjedavajući sudac onaj je kojeg je OPCL prvog odabrao).

([375]) Članak 201.4. Uredbe glavnog državnog odvjetnika. Glavni državni odvjetnik u dogovoru s ministrom trgovine, direktorom za nacionalna obavještajna pitanja i PCLOB-om imenuje najmanje dva posebna odvjetnika na dva mandata s mogućnošću produljenja. Posebni odvjetnici moraju imati odgovarajuće iskustvo u području propisa o privatnosti i nacionalnoj sigurnosti te biti iskusni pravni stručnjaci, aktivni članovi koji ispunjavaju sve obveze u komori i propisno licencirani za obavljanje odvjetničke službe. Nadalje, u trenutku prvog imenovanja nisu smjeli biti zaposleni u izvršnoj vlasti u prethodne dvije godine. Za svako preispitivanje zahtjeva predsjedavajući sudac odabire posebnog odvjetnika koji će pomagati sudskom vijeću, vidjeti članak 201.8. točku (a) Uredbe glavnog državnog odvjetnika.

([376]) Članak 201.8. točka (c) i članak 201.11. Uredbe glavnog državnog odvjetnika.

([377]) Članak 3. točka (d)(i)(C) Izvršnog naloga br. 14086 i članak 201.8. točka (e) Uredbe glavnog državnog odvjetnika. Posebni odvjetnik ne postupa u ime podnositelja pritužbe niti mu je podnositelj pritužbe klijent.

([378]) Vidjeti članak 201.8. točke (d)–(e) Uredbe glavnog državnog odvjetnika. Ta pitanja prvo provjerava OPCL uz savjetovanje s nadležnim subjektom obavještajne zajednice kako bi utvrdio i izuzeo sve klasificirane, privilegirane ili zaštićene informacije prije njihova slanja podnositelju pritužbe. Dodatne informacije koje posebni odvjetnik primi u odgovorima na ta pitanja unose se u podneske posebnog odvjetnika DPRC-u.

([379]) Članak 3. točka (d)(i)(D) Izvršnog naloga br. 14086.

([380]) Članak 3. točka (d)(iii) Izvršnog naloga br. 14086 i članak 201.9. točka (b) Uredbe glavnog državnog odvjetnika.

([381]) Članak 3. točka (d)(i)(E) Izvršnog naloga br. 14086 i članak 201.9. točke (c)–(e) Uredbe glavnog državnog odvjetnika. U skladu s definicijom „primjerenih korektivnih mjera” iz članka 4. točke (a) Izvršnog naloga br. 14086 DPRC mora uzeti u obzir „načine na koje se obično rješavala utvrđena povreda” kad odlučuje koja bi korektivna mjera u potpunosti riješila povredu, tj. DPRC će, među ostalim čimbenicima, razmotriti kako su slični problemi zbog neusklađenosti riješeni u prošlosti kako bi se osiguralo da je pravni lijek djelotvoran i primjeren.

(191) DPRC u svim predmetima donosi pisanu odluku većinom glasova. Ako se preispitivanjem otkrije povreda primjenjivih pravila, u odluci će se navesti primjerene korektivne mjere, što uključuje brisanje nezakonito prikupljenih podataka, brisanje rezultata neispravnih pretraživanja, ograničavanje pristupa zakonito prikupljenim podacima na primjereno osposobljeno osoblje ili povlačenje obavještajnih izvješća s podacima koji su prikupljeni bez zakonitog odobrenja ili su se nezakonito širili ([382]). DPRC donosi odluke o pritužbama koje su obvezujuće i pravomoćne ([383]). Nadalje, ako se preispitivanjem otkrije povreda koju je počinilo tijelo koje nadzire FISC, DPRC mora izraditi i klasificirano izvješće za pomoćnika glavnog državnog odvjetnika za nacionalnu sigurnost, koji je potom o neusklađenosti obvezan obavijestiti FISC, koji može poduzeti daljnje provedbene mjere (u skladu s postupkom opisanim u izjavama od 173. do 174.) ([384]).

(192) Sve odluke sudskog vijeća DPRC-a prosljeđuju se službeniku za zaštitu građanskih sloboda ODNI-ja ([385]). Ako DPRC provodi preispitivanje na temelju zahtjeva podnositelja pritužbe, preko nacionalnog tijela obavješćuje se podnositelja pritužbe da je DPRC završio preispitivanje i da „preispitivanjem nisu utvrđene predmetne povrede ili je DPRC utvrdio koje primjerene korektivne mjere treba provesti" ([386]). Ured za privatnost i građanske slobode pri Ministarstvu pravosuđa vodi evidenciju svih informacija koje DPRC preispituje i svih izdanih odluka pa se buduća sudska vijeća DPRC-a mogu njome poslužiti kao neobvezujućom zbirkom presedana ([387]).

(193) Osim toga, Ministarstvo trgovine mora voditi evidenciju o svim podnositeljima pritužbe koji su podnijeli pritužbu ([388]). Radi veće transparentnosti Ministarstvo trgovine mora najmanje svakih pet godina s nadležnom obavještajnom agencijom provjeriti jesu li informacije o preispitivanju DPRC-a deklasificirane ([389]). Ako jesu, pojedinca će se obavijestiti da se te informacije mogu dobiti u skladu s primjenjivim pravom (tj. da može zatražiti pristup tim informacijama u skladu sa Zakonom o pravu na pristup informacijama, vidjeti uvodnu izjavu 199.).

(194) Naposljetku, pravilno funkcioniranje tog mehanizma pravne zaštite redovito će se i neovisno evaluirati. Točnije, u skladu s Izvršnim nalogom br. 14086 PCLOB, neovisno tijelo svake godine mora preispitati funkcioniranje mehanizma pravne zaštite (vidjeti uvodnu izjavu 110.) ([390]). Pritom će PCLOB, među ostalim, ocijeniti jesu li službenik za zaštitu građanskih sloboda ODNI-ja i DPRC pravodobno riješili pritužbe, jesu li dobili potpun pristup nužnim informacijama, jesu li pri preispitivanju na odgovarajući način uzeli u obzir materijalne zaštitne mjere iz Izvršnog naloga br. 14086 i je li obavještajna zajednica u potpunosti postupila u skladu s odlukama službenika za zaštitu građanskih sloboda ODNI-ja i DPRC-a. PCLOB će izraditi izvješće o ishodu preispitivanja za predsjednika, glavnog državnog odvjetnika, direktora za nacionalna obavještajna pitanja, ravnatelje obavještajnih agencija, službenika za zaštitu građanskih sloboda ODNI-ja i kongresne odbore za obavještajna pitanja, objaviti i njegovu neklasificiranu inačicu te će ga Komisija uzeti u obzir pri periodičnom preispitivanju funkcioniranja ove Odluke. Glavni državni odvjetnik, direktor za nacionalna obavještajna pitanja, službenik za zaštitu građanskih sloboda ODNI-ja i ravnatelji obavještajnih agencija moraju provesti sve preporuke iz tih izvješća ili ih na drugi način uzeti u obzir. Nadalje, PCLOB će izdati godišnju javnu potvrdu o tome rješavaju li se pritužbe u okviru mehanizma pravne zaštite u skladu sa zahtjevima iz Izvršnog naloga br. 14086.

([382]) Članak 4. točka (a) Izvršnog naloga br. 14086.

([383]) Članak 3. točka (d)(ii) Izvršnog naloga br. 14086 i članak 201.9. točka (g) Uredbe glavnog državnog odvjetnika. Budući da je odluka DPRC-a pravomoćna i obvezujuća, nijedna druga izvršna ni upravna institucija/tijelo (uključujući predsjednika SAD-a) ne može poništiti odluku DPRC-a. To je potvrđeno i u sudskoj praksi Vrhovnog suda, u kojoj je pojašnjeno da si glavni državni odvjetnik, delegiranjem svoje jedinstvene ovlasti u izvršnoj vlasti za donošenje obvezujućih odluka neovisnom tijelu, uskraćuje mogućnost da na bilo koji način utječe na odluku tog tijela (vidjeti *Sjedinjene Američke Države ex rel. Accardi protiv Shaughnessyja*, 347 U.S. 260 (1954.)).

([384]) Članak 3. točka (d)(i)(F) Izvršnog naloga br. 14086 i članak 201.9. točka (i) Uredbe glavnog državnog odvjetnika.

([385]) Članak 201.9. točka (h) Uredbe glavnog državnog odvjetnika.

([386]) Članak 3. točka (d)(i)(H) Izvršnog naloga br. 14086 i članak 201.9. točka (h) Uredbe glavnog državnog odvjetnika. Za prirodu obavijesti vidjeti članak 201.9. točku (h)(3) Uredbe glavnog državnog odvjetnika.

([387]) Članak 201.9. točka (j) Uredbe glavnog državnog odvjetnika.

([388]) Članak 3. točka (d)(v)(A) Izvršnog naloga br. 14086.

([389]) Članak 3. točka (d)(v) Izvršnog naloga br. 14086.

([390]) Članak 3. točka (e) Izvršnog naloga br. 14086. Vidjeti i https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf

(195) Uz poseban mehanizam pravne zaštite uspostavljen u skladu s Izvršnim nalogom br. 14086 postoje i drugi oblici pravne zaštite pred redovnim sudovima SAD-a koji su dostupni svim pojedincima (neovisno o državljanstvu ili boravištu) ([391]).

(196) Točnije, u skladu sa Zakonom o nadzoru stranih obavještajnih aktivnosti i povezanim zakonom pojedinci mogu pokrenuti građanski postupak protiv SAD-a ako su se informacije o njima nezakonito i samovoljno upotrebljavale ili otkrivale ([392]), podnijeti tužbu protiv dužnosnika američke vlade kao privatne osobe radi novčane odštete ([393]) i osporavati zakonitost nadzora (i tražiti uklanjanje informacija) ako američka vlada namjerava upotrijebiti ili otkriti informacije dobivene elektroničkim izviđanjem ili izvedene iz njega protiv osobe u sudskim ili upravnim postupcima u SAD-u ([394]). Općenitije, ako informacije dobivene obavještajnim aktivnostima vlada namjerava upotrijebiti protiv osumnjičenika u kaznenom predmetu, u skladu s ustavnim i zakonskim zahtjevima ([395]) dužna je otkriti određene informacije kako bi tuženik mogao osporavati zakonitost vladina prikupljanja i uporabe dokaza.

(197) Nadalje, postoji nekoliko posebnih oblika zaštite u okviru kojih se nudi podnošenje pravnog sredstva protiv vladinih dužnosnika zbog nezakonitog pristupa vlade osobnim podacima ili njihove uporabe, među ostalim u navodne svrhe nacionalne sigurnosti (tj. Zakon o računalnoj prijevari i zlouporabi ([396]), Zakon o zaštiti privatnosti elektroničke komunikacije ([397]) i Zakon o pravu na privatnost financijskih podataka ([398])). Svi ti postupci odnose se na konkretne podatke, ciljane osobe i/ili vrste pristupa (npr. daljinski pristup računalu internetom) i dostupni su pod određenim uvjetima (npr. namjerno/samovoljno postupanje, postupanje izvan službene dužnosti, pretrpljena šteta).

(198) Općenitija pravna zaštita može se ostvariti na temelju Zakona o upravnom postupku ([399]), prema kojem „svaka osoba koja je pretrpjela štetu zbog mjere agencije protivne zakonu ili na koju je mjera agencije štetno djelovala odnosno kojoj su mjerom agencije povrijeđena prava” ima pravo tražiti sudsko preispitivanje ([400]). To uključuje mogućnost da od suda zatraži da „proglasi nezakonitima i ukine mjere, nalaze i zaključke agencija za koje se utvrdi da su […] samovoljni i doneseni iz inata, da čine zlouporabu diskrecijskih prava ili da na drugi način nisu u skladu sa zakonom” ([401]). Na primjer, savezni žalbeni sud u postupku pokrenutom na temelju Zakona o upravnom postupku 2015. donio je odluku da skupno prikupljanje metapodataka o telefonskim pozivima koje je obavljala američka vlada nije dopušteno člankom 501. Zakona o nadzoru stranih obavještajnih aktivnosti ([402]).

([391]) Ti se oblici zaštite mogu iskoristiti ako se dokaže „aktivna legitimacija”. Taj standard, koji se primjenjuje na sve pojedince neovisno o državljanstvu, proizlazi iz zahtjeva iz članka III. američkog Ustava da postoji „predmet ili spor”. Prema Vrhovnom sudu, da bi se taj zahtjev ispunio, 1. pojedinac mora pretrpjeti „činjeničnu štetu” (tj. stvarna i individualizirana te postojeća ili neminovna šteta zakonom zaštićenog interesa), 2. mora postojati uzročno-posljedična veza između štete i postupanja osporavanog pred sudom i 3. ne nagađa se, nego je vjerojatno da će se sudskom odlukom u korist pojedinca ukloniti šteta (vidjeti *Lujan protiv Defenders of Wildlife*, 504 U.S. 555 (1992.)).

([392]) Glava 18. članak 2712. Zakonika SAD-a.

([393]) Glava 50. članak 1810. Zakonika SAD-a.

([394]) Glava 50. članak 1806. Zakonika SAD-a.

([395]) Vidjeti *Brady protiv Marylanda*, 373 U.S. 83 (1963.) odnosno Zakon Jencks, glava 18. članak 3500. Zakonika SAD-a.

([396]) Glava 18. članak 1030. Zakonika SAD-a.

([397]) Glava 18. članci od 2701. do 2712. Zakonika SAD-a.

([398]) Glava 12. članak 3417. Zakonika SAD-a.

([399]) Glava 5. članak 702. Zakonika SAD-a.

([400]) Sudskom preispitivanju obično podliježe samo „krajnja”, a ne „prethodna, postupovna ili privremena” mjera agencije. Vidjeti glavu 5. članak 704. Zakonika SAD-a.

([401]) Glava 5. članak 706. točka (2)(A) Zakonika SAD-a.

([402]) *ACLU protiv Clappera*, 785 F.3d 787 (2. okrug, 2015.); program skupnog prikupljanja podataka o telefonskim pozivima osporavan u tim predmetima ukinut je 2015. Zakonom SAD-a o slobodi (FREEDOM Act).

(199) Naposljetku, uz oblike pravne zaštite navedene u uvodnim izjavama od 176. do 198. svi pojedinci imaju pravo tražiti pristup postojećim evidencijama saveznih agencija u skladu sa Zakonom o pravu na pristup informacijama, među ostalim kad se u njima nalaze osobni podaci pojedinca ([403]). Dobivanje pristupa može olakšati i pokretanje postupka pred redovnim sudovima, među ostalim kao dokaz aktivne legitimacije. Agencije mogu uskratiti pristup informacijama koje su obuhvaćene određenim propisanim iznimkama, uključujući klasificirane informacije u području nacionalne sigurnosti i informacije o istragama tijela kaznenog progona ([404]), no podnositelji pritužbi koji nisu zadovoljni njihovim odgovorom mogu ga osporavati u postupku upravnog, a potom i sudskog preispitivanja (pred saveznim sudovima) ([405]).

(200) Iz prethodno navedenog proizlazi da je pristup američkih tijela kaznenog progona i tijela za nacionalnu sigurnost osobnim podacima koji su obuhvaćeni područjem primjene ove Odluke uređen pravnim okvirom u kojem su utvrđeni uvjeti za pristup podacima te kojim se pristup podacima i njihova daljnja uporaba ograničavaju na ono što je nužno i proporcionalno postavljenom cilju od javnog interesa. Provedbu tih zaštitnih mjera mogu zatražiti pojedinci koji uživaju prava na djelotvornu pravnu zaštitu.

4. **ZAKLJUČAK**

(201) Komisija smatra da Načelima, koja je objavilo Ministarstvo trgovine, SAD osigurava razinu zaštite osobnih podataka koji se prenose iz Unije u certificirane organizacije u SAD-u u skladu s okvirom EU-a i SAD-a za privatnost podataka koja je u načelu istovjetna onoj koja se jamči Uredbom (EU) 2016/679.

(202) Nadalje, Komisija smatra da se djelotvorna primjena Načela jamči obvezama transparentnosti i načinom na koji Ministarstvo trgovine upravlja okvirom za privatnost podataka. Osim toga, nadzorni mehanizmi i oblici pravne zaštite u američkom pravu kao cjelina u praksi omogućuju utvrđivanje kršenja pravila o zaštiti podataka i njihovo kažnjavanje te ispitanicima stavljaju na raspolaganje pravna sredstva za dobivanje pristupa osobnim podacima koji se odnose na njih te u konačnici za ispravak ili brisanje tih podataka.

(203) Naposljetku, prema dostupnim informacijama o američkom pravnom poretku, uključujući informacije iz priloga VI. i VII., Komisija smatra da će zadiranje američkih javnih tijela u temeljna prava pojedinaca čiji se podaci prenose iz Unije u SAD u skladu s okvirom EU-a i SAD-a za privatnost podataka u javnom interesu, ponajprije u svrhe kaznenog progona i svrhe nacionalne sigurnosti, biti ograničeno na ono što je nužno za ostvarenje predmetnog legitimnog cilja i da postoji učinkovita pravna zaštita protiv takvog zadiranja. Stoga bi, s obzirom na prethodne zaključke, trebalo odlučiti da SAD osigurava primjerenu razinu zaštite u smislu članka 45. Uredbe (EU) 2016/679, kako se tumači s obzirom na Povelju Europske unije o temeljnim pravima, kad je riječ o osobnim podacima koji se prenose iz Europske unije organizacijama certificiranima u skladu s okvirom EU-a i SAD-a za privatnost podataka.

(204) Budući da su ograničenja, zaštitne mjere i mehanizam pravne zaštite uspostavljeni Izvršnim nalogom br. 14086 ključni elementi američkog pravnog okvira na kojem se temelji Komisijina procjena, donošenje ove Odluke prvenstveno ovisi o donošenju ažuriranih politika i postupaka za provedbu Izvršnog naloga br. 14086 u svim američkim obavještajnim agencijama, što je učinjeno 3. srpnja 2023. (vidjeti uvodnu izjavu 126.), i dodjeljivanju Uniji statusa organizacije koja ispunjava uvjete za potrebe mehanizma pravne zaštite, što je učinjeno 30. lipnja 2023. (vidjeti uvodnu izjavu 176.).

([403]) Glava 5. članak 552. Zakonika SAD-a. Slični zakoni postoje na razini saveznih država.

([404]) U tom slučaju pojedinac će obično zaprimiti samo standardni odgovor kojim agencija odbija potvrditi ili poreći postojanje evidencije. Vidjeti *ACLU/CIA*, 710 F.3d 422 (Okrug Columbia, 2014.). Kriteriji za klasifikaciju i trajanje klasifikacije utvrđeni su u Izvršnom nalogu br. 13526, kojim se u pravilu predviđa da se na temelju trajanja osjetljivosti informacija za nacionalnu sigurnost mora utvrditi određeni datum ili događaj za deklasifikaciju kad se podaci moraju automatski deklasificirati (vidjeti članak 1.5. Izvršnog naloga br. 13526).

([405]) Sud ponovno utvrđuje je li uskraćivanje pristupa evidencijama zakonito i može naložiti vladi da omogući pristup (glava 5. članak 552. točka (a)(4)(B) Zakonika SAD-a).

5. **UČINCI OVE ODLUKE I AKTIVNOSTI TIJELA ZA ZAŠTITU PODATAKA**

(205) Države članice i njihova tijela dužni su poduzeti mjere potrebne za usklađivanje s aktima institucija Unije jer se potonji 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.

(206) Stoga je odluka Komisije o primjerenosti donesena u skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 obvezujuća za sva tijela država članica kojima je upućena, uključujući njihova neovisna nadzorna tijela. Točnije, za prijenose od voditelja ili izvršitelja obrade u Uniji certificiranim organizacijama u SAD-u nisu potrebna daljnja odobrenja.

(207) Trebalo bi podsjetiti na to da, u skladu s člankom 58. stavkom 5. Uredbe (EU) 2016/679 i kako je objašnjeno u presudi Suda u predmetu *Schrems* ([406]), ako nacionalno tijelo za zaštitu podataka, među ostalim nakon što je zaprimilo pritužbu, ima sumnje u pogledu spojivosti odluke Komisije o primjerenosti s temeljnim pravima pojedinca na privatnost i zaštitu podataka, nacionalnim pravom mora biti predviđeno pravno sredstvo za iznošenje tih prigovora pred nacionalnim sudom, od kojeg se može tražiti da Sudu Europske unije uputi zahtjev za prethodnu odluku ([407]).

6. **PRAĆENJE I PREISPITIVANJE OVE ODLUKE**

(208) U skladu sa sudskom praksom Suda ([408]), a kako je potvrđeno u članku 45. stavku 4. Uredbe (EU) 2016/679, Komisija bi nakon donošenja odluke o primjerenosti trebala kontinuirano pratiti relevantne događaje u trećoj zemlji kako bi ocijenila osigurava li ta treća zemlja i dalje u načelu istovjetnu razinu zaštite. Takva provjera potrebna je, u svakom slučaju, kad Komisija dobije informacije na temelju kojih može opravdano posumnjati u to.

(209) Stoga bi Komisija trebala kontinuirano pratiti situaciju u SAD-u u pravnom okviru i stvarnoj praksi za obradu osobnih podataka kako je ocijenjeno u ovoj Odluci. Kako bi olakšala taj proces, američka tijela trebala bi odmah obavijestiti Komisiju o svim bitnim promjenama američkog pravnog poretka koje imaju učinak na pravni okvir koji je predmet ove Odluke, kao i o svim promjenama prakse povezane s obradom osobnih podataka koja se ocjenjuje u ovoj Odluci u pogledu obrade osobnih podataka koju provode certificirane organizacije u SAD-u, ali i ograničenja i zaštitnih mjera koji se primjenjuju na pristup javnih tijela osobnim podacima.

(210) Nadalje, kako bi Komisija mogla djelotvorno obavljati svoju funkciju praćenja, države članice trebale bi je obavješćivati o svim relevantnim mjerama koje poduzimaju nacionalna tijela za zaštitu podataka, naročito u pogledu upita ili pritužbi ispitanika iz Unije o prijenosu osobnih podataka iz Unije certificiranim organizacijama u SAD-u. Komisiju bi trebalo obavijestiti i o svakoj naznaci da se mjerama američkih javnih tijela odgovornih za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili za nacionalnu sigurnost, uključujući nadzorna tijela, ne osigurava potrebna razina zaštite.

([406]) *Schrems*, t. 65.

([407]) *Schrems*, t. 65: „U tom je pogledu nacionalni zakonodavac dužan predvidjeti pravna sredstva koja neovisnom nadzornom tijelu omogućavaju isticanje prigovora pred nacionalnim sudovima koje smatra osnovanima, kako bi ti sudovi mogli, u slučaju da dijele sumnje tog tijela u vezi s valjanošću Komisijine odluke, uputiti zahtjev za prethodnu odluku radi ispitivanja valjanosti te odluke”.

([408]) *Schrems*, t. 76.

(211) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 ([409]) Komisija bi nakon donošenja ove Odluke trebala periodično preispitati jesu li zaključci o primjerenosti razine zaštite koju Sjedinjene Američke Države osiguravaju u skladu s okvirom EU-a i SAD-a za privatnost podataka i dalje činjenično i pravno opravdani. Budući da su ponajprije Izvršnim nalogom br. 14086 i Uredbom glavnog državnog odvjetnika propisane uspostava novih mehanizama i provedba novih zaštitnih mjera, ovu Odluku trebalo bi prvi put preispitati godinu dana od njezina stupanja na snagu kako bi se provjerilo jesu li svi relevantni elementi u potpunosti provedeni i funkcioniranju li stvarno u praksi. Nakon prvog preispitivanja i ovisno o njegovu ishodu Komisija će u bliskoj suradnji s odborom osnovanim na temelju članka 93. stavka 1. Uredbe (EU) 2016/679 i Europskim odborom za zaštitu podataka odlučiti o periodičnosti budućih preispitivanja ([410]).

(212) Za potrebe preispitivanja Komisija bi se trebala sastati s Ministarstvom trgovine, FTC-om i Ministarstvom prometa te prema potrebi s drugim ministarstvima i agencijama uključenima u provedbu okvira EU-a i SAD-a za privatnost podataka, a u vezi s pitanjima povezanima s pristupom vlade podacima s predstavnicima Ministarstva pravosuđa, ODNI-jem (uključujući službenika za zaštitu građanskih sloboda), drugim subjektima obavještajne zajednice, DPRC-om i posebnim odvjetnicima. Sudjelovanje na tom sastanku trebalo bi biti otvoreno za predstavnike članova Europskog odbora za zaštitu podataka.

(213) Ta bi preispitivanja trebala obuhvatiti sve aspekte funkcioniranja ove Odluke u pogledu obrade osobnih podataka u SAD-u, a posebno primjenu i provedbu Načela, pri čemu bi posebnu pozornost trebalo posvetiti zaštiti koja se pruža u slučaju daljnjeg prijenosa, razvoju relevantne sudske prakse, djelotvornosti ostvarivanja prava pojedinaca, praćenju i osiguravanju usklađenosti s Načelima, kao i ograničenjima i zaštitnim mjerama za pristup vlade, posebice provedbi i primjeni zaštitnih mjera uvedenih Izvršnim nalogom br. 14086 među ostalim u okviru politika i postupaka koje su osmislile obavještajne agencije, međudjelovanju Izvršnog naloga br. 14086 i članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti i Izvršnog naloga br. 12333 te djelotvornosti nadzornih mehanizama i oblika pravne zaštite (uključujući funkcioniranje novog mehanizma pravne zaštite uspostavljenog Izvršnim nalogom br. 14086). U okviru tih preispitivanja pozornost će se posvetiti i suradnji između tijela za zaštitu podataka i nadležnih tijela SAD-a, uključujući pripremu smjernica i drugih instrumenata za tumačenje primjene Načela te drugih aspekata funkcioniranja Okvira.

(214) Na temelju preispitivanja Komisija bi trebala sastaviti javno izvješće koje podnosi Europskom parlamentu i Vijeću.

7. **SUSPENZIJA, STAVLJANJE IZVAN SNAGE ILI IZMJENA OVE ODLUKE**

(215) Ako dostupne informacije, naročito one dobivene praćenjem primjene ove Odluke ili one koje dostavljaju američka tijela ili tijela država članica, pokažu da razina zaštite podataka koji se prenose na temelju ove Odluke možda više nije primjerena, Komisija bi o tome trebala bez odgode obavijestiti nadležna američka tijela i zatražiti poduzimanje odgovarajućih mjera u određenom, razumnom roku.

(216) Ako nakon isteka navedenog roka nadležna američka tijela ne poduzmu te mjere ili na drugi zadovoljavajući način ne dokažu da se ova Odluka i dalje temelji na primjerenoj razini zaštite, Komisija će pokrenuti postupak iz članka 93. stavka 2. Uredbe (EU) 2016/679 radi djelomične ili potpune suspenzije ili stavljanja izvan snage ove Odluke.

(217) Alternativno, Komisija će pokrenuti taj postupak radi izmjene Odluke, ponajprije utvrđivanjem dodatnih uvjeta za prijenose podataka ili ograničavanjem područja primjene zaključka o primjerenosti samo na prijenose podataka za koje se i dalje osigurava primjerena razina zaštite.

([409]) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 „[u] provedbenom aktu predviđa se mehanizam za periodično preispitivanje, […] kojim će se uzeti u obzir svi relevantni događaji u toj trećoj zemlji ili međunarodnoj organizaciji".

([410]) Člankom 45. stavkom 3. Uredbe (EU) 2016/679 predviđeno je da se periodično preispitivanje mora provoditi „najmanje svake četiri godine". Vidjeti i Europski odbor za zaštitu podataka, Referentni dokument o primjerenosti, WP 254 rev.01.

(218) Točnije, Komisija bi trebala pokrenuti postupak suspenzije ili stavljanja izvan snage u sljedećim slučajevima:

(a) postoje naznake da organizacije koje su primale osobne podatke iz Unije na temelju ove Odluke nisu usklađene s Načelima te da nadležna nadzorna i provedbena tijela nisu na djelotvoran način pokušala riješiti tu neusklađenost;

(b) postoje naznake da se američka tijela ne pridržavaju primjenjivih uvjeta ni ograničenja za pristup američkih javnih tijela, u svrhe kaznenog progona i nacionalne sigurnosti, osobnim podacima koji se prenose u skladu s okvirom EU-a i SAD-a za privatnost podataka; ili

(c) tijela, među ostalim ODNI, službenik za zaštitu građanskih sloboda i/ili DPRC, ne rješavaju na djelotvoran način pritužbe ispitanika iz Unije.

(219) Komisija bi trebala razmotriti i pokretanje postupka za izmjenu, suspenziju ili stavljanje izvan snage ove Odluke ako nadležna američka tijela ne dostave informacije ili pojašnjenja koja su potrebna za ocjenu razine zaštite osobnih podataka koji se prenose iz Unije u SAD ili usklađenosti s ovom Odlukom. S obzirom na to Komisija bi trebala uzeti u obzir opseg u kojem se relevantne informacije mogu dobiti iz drugih izvora.

(220) Zbog opravdanih krajnje hitnih razloga, na primjer ako se Izvršni nalog br. 14086 ili Uredba glavnog državnog odvjetnika izmijene tako da se naruši razina zaštite opisana u ovoj Odluci ili ako se Uniji oduzme status organizacije koja ispunjava uvjete za potrebe mehanizma pravne zaštite koji joj je dodijelio glavni državni odvjetnik, Komisija će iskoristiti mogućnost donošenja, u skladu s postupkom iz članka 93. stavka 3. Uredbe (EU) 2016/679, odmah primjenjivih provedbenih akata o suspenziji, stavljanju izvan snage ili izmjeni ove Odluke.

8. **ZAVRŠNA RAZMATRANJA**

(221) Europski odbor za zaštitu podataka objavio je svoje mišljenje ([411]), koje je uzeto u obzir pri pripremi ove Odluke.

(222) Europski parlament donio je rezoluciju o primjerenosti zaštite koju pruža okvir EU-a i SAD-a za zaštitu podataka ([412]).

(223) Mjere predviđene u ovoj Odluci u skladu su s mišljenjem Odbora osnovanog na temelju članka 93. stavka 1. Uredbe (EU) 2016/679,

DONIJELA JE OVU ODLUKU:

Članak 1.

Za potrebe članka 45. Uredbe (EU) 2016/679 SAD osigurava primjerenu razinu zaštite osobnih podataka koji se prenose iz Unije organizacijama u SAD-u koje se nalaze na popisu organizacija uključenih u okvir za privatnost podataka, koji vodi i objavljuje američko Ministarstvo trgovine u skladu s odjeljkom I.3. Priloga I.

Članak 2.

Kad god nadležna tijela u državama članicama radi zaštite pojedinaca u vezi s obradom njihovih osobnih podataka izvršavaju svoje ovlasti u skladu s člankom 58. Uredbe (EU) 2016/679 u pogledu prijenosa podataka iz članka 1. ove Odluke, predmetna država članica o tome bez odgode obavješćuje Komisiju.

([411]) Mišljenje 5/2023 o Nacrtu provedbene odluke Europske komisije o primjerenosti zaštite osobnih podataka na temelju okvira EU-a i SAD-a za privatnost podataka od 28. veljače 2023.

([412]) Rezolucija Europskog parlamenta od 11. svibnja 2023. o primjerenosti zaštite koju pruža okvir EU-a i SAD-a za zaštitu podataka (2023/2501(RSP)).

Članak 3.

1. Komisija neprekidno prati primjenu pravnog okvira koji je predmet ove Odluke, uključujući uvjete pod kojima se odvijaju daljnji prijenosi, ostvaruju prava pojedinaca i američka javna tijela imaju pristup podacima koji se prenose na temelju ove Odluke, kako bi ocijenila osigurava li SAD i dalje primjerenu razinu zaštite kako je navedeno u članku 1.

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

3. Države članice i Komisija uzajamno se obavješćuju o naznakama da se 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 proporcionalno i/ili da ne postoji učinkovita pravna zaštita protiv takvog zadiranja.

4. Godinu dana od dana kad su države članice obaviještene o ovoj Odluci, a potom u vremenskom intervalu koji će se utvrditi u bliskoj suradnji s odborom osnovanim na temelju članka 93. stavka 1. Uredbe (EU) 2016/679 i Europskim odborom za zaštitu podataka, Komisija ocjenjuje zaključak iz članka 1. stavka 1. na temelju svih dostupnih informacija, uključujući informacije dobivene u okviru preispitivanja provedenog s nadležnim tijelima SAD-a.

5. Ako Komisija ima naznake za to da primjerena razina zaštite više nije osigurana, o tome obavješćuje nadležna američka tijela. Ako je potrebno, može odlučiti suspendirati, izmijeniti ili staviti izvan snage ovu Odluku ili ograničiti njezino područje primjene u skladu s člankom 45. stavkom 5. Uredbe (EU) 2016/679. Komisija može donijeti takvu odluku ako zbog nesuradnje američke vlade ne može utvrditi osigurava li SAD i dalje primjerenu razinu zaštite.

Članak 4.

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 10. srpnja 2023.

Za Komisiju
Didier REYNDERS
Član Komisije

PRILOG I.

NAČELA OKVIRA EU-a i SAD-a ZA PRIVATNOST PODATAKA KOJA JE OBJAVILO AMERIČKO MINISTARSTVO TRGOVINE

I. PREGLED

1. Iako Sjedinjene Američke Države (SAD) i Europska unija (EU) imaju isti cilj povećanja zaštite privatnosti, vladavine prava i prepoznavanja važnosti transatlantskog protoka podataka za državljane, gospodarstva i društva SAD-a i EU-a, njihov se pristup privatnosti razlikuje. SAD primjenjuje sektorski pristup koji se oslanja na kombinaciju zakonodavstva, propisa i samoregulacije. Američko Ministarstvo trgovine objavljuje Načela okvira EU-a i SAD-a za privatnost podataka, uključujući Dodatna načela (zajedno „Načela") i Prilog I. Načelima („Prilog I.") u skladu sa svojom zakonskom ovlasti poticanja, promicanja i razvoja međunarodne trgovine (glava 15. članak 1512. Zakonika SAD-a). Načela su izrađena u dogovoru s Europskom komisijom („Komisija"), predstavnicima industrije i drugim dionicima kako bi se olakšala trgovina između SAD-a i EU-a. Načela, koja su ključna sastavnica okvira EU-a i SAD-a za privatnost podataka, organizacijama u SAD-u pružaju pouzdan mehanizam za prijenose osobnih podataka iz EU-a u SAD i ujedno osiguravaju kontinuirani pristup ispitanika iz EU-a djelotvornim zaštitnim mjerama i zaštiti kako je propisano europskim zakonodavstvom u pogledu obrade njihovih osobnih podataka pri prijenosu u treće zemlje. Načela su namijenjena isključivo prihvatljivim organizacijama u SAD-u koje primaju osobne podatke iz EU-a kako bi mogle sudjelovati u okviru EU-a i SAD-a za privatnost podataka te kako bi se Komisijina odluka o primjerenosti mogla primjenjivati na njih ([1]). Načela ne utječu na primjenu Uredbe (EU) 2016/679 („Opća uredba o zaštiti podataka" ili „OUZP") ([2]), koja se primjenjuje na obradu osobnih podataka u državama članicama EU-a. Načela ne ograničavaju obveze u pogledu privatnosti koje se inače primjenjuju u skladu s američkim pravom.

2. Da bi mogla sudjelovati u okviru EU-a i SAD-a za privatnost podataka radi prijenosa osobnih podataka iz EU-a, organizacija mora samocertificiranjem Ministarstvu trgovine (ili tijelu koje je ono za to odredilo) potvrditi da se pridržava Načela. Iako organizacije mogu dobrovoljno odlučiti hoće li sudjelovati u okviru EU-a i SAD-a za privatnost podataka, u slučaju sudjelovanja stvarna je usklađenost obvezna: organizacije koje se samocertificiraju Ministarstvu trgovine i javno izjave da se obvezuju da će se pridržavati Načela moraju biti u potpunosti usklađene s njima. Da bi postala članica okvira EU-a i SAD-a za privatnost podataka, organizacija je obvezna (a) podvrgnuti se istražnim i provedbenim ovlastima Savezne trgovinske komisije (FTC), američkog Ministarstva prometa ili drugog zakonskog tijela koje će osigurati stvarnu usklađenost s Načelima (druga američka zakonska tijela koja je EU priznao mogu se u budućnosti uključiti kao prilog), (b) javno izjaviti da se obvezuje na usklađenost s Načelima, (c) javno izjaviti da su njezine politike zaštite privatnosti u skladu s ovim Načelima i (d) potpuno provoditi Načela ([3]). Organizaciju koja nije usklađena s Načelima može kazniti FTC u skladu s člankom 5. Zakona o FTC-u, kojim se zabranjuje nepošteno ili prijevarno postupanje u trgovini ili koje utječe na trgovinu (glava 15. članak 45. Zakonika SAD-a), Ministarstvo prometa u skladu s glavom 49. člankom 41712. Zakonika SAD-a, kojim se prijevozniku ili posredniku u prodaji karata zabranjuje nepoštena ili prijevarna praksa u zračnom prijevozu ili prodaji usluga zračnog prijevoza, ili može biti kažnjena u skladu s drugim zakonima ili propisima kojima se zabranjuje takvo postupanje.

([1]) Ako se odluka Komisije o primjerenosti zaštite koju pruža okvir EU-a i SAD-a za privatnost podataka primjenjuje na Island, Lihtenštajn i Norvešku, okvir EU-a i SAD-a za privatnost podataka obuhvatit će EU i tri navedene zemlje. Stoga se smatra da upućivanja na EU i države članice uključuju Island, Lihtenštajn i Norvešku.

([2]) Uredba (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).

([3]) Naziv „Načela europsko-američkog sustava zaštite privatnosti" promijenjen je u „Načela okvira EU-a i SAD-a za privatnost podataka". (Vidjeti dodatno načelo o samocertificiranju).

3. Ministarstvo trgovine vodit će i objavljivati obvezujući popis američkih organizacija koje su se samocertificirale tom ministarstvu i izjavile da će se pridržavati Načela („popis organizacija uključenih u okvir za privatnost podataka”). Okvir EU-a i SAD-a za privatnost podataka primjenjuje se od datuma kad Ministarstvo trgovine uvrsti organizaciju na popis organizacija uključenih u okvir za privatnost podataka. Ministarstvo trgovine s tog će popisa ukloniti organizacije koje se dobrovoljno povuku iz okvira EU-a i SAD-a za privatnost podataka ili ne ispune obvezu godišnje ponovne certifikacije Ministarstvu trgovine, pri čemu te organizacije moraju nastaviti primjenjivati Načela na osobne informacije koje su primile u skladu s okvirom EU-a i SAD-a za privatnost podataka i Ministarstvu trgovine svake godine potvrđivati svoju obvezu da će to činiti (odnosno sve dok zadržavaju te informacije), osigurati „primjerenu” zaštitu informacija drugim odobrenim sredstvima (npr. ugovorom u kojem se u cijelosti uzimaju u obzir zahtjevi relevantnih standardnih ugovornih klauzula koje je odobrila Komisija), ili vratiti odnosno izbrisati te informacije. Ministarstvo trgovine s tog će popisa ukloniti i organizacije koje su ustrajno neusklađene s Načelima, pri čemu te organizacije moraju vratiti ili izbrisati osobne informacije koje su primile u skladu s okvirom EU-a i SAD-a za privatnost podataka. Uklanjanje organizacije s popisa organizacija uključenih u okvir za privatnost podataka znači da se na njezino primanje osobnih informacija iz EU-a više ne primjenjuje Komisijina odluka o primjerenosti.

4. Ministarstvo trgovine vodit će i objavljivati obvezujuću evidenciju američkih organizacija koje su se prethodno samocertificirale tom ministarstvu, ali su uklonjene s popisa organizacija uključenih u okvir za privatnost podataka. Ministarstvo trgovine navest će jasno upozorenje da te organizacije ne sudjeluju u okviru EU-a i SAD-a za privatnost podataka, da uklanjanje s popisa organizacija uključenih u okvir za privatnost podataka znači da te organizacije ne mogu iznositi izjave o tome da su usklađene s okvirom EU-a i SAD-a za privatnost podataka i da moraju izbjegavati tvrdnje ili obmanjujuću praksu koje upućuju na to da sudjeluju u tom okviru te da se Komisijina odluka o primjerenosti više ne primjenjuje na primanje osobnih informacija iz EU-a takvih organizacija. Organizacija koja nastavi iznositi izjave o sudjelovanju u okviru EU-a i SAD-a za privatnost podataka ili iznosi druge lažne tvrdnje o tom okviru nakon što je uklonjena s popisa organizacija uključenih u okvir za privatnost podataka može biti predmet provedbenih mjera FTC-a, Ministarstva prometa ili drugih provedbenih tijela.

5. Pridržavanje tih načela može biti ograničeno: (a) na mjeru koja je nužna da se postupi u skladu sa sudskim nalogom ili ispune zahtjevi u pogledu javnog interesa, kaznenog progona ili nacionalne sigurnosti, među ostalim kad zbog zakona ili vladina propisa nastanu proturječne obveze, (b) zakonom, sudskim nalogom ili propisom vlade koji proizvode izričita dopuštenja, ako pri korištenju takvog dopuštenja organizacija može dokazati da je njezina neusklađenost s Načelima ograničena na mjeru potrebnu da se ostvare viši legitimni interesi za koje je predviđeno takvo dopuštenje, ili (c) ako su iznimke ili odstupanja dopušteni pod uvjetima utvrđenima u OUZP-u i ako se primjenjuju u sličnim kontekstima. Zaštitne mjere u pogledu privatnosti i građanskih sloboda u američkom pravu uključuju one koje se zahtijevaju Izvršnim nalogom br. 14086 ([4]) u skladu s uvjetima utvrđenima u tom nalogu (uključujući zahtjeve nužnosti i proporcionalnosti). U skladu s ciljem povećanja zaštite privatnosti organizacije trebaju nastojati u potpunosti i transparentno provoditi ova Načela, među ostalim tako da u svojim politikama zaštite privatnosti navode kad se primjenjuju iznimke od Načela dopuštene u prethodno opisanom slučaju (b). Iz istog se razloga, ako je mogućnost odabira dopuštena u skladu s Načelima i/ili američkim pravom, očekuje da organizacije kad je moguće odaberu višu razinu zaštite.

6. Nakon što organizacije postanu članice okvira EU-a i SAD-a za privatnost podataka, obvezne su primjenjivati Načela na sve osobne podatke prenesene u skladu s tim okvirom. Organizacija koja želi da se okvir EU-a i SAD-a za privatnost podataka primjenjuje i na osobne informacije o ljudskim resursima prenesene iz EU-a za uporabu u kontekstu radnog odnosa mora to navesti kad se samocertificira Ministarstvu trgovine i mora ispuniti zahtjeve iz dodatnog načela o samocertificiranju.

([4]) Izvršni nalog od 7. listopada 2022. o poboljšanju zaštitnih mjera u američkim aktivnostima elektroničkog izviđanja.

7. Američko pravo primjenjivat će se na pitanja tumačenja i usklađenosti s Načelima i relevantne politike zaštite privatnosti organizacija koje sudjeluju u okviru EU-a i SAD-a za privatnost podataka, osim ako su se organizacije obvezale na suradnju s tijelima za zaštitu podataka iz EU-a. Ako nije navedeno drukčije, sve odredbe Načela primjenjuju se kad su relevantne.

8. Definicije:

   a. „osobni podaci" i „osobne informacije" su podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi i koji su obuhvaćeni područjem primjene OUZP-a te koje je organizacija u SAD-u primila iz EU-a i koji su zabilježeni u bilo kojem obliku;

   b. „obrada" osobnih podataka znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima, bilo automatiziranim bilo neautomatiziranim sredstvima, kao što su prikupljanje, bilježenje, organizacija, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje ili širenje te brisanje ili uništavanje;

   c. „voditelj obrade" znači osoba ili organizacija koja sama ili zajedno s drugima utvrđuje svrhe i sredstva obrade osobnih podataka.

9. Datum stupanja na snagu Načela i Priloga I. Načelima datum je stupanja na snagu odluke Europske komisije o primjerenosti.

II. NAČELA

1. OBAVIJEST

a. Organizacija mora obavijestiti pojedince o sljedećem:

   i. da sudjeluje u okviru EU-a i SAD-a za privatnost podataka, uz navođenje poveznice koja vodi na popis organizacija uključenih u okvir za privatnost podataka ili internetsku adresu na kojoj se on nalazi;

   ii. vrstama osobnih podataka koje prikuplja i prema potrebi o subjektima ili podružnicama organizacije u SAD-u koji se isto tako pridržavaju Načela;

   iii. da se obvezala primjenjivati Načela pri obradi svih osobnih podataka koje primi od EU-a u skladu s okvirom EU-a i SAD-a za privatnost podataka;

   iv. svrhama u koje prikuplja njihove osobne informacije i za što ih upotrebljava;

   v. kako joj se obratiti s upitima ili pritužbama, među ostalim o relevantnom subjektu u EU-u koji može odgovoriti na te upite ili pritužbe;

   vi. vrsti ili identitetu trećih strana kojima otkriva osobne informacije te u koje svrhe to čini;

   vii. pravu pojedinaca da pristupe svojim osobnim podacima;

   viii. mogućnostima izbora i sredstvima za ograničavanje uporabe i otkrivanja njihovih osobnih podataka koje organizacija nudi pojedincima;

   ix. neovisnom tijelu za rješavanje sporova koje je imenovano za rješavanje pritužbi i davanje besplatnog pristupa prikladnoj pravnoj zaštiti pojedincu, uz navođenje je li riječ o: 1. odboru 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 SAD-u;

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

   xi. mogućnosti pojedinca da u određenim okolnostima zatraži obvezujuću arbitražu ([5]);

   xii. obvezi otkrivanja osobnih informacija u odgovoru na zakonite zahtjeve javnih tijela, među ostalim da bi se ispunili zahtjevi u pogledu nacionalne sigurnosti ili kaznenog progona; i

   xiii. svojoj odgovornosti u slučajevima daljnjih prijenosa trećim stranama.

([5]) Vidjeti npr. odjeljak (c) načela pravne zaštite, provedbe i odgovornosti.

b. Ta obavijest mora biti jasno i razumljivo navedena kad se od pojedinaca prvi put traži da dostave osobne informacije organizaciji ili što prije nakon toga, no u svakom slučaju prije nego što organizacija upotrijebi te informacije u neku drugu svrhu od one u koju ih je izvorno prikupila ili obradila organizacija koja je izvršila prijenos ili prije nego što ih se prvi put otkrije trećoj strani.

2. **IZBOR**

a. Organizacija mora pojedincima ponuditi mogućnost da odaberu hoće li se njihove osobne informacije i. otkriti trećoj strani ili ii. upotrijebiti u svrhu koja je bitno različita od svrha u koje su izvorno prikupljene ili za koju su pojedinci naknadno dali odobrenje, odnosno da traže izuzeće od navedenoga. Pojedincima moraju biti ponuđeni jasni, vidljivi i lako dostupni mehanizmi izbora.

b. Odstupajući od prethodnog stavka, nije nužno ponuditi izbor kad se podaci otkrivaju trećoj strani koja u ulozi posrednika izvršava zadaće u ime organizacije i prema njezinim uputama. Međutim, organizacija uvijek sklapa ugovor s posrednikom.

c. Za osjetljive informacije (tj. osobne informacije o medicinskom ili zdravstvenom stanju, rasi ili etničkom podrijetlu, političkim stavovima, vjerskim ili filozofskim uvjerenjima, članstvu u sindikatu ili informacije o spolnom životu pojedinca) organizacije moraju pribaviti izričitu suglasnost (pristanak) pojedinaca ako će se te informacije i. otkriti trećoj strani ili ii. upotrijebiti u neku drugu svrhu osim one u koju su izvorno prikupljene ili za koju su pojedinci naknadno dali odobrenje izabravši pristanak. Osim toga, organizacija treba smatrati osjetljivima osobne informacije koje je primila od treće strane ako ih treća strana smatra osjetljivima i odnosi se prema njima kao takvima.

3. **ODGOVORNOST ZA DALJNI PRIJENOS**

a. Da bi mogle prenijeti osobne informacije voditelju obrade koji je treća strana, organizacije moraju biti usklađene s načelima obavješćivanja i izbora. Organizacije osim toga moraju sklopiti ugovor s voditeljem obrade koji je treća strana, u kojem je propisano da se takvi podaci mogu obrađivati samo u ograničene i posebno navedene svrhe u skladu sa suglasnošću pojedinca, da će primatelj osigurati razinu zaštite jednaku onoj koja je osigurana Načelima i da će obavijestiti organizaciju ako utvrdi da više ne može ispunjavati tu obvezu. U ugovoru je predviđeno da, ako se to utvrdi, voditelj obrade koji je treća strana prestaje s obradom ili poduzima druge razumne i odgovarajuće korake za rješavanje te situacije.

b. Da bi mogle prenijeti osobne podatke posredniku koji je treća strana, organizacije moraju: i. prenositi takve podatke samo u ograničene i posebne svrhe, ii. utvrditi da posrednik ima obvezu pružiti razinu zaštite privatnosti najmanje jednaku onoj propisanoj Načelima, iii. poduzeti razumne i prikladne korake kako bi osigurale da posrednik stvarno obrađuje prenesene osobne informacije na način koji je u skladu s obvezama koje organizacija ima na temelju Načela, iv. zahtijevati da posrednik obavijesti organizaciju ako utvrdi da više ne može ispunjavati svoju obvezu pružanja razine zaštite jednake onoj propisanoj Načelima; v. na temelju obavijesti, uključujući onu navedenu u točki iv., poduzeti razumne i odgovarajuće korake da zaustavi i ispravi neovlaštenu obradu, i vi. Ministarstvu trgovine na zahtjev dostaviti sažetak ili reprezentativni primjerak relevantnih odredbi o zaštiti privatnosti iz svojeg ugovora s tim posrednikom.

4. **SIGURNOST**

a. Organizacije koje stvaraju, održavaju, upotrebljavaju ili šire osobne informacije moraju poduzeti razumne i odgovarajuće mjere kako bi ih zaštitile od gubitka, zlouporabe i neovlaštenog pristupa, otkrivanja, izmjene i uništenja, uzimajući u obzir rizike povezane s obradom i prirodu osobnih podataka.

5. **CJELOVITOST PODATAKA I OGRANIČENJE SVRHE**

a. U skladu s Načelima osobne informacije moraju biti ograničene na informacije koje su relevantne za svrhe obrade ([6]). Organizacija ne smije obrađivati osobne informacije na način koji nije u skladu sa svrhama u koje su izvorno prikupljene ili za koje je pojedinac naknadno dao odobrenje. Ako je to potrebno za te svrhe, organizacija mora poduzeti razumne korake da osobni podaci budu pouzdani za namjeravanu uporabu, točni, potpuni i ažurni. Organizacija se mora pridržavati Načela sve dok čuva takve informacije.

b. Informacije se mogu čuvati u obliku kojim se utvrđuje identitet pojedinca ili koji omogućuje utvrđivanje njegova identiteta ([7]) samo dok služe svrsi obrade u okviru značenja iz točke 5. podtočke (a). Ta obveza ne sprečava organizacije da obrađuju osobne informacije i dulje, odnosno onoliko dugo i u onoj mjeri u kojoj takva obrada razumno služi svrhama pohranjivanja u javnom interesu, novinarstva, književnosti i umjetnosti, povijesnih ili znanstvenih istraživanja te statističke analize. U tim slučajevima takva obrada podliježe ostalim načelima i odredbama okvira EU-a i SAD-a za privatnost podataka. Organizacije trebaju poduzeti razumne i odgovarajuće mjere za usklađivanje s tom odredbom.

6. **PRISTUP**

a. Pojedinci moraju imati pristup svojim osobnim informacijama koje organizacija čuva i moraju ih moći ispraviti, promijeniti ili izbrisati ako su netočne ili obrađene u suprotnosti s Načelima, osim ako bi teret ili trošak omogućivanja pristupa bio nerazmjeran rizicima za privatnost pojedinca u okolnostima slučaja ili ako bi bila povrijeđena prava drugih osoba.

7. **PRAVNA ZAŠTITA, PROVEDBA I ODGOVORNOST**

a. Učinkovita zaštita privatnosti mora uključivati pouzdane mehanizme kojima se osigurava usklađenost s Načelima, pravnu zaštitu za pojedince na koje utječe neusklađenost s Načelima i posljedice za organizaciju u slučaju neusklađenosti. Takvi mehanizmi moraju obuhvaćati barem sljedeće:

i. lako dostupne neovisne mehanizme pravne zaštite u okviru kojih se pritužbe i sporovi svakog pojedinca mogu istražiti i brzo riješiti bez naknade upućivanjem na Načela te odštetu koja se dodjeljuje ako je tako predviđeno primjenjivim pravom ili inicijativama iz privatnog sektora;

ii. postupke praćenja kojima se provjerava jesu li potvrde i navodi koje organizacije iznose o svojoj praksi zaštite privatnosti istinite i provodi li se ta praksa kako je navedeno, osobito u pogledu slučajeva neusklađenosti; i

iii. obveze rješavanja problema koji proizlaze iz činjenice da se organizacije ne pridržavaju Načela, iako navode suprotno, i posljedice za takve organizacije. Sankcije moraju biti dovoljno stroge da bi se osigurala usklađenost organizacija s Načelima.

b. Organizacije i njihovi odabrani neovisni mehanizmi pravne zaštite žurno će odgovarati na upite i zahtjeve za informacije povezane s okvirom EU-a i SAD-a za privatnost podataka koje im uputi Ministarstvo trgovine. Sve organizacije moraju žurno odgovarati na pritužbe u pogledu usklađenosti s Načelima koje su im uputila tijela država članica EU-a preko Ministarstva trgovine. Organizacije koje su odlučile surađivati s tijelima za zaštitu podataka, uključujući organizacije koje obrađuju podatke o ljudskim resursima, moraju izravno odgovoriti takvim tijelima u vezi s istragom i rješavanjem pritužbi.

([6]) Ovisno o okolnostima, primjeri usklađenih svrha obrade mogu uključivati obradu koja je u razumnoj mjeri usmjerena na odnose s potrošačima, usklađenost i pravne aspekte, reviziju, sigurnost i sprečavanje prijevare, očuvanje ili obranu zakonskih prava organizacije ili druge svrhe u skladu s očekivanjima razumne osobe s obzirom na kontekst prikupljanja podataka.

([7]) Ako u tom kontekstu i s obzirom na sredstva identificiranja za koja se može razumno očekivati da će se upotrijebiti (uzimajući u obzir, među ostalim, troškove i vrijeme potrebne za utvrđivanje identiteta te tehnologiju dostupnu u trenutku obrade) te oblik u kojem se čuvaju podaci, organizacija ili treća strana, ako ima pristup podacima, mogu u razumnoj mjeri identificirati pojedinca, tada se njegov „identitet može utvrditi”.

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

d. Organizacija uključena u okvir za privatnost podataka odgovorna je, u kontekstu daljnjeg prijenosa, za obradu osobnih informacija koje primi u skladu s okvirom EU-a i SAD-a za privatnost podataka i koje zatim prenese trećoj strani koja djeluje kao posrednik u njezino ime. Organizacija uključena u okvir za privatnost podataka snosi odgovornost u skladu s Načelima ako njezin posrednik obrađuje takve osobne informacije na način koji nije u skladu s Načelima, osim ako organizacija dokaže da nije odgovorna za događaj zbog kojeg je nastala šteta.

e. Kad organizacija zbog neusklađenosti postane predmet sudskog naloga ili naloga koji je izdalo američko zakonsko tijelo (npr. FTC ili Ministarstvo prometa) navedeno u Načelima ili u budućem prilogu Načelima, organizacija objavljuje sve relevantne dijelove povezane s okvirom EU-a i SAD-a za privatnost podataka iz svojeg izvješća o usklađenosti ili o ocjeni koje je dostavljeno sudu ili američkom zakonskom tijelu, u mjeri u kojoj je to u skladu sa zahtjevima u pogledu povjerljivosti. Ministarstvo trgovine uspostavilo je posebnu kontaktnu točku za tijela za zaštitu podataka u slučaju problema s usklađenošću organizacija uključenih u okvir za privatnost podataka. FTC i Ministarstvo prometa dat će prednost predmetima o neusklađenosti s Načelima koje su im uputili Ministarstvo trgovine i tijela država članica EU-a te će pravodobno razmijeniti informacije o upućenim predmetima s državnim tijelima koja su ih uputila, uz primjenu postojećih ograničenja u pogledu povjerljivosti.

III. DODATNA NAČELA

1. Osjetljivi podaci

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

i. od životno važnog interesa za ispitanika ili neku drugu osobu;

ii. potrebna za postavljanje pravnih zahtjeva ili obrane;

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

iv. provedena tijekom obavljanja legitimnih aktivnosti zaklade, udruge ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem i pod uvjetom da se obrada odnosi isključivo na članove tog tijela ili na osobe koje su u redovitom kontaktu s njim u vezi s tim svrhama te da se podaci ne otkrivaju trećoj strani bez suglasnosti ispitanika;

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

vi. povezana s podacima koje je očigledno objavio pojedinac.

2. Novinarska izuzeća

a. Budući da je sloboda tiska zaštićena američkim Ustavom, ako su prava na slobodu tiska iz prvog amandmana američkog Ustava u suprotnosti s interesima zaštite privatnosti, ravnoteža tih interesa kad je riječ o aktivnostima američkih državljana ili organizacija mora se uspostaviti na temelju prvog amandmana.

b. Osobne informacije koje se prikupljaju radi objavljivanja, emitiranja ili drugih oblika javnog priopćavanja novinarskih materijala, bez obzira na to upotrebljavaju li se, i informacije pronađene u prethodno objavljenom materijalu iz medijskih arhiva ne podliježu zahtjevima Načela.

3. Sekundarna odgovornost

a. Pružatelji internetskih usluga, telekomunikacijski operateri i ostale organizacije ne snose odgovornost u skladu s Načelima ako u ime neke druge organizacije samo prenose, usmjeravaju, prespajaju ili privremeno pohranjuju informacije. Okvirom EU-a i SAD-a za privatnost podataka ne stvara se sekundarna odgovornost. Organizacija koja djeluje samo kao posrednik za podatke koje prenose treće strane i ne određuje svrhu i sredstva obrade tih osobnih podataka ne snosi odgovornost.

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

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

b. Javna dionička društva i poduzeća s malim brojem dioničara, uključujući organizacije uključene u okvir za privatnost podataka, redovito podliježu reviziji. Takve revizije, posebno one kojima se istražuju moguće povrede, mogle bi se ugroziti preranom objavom. Slično tomu, organizacija uključena u okvir za privatnost podataka koja sudjeluje u mogućem spajanju ili preuzimanju morat će obaviti dubinsku analizu ili biti predmet dubinske analize. 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 čak povrijediti primjenjivi propisi o vrijednosnim papirima. Investicijski bankari i odvjetnici koji sudjeluju u dubinskoj analizi ili revizori koji provode reviziju mogu obrađivati informacije bez znanja pojedinca samo u onoj mjeri i onoliko dugo koliko je to potrebno da se zadovolje zahtjevi u pogledu zakona ili javnog interesa i u drugim okolnostima u kojima bi primjena ovih Načela naškodila legitimnim interesima organizacije. Ti legitimni interesi uključuju praćenje ispunjavaju li organizacije svoje zakonske obveze i legitimne računovodstvene aktivnosti te potrebu za tajnošću podataka povezanih s mogućim preuzimanjima, spajanjima, zajedničkim pothvatima ili drugim sličnim transakcijama koje obavljaju investicijski bankari ili revizori.

5. **Uloga tijela za zaštitu podataka**

a. Organizacije će ispunjavati svoju obvezu suradnje s tijelima za zaštitu podataka na način opisan u nastavku. U skladu s okvirom EU-a i SAD-a za privatnost podataka američke organizacije koje primaju osobne podatke iz EU-a moraju se obvezati na primjenu učinkovitih mehanizama kojima se osigurava usklađenost s Načelima. Točnije, kako je utvrđeno u načelu pravne zaštite, provedbe i odgovornosti, organizacije uključene u okvir za privatnost podataka moraju: (a) i. osigurati pravnu zaštitu pojedincima na koje se podaci odnose, (a) ii. uspostaviti postupke praćenja kojima se provjerava jesu li potvrde i navodi koje organizacije iznesu o svojim praksama zaštite privatnosti istinite, i (a) iii. uvesti obveze da se riješe problemi koji proizlaze iz neusklađenosti s Načelima te navesti posljedice za takve organizacije. Organizacija može ispuniti zahtjeve iz točke (a) podtočaka i. i iii. načela pravne zaštite, provedbe i odgovornosti ako ispuni ovdje navedene zahtjeve za suradnju s tijelima za zaštitu podataka.

b. Organizacija se obvezuje na suradnju s tijelima za zaštitu podataka tako da u svojoj prijavi za samocertificiranje za okvir EU-a i SAD-a za privatnost podataka upućenoj Ministarstvu trgovine (vidjeti dodatno načelo o samocertificiranju) izjavi:

i. da svojevoljno pristaje ispuniti zahtjeve iz točke (a) podtočaka i. i iii. načela pravne zaštite, provedbe i odgovornosti obvezujući se na suradnju s tijelima za zaštitu podataka;

ii. da će surađivati s tijelima za zaštitu podataka u istraživanju i rješavanju pritužbi podnesenih u skladu s Načelima; i

iii. da će postupiti u skladu sa savjetima tijela za zaštitu podataka ako ta tijela smatraju da organizacija treba poduzeti određenu radnju za usklađivanje s Načelima, uključujući korektivne ili kompenzacijske mjere u korist pojedinaca na koje utječe neusklađenost s Načelima, te da će tijelima za zaštitu podataka dostaviti pisanu potvrdu da je takva radnja poduzeta.

c. Rad odbora tijela za zaštitu podataka

i. Tijela za zaštitu podataka surađivat će pružanjem informacija i savjeta na sljedeći način:

1. savjeti tijela za zaštitu podataka dostavit će se preko neslužbenog odbora tijela za zaštitu podataka uspostavljenog na razini EU-a, koji će među ostalim pridonijeti usklađenom i dosljednom pristupu;

2. odbor će davati savjete predmetnim američkim organizacijama o neriješenim pritužbama pojedinaca na postupanje s osobnim informacijama koje su prenesene iz EU-a u skladu s okvirom EU-a i SAD-a za privatnost podataka. Tim će se savjetima nastojati osigurati pravilna primjena Načela i uključivat će sva pravna sredstva za dotične pojedince koja tijela za zaštitu podataka smatraju prikladnima;

3. odbor će davati te savjete u odgovoru na predmete koje su uputile predmetne organizacije i/ili pritužbe zaprimljene izravno od pojedinaca protiv organizacija koje su se obvezale surađivati s tijelima za zaštitu podataka za potrebe okvira EU-a i SAD-a za privatnost podataka, a ujedno će poticati takve pojedince i prema potrebi im pomagati da prvo iskoriste interne načine rješavanja pritužbi koje organizacija nudi;

4. savjeti će biti izdani tek nakon što su obje stranke u sporu imale razumnu mogućnost iznijeti primjedbe i dostaviti dokaze. Odbor će pokušati dati savjete čim to bude moguće u skladu s propisanim postupkom. Odbor će u pravilu nastojati dati savjete u roku od 60 dana od primitka pritužbe ili upućenog predmeta, a ako je moguće i brže;

5. odbor će objaviti rezultate svojeg razmatranja pritužbe koja mu je podnesena ako to smatra prikladnim;

6. davanje savjeta preko odbora ne znači da odbor ili pojedinačno tijelo za zaštitu podataka snosi ikakvu odgovornost.

ii. Kako je prethodno navedeno, organizacije koje odaberu tu mogućnost rješavanja sporova moraju se obvezati da će postupiti u skladu sa savjetom tijela za zaštitu podataka. Ako organizacija to ne učini u roku od 25 dana od primitka savjeta i ne ponudi prihvatljivo objašnjenje za kašnjenje, odbor će poslati obavijest o svojoj namjeri da proslijedi predmet FTC-u, Ministarstvu prometa ili drugom američkom saveznom ili državnom tijelu sa zakonskim ovlastima da poduzme provedbene mjere u slučajevima prijevare ili lažnog prikazivanja, ili da zaključi da je sporazum o suradnji ozbiljno prekršen i stoga se mora smatrati ništavim. U potonjem će slučaju odbor obavijestiti Ministarstvo trgovine kako bi se popis organizacija uključenih u okvir za privatnost podataka mogao prikladno ispraviti. Svako neispunjenje obveze suradnje s tijelima za zaštitu podataka, kao i neusklađenost s Načelima, bit će kažnjivo kao prijevarna praksa u skladu s člankom 5. Zakona o FTC-u (glava 15. članak 45. Zakonika SAD-a), glavom 49. člankom 41712. Zakonika SAD-a ili nekim sličnim propisom.

d. Organizacija koja želi da se okvir EU-a i SAD-a za privatnost podataka primjenjuje i na podatke o ljudskim resursima prenesene iz EU-a u kontekstu radnog odnosa mora se obvezati na suradnju s tijelima za zaštitu podataka u pogledu tih podataka (vidjeti dodatno načelo o podacima o ljudskim resursima).

e. Organizacije koje odaberu tu mogućnost morat će platiti godišnju naknadu koja će biti namijenjena za pokrivanje operativnih troškova odbora. Može se dodatno zatražiti i da te organizacije podmire potrebne troškove prevođenja koji nastaju kad članovi odbora razmatraju upućene predmete ili pritužbe protiv njih. Iznos naknade utvrdit će Ministarstvo trgovine nakon dogovora s Komisijom. Naknadu može prikupljati treća strana koju Ministarstvo trgovine odabere za čuvara sredstava prikupljenih u tu svrhu. Ministarstvo trgovine blisko će surađivati s Komisijom i tijelima za zaštitu podataka na uspostavljanju prikladnih postupaka za raspodjelu sredstava prikupljenih plaćanjem naknade te na drugim postupovnim i administrativnim aspektima odbora. Ministarstvo trgovine i Komisija mogu se dogovoriti o izmjeni učestalosti prikupljanja naknade.

6. **Samocertificiranje**

a. Okvir EU-a i SAD-a za privatnost podataka primjenjuje se od datuma kad Ministarstvo trgovine uvrsti organizaciju na popis organizacija uključenih u okvir za privatnost podataka. Ministarstvo trgovine to će učiniti tek kad utvrdi da je izvorna prijava organizacije za samocertificiranje potpuna, a uklonit će organizaciju s tog popisa ako se dobrovoljno povuče ili ne ispuni obvezu godišnjeg ponovnog certificiranja, kao i u slučaju njezine ustrajne neusklađenosti s Načelima (vidjeti dodatno načelo o rješavanju sporova i provedbi).

b. Da bi se mogla samocertificirati ili naknadno ponovno certificirati za okvir EU-a i SAD-a za privatnost podataka, organizacija svaki put mora Ministarstvu trgovine dostaviti prijavu nadležnog službenika u ime organizacije koja se samocertificira ili ponovno certificira (prema potrebi) za pridržavanje Načela ([8]), a ta prijava sadržava najmanje sljedeće informacije:

([8]) Prijavu mora dostaviti pojedinac u organizaciji ovlašten za podnošenje očitovanja o pridržavanju Načela u ime organizacije i obuhvaćenih subjekata na internetskim stranicama Ministarstva trgovine za okvir za privatnost podataka.

i. ime američke organizacije koja se samocertificira ili ponovno certificira, kao i imena svih njezinih subjekata ili podružnica u SAD-u koji se isto tako pridržavaju Načela i koje organizacija želi uključiti;

ii. opis aktivnosti organizacije u pogledu osobnih informacija koje će primati iz EU-a u skladu s okvirom EU-a i SAD-a za privatnost podataka;

iii. opis njezinih relevantnih politika zaštite privatnosti takvih osobnih informacija, uključujući:

1. ako organizacija ima javne internetske stranice, relevantnu internetsku adresu na kojoj je dostupna politika zaštite privatnosti, a ako nema, internetsku adresu na kojoj se može pregledati politika zaštite privatnosti; i

2. datum od kojeg se provodi;

iv. kontaktni ured u organizaciji za rješavanje pritužbi, zahtjeva za pristup i svih ostalih pitanja povezanih s Načelima ([9]), uključujući:

1. ime, naziv radnog mjesta (prema potrebi), e-adresu i broj telefona relevantnih pojedinaca ili kontaktnih ureda u organizaciji; i

2. relevantnu poštansku adresu organizacije u SAD-u;

v. posebno zakonsko tijelo koje je nadležno rješavati pritužbe protiv organizacije u pogledu moguće nepoštene ili prijevarne prakse i povreda zakona ili propisa kojima se uređuje zaštita privatnosti (i koje je navedeno u Načelima ili budućem prilogu Načelima);

vi. naziv programa za zaštitu privatnosti u kojima organizacija sudjeluje kao članica;

vii. metodu provjere (tj. samoprocjena ili vanjsko preispitivanje usklađenosti, uključujući informacije o trećoj strani koja provodi ta preispitivanja) ([10]); i

viii. relevantne neovisne mehanizme pravne zaštite koji su dostupni za istragu neriješenih pritužbi koje se odnose na Načela ([11]).

c. Ako organizacija želi da se okvir EU-a i SAD-a za privatnost podataka primjenjuje i na informacije o ljudskim resursima prenesene iz EU-a za uporabu u kontekstu radnog odnosa, može to 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 izvornoj prijavi za samocertificiranje i u eventualnim prijavama za ponovno certificiranje, te mora izjaviti da se obvezuje na suradnju s tijelima EU-a u skladu s dodatnim načelima o podacima o ljudskim resursima i ulozi tijela za zaštitu podataka (prema potrebi) i da će postupati u skladu sa savjetima takvih tijela. Organizacija Ministarstvu trgovine mora dostaviti i presliku svoje politike zaštite privatnosti podataka o ljudskim resursima i navesti gdje obuhvaćeni zaposlenici mogu pročitati tu politiku.

([9]) Primarni „kontakt u organizaciji" ili „nadležni službenik organizacije" ne može biti vanjski suradnik organizacije (npr. vanjski pravni zastupnik ili vanjski savjetnik).

([10]) Vidjeti dodatno načelo o provjeri.

([11]) Vidjeti dodatno načelo o rješavanju sporova i provedbi.

d. Ministarstvo trgovine vodit će i objavljivati popis organizacija uključenih u okvir za privatnost podataka koje su dostavile potpune izvorne prijave za samocertificiranje i ažurirat će taj popis na temelju potpunih godišnjih prijava za ponovno certificiranje te na temelju obavijesti zaprimljenih u skladu s dodatnim načelom o rješavanju sporova i provedbi. Takve prijave za samocertificiranje moraju se dostaviti najmanje jednom godišnje, u suprotnom se organizacija uklanja s popisa organizacija uključenih u okvir za privatnost podataka i okvir EU-a i SAD-a za privatnost podataka više se neće primjenjivati na nju. Sve organizacije koje Ministarstvo trgovine uvrsti na popis organizacija uključenih u okvir za privatnost podataka moraju imati relevantne politike zaštite privatnosti koje su usklađene s načelom obavješćivanja i u tim politikama moraju navesti da se pridržavaju Načela ([12]). Ako je politika zaštite privatnosti određene organizacije dostupna na internetu, mora uključivati poveznicu na internetske stranice Ministarstva trgovine za okvir za privatnost podataka i poveznicu na internetske stranice ili obrazac za podnošenje pritužbi neovisnog mehanizma pravne zaštite koji je pojedincu dostupan besplatno za rješavanje neriješenih pritužbi koje se odnose na Načela.

e. Načela se primjenjuju odmah nakon samocertificiranja. Organizacije uključene u okvir za privatnost podataka koje su se prethodno samocertificirale za usklađenost s Načelima okvira europsko-američkog sustava zaštite privatnosti morat će ažurirati svoje politike zaštite privatnosti kako bi se u njima umjesto toga upućivalo na „Načela okvira EU-a i SAD-a za privatnost podataka”. Organizacije to moraju učiniti što prije, a u svakom slučaju najkasnije tri mjeseca nakon datuma stupanja na snagu Načela okvira EU-a i SAD-a za privatnost podataka.

f. Organizacija mora primjenjivati Načela pri obradi svih osobnih podataka koje primi od EU-a u skladu s okvirom EU-a i SAD-a za privatnost podataka. Preuzeta obveza pridržavanja Načela nije vremenski ograničena u odnosu na osobne podatke zaprimljene u razdoblju u kojem se na organizaciju primjenjuje okvir EU-a i SAD-a za privatnost podataka, nego ta obveza znači da će organizacija nastaviti primjenjivati Načela na takve podatke sve dok ih pohranjuje, upotrebljava ili otkriva, čak i ako poslije iz bilo kojeg razloga napusti okvir EU-a i SAD-a za privatnost podataka. Organizacija koja se želi povući iz okvira EU-a i SAD-a za privatnost podataka mora o tome unaprijed obavijestiti Ministarstvo trgovine. U toj obavijesti mora biti navedeno i što će učiniti s osobnim podacima koje je primila u skladu s okvirom EU-a i SAD-a za privatnost podataka (tj. hoće li zadržati, vratiti ili izbrisati podatke i, ako će ih zadržati, odobrena sredstva kojima će ih zaštititi). Organizacija koja se povuče iz okvira EU-a i SAD-a za privatnost podataka, ali želi zadržati te podatke, mora svake godine potvrditi Ministarstvu trgovine da se obvezuje i dalje primjenjivati Načela na podatke ili osigurati njihovu „primjerenu” zaštitu drugim odobrenim sredstvima (npr. ugovorom koji je u potpunosti u skladu sa zahtjevima relevantnih standardnih ugovornih odredbi koje je odobrila Komisija), u protivnom ih mora vratiti ili izbrisati ([13]). Organizacija koja se povuče iz okvira EU-a i SAD-a za privatnost podataka mora iz relevantnih politika zaštite privatnosti ukloniti sva upućivanja na taj okvir iz kojih bi se moglo zaključiti da i dalje sudjeluje u njemu i da ima pravo na pogodnosti koje iz njega proizlaze.

([12]) Organizacija koja se prvi put samocertificira ne može u svojoj konačnoj politici zaštite privatnosti iznositi izjave o tome da sudjeluje u okviru EU-a i SAD-a za privatnost podataka dok je Ministarstvo trgovine ne obavijesti da to može učiniti. Organizacija pri podnošenju izvorne izjave o samocertificiranju Ministarstvu trgovine mora dostaviti nacrt svoje politike zaštite privatnosti, koja mora biti usklađena s Načelima. Kad Ministarstvo trgovine utvrdi da je izvorna prijava za samocertificiranje organizacije u ostalim segmentima potpuna, obavijestit će je da bi trebala dovršiti (npr. prema potrebi objaviti) svoju politiku zaštite privatnosti usklađenu s okvirom EU-a i SAD-a za privatnost podataka. Organizacija mora obavijestiti Ministarstvo trgovine čim dovrši relevantnu politiku zaštite privatnosti, nakon čega će je to ministarstvo uvrstiti na popis organizacija uključenih u okvir za privatnost podataka.

([13]) Ako organizacija u vrijeme povlačenja odabere da će zadržati osobne podatke koje je primila u skladu s okvirom EU-a i SAD-a za privatnost podataka i svake godine potvrđivati Ministarstvu trgovine da i dalje primjenjuje Načela na takve podatke, jednom godišnje nakon povlačenja (tj. osim ako i sve dok ne osigura „primjerenu” zaštitu tih podataka drugim odobrenim sredstvima ili vrati ili izbriše sve takve podatke te obavijesti Ministarstvo trgovine o tome) mora tom ministarstvu potvrditi što je učinila s osobnim podacima, što će učiniti s onima koje je zadržala i tko će biti stalna kontaktna točka za pitanja koja se odnose na Načela.

g. Organizacija koja prestane postojati kao zasebna pravna osoba zbog statusne promjene društva, primjerice zbog spajanja, preuzimanja, stečaja ili prestanka, mora unaprijed o tome obavijestiti Ministarstvo trgovine. U obavijesti bi trebalo navesti i hoće li subjekt koji je nastao statusnom promjenom društva i. nastaviti sudjelovati u okviru EU-a i SAD-a za privatnost podataka na temelju postojećeg samocertificiranja, ii. provesti samocertificiranje kao novi sudionik okvira EU-a i SAD-a za privatnost podataka (npr. ako novi subjekt ili subjekt koji nastavlja postojati već nije proveo samocertificiranje na temelju kojeg bi mogao sudjelovati u okviru EU-a i SAD-a za privatnost podataka), ili iii. uspostaviti druge zaštitne mjere, kao što je pisani sporazum kojim će se osigurati daljnja primjena Načela na sve osobne podatke koje je organizacija primila u skladu s okvirom EU-a i SAD-a za privatnost podataka i koje će zadržati. Ako ništa od navedenog nije primjenjivo, svi osobni podaci zaprimljeni u skladu s okvirom EU-a i SAD-a za privatnost podataka moraju se odmah vratiti ili izbrisati.

h. Ako organizacija napusti okvir EU-a i SAD-a za privatnost podataka iz bilo kojeg razloga, mora ukloniti sve izjave iz kojih bi se moglo zaključiti da i dalje sudjeluje u tom okviru ili da ima pravo na pogodnosti koje iz njega proizlaze. Ako se upotrebljava certifikacijska oznaka okvira EU-a i SAD-a za privatnost podataka, i ona se mora ukloniti. FTC, Ministarstvo prometa ili drugo relevantno vladino tijelo može pokrenuti sudski postupak u slučaju lažnog prikazivanja da se organizacija pridržava Načela. Lažno prikazivanje Ministarstvu trgovine kažnjivo je u skladu sa Zakonom o davanju lažnog iskaza (*False Statements Act*, glava 18. članak 1001. Zakonika SAD-a).

7. **Provjera**

a. Organizacije moraju uspostaviti postupke praćenja kojima se provjerava jesu li potvrde i navodi koje iznose o svojoj praksi zaštite privatnosti u skladu s okvirom EU-a i SAD-a za privatnost podataka istiniti te provodi li se ta praksa na način na koji organizacije tvrde i u skladu s Načelima.

b. Kako bi ispunila zahtjeve za provjeru iz načela pravne zaštite, provedbe i odgovornosti, organizacija mora provjeriti takve potvrde i navode samoprocjenom ili vanjskim preispitivanjima usklađenosti.

c. Ako organizacija odabere samoprocjenu, takvom se provjerom mora dokazati da je njezina politika zaštite privatnosti osobnih informacija zaprimljenih iz EU-a točna, sveobuhvatna, lako dostupna, usklađena s Načelima i u potpunosti provedena (tj. da se postupa u skladu s njom). Mora se pokazati i da su pojedinci obaviješteni o eventualnim unutarnjim mehanizmima organizacije za rješavanje pritužbi i o neovisnim mehanizmima pravne zaštite u okviru kojih mogu podnositi pritužbe; da je organizacija uvela postupke za osposobljavanje zaposlenika za primjenu te politike i disciplinske mjere za njezino neprovođenje te da je uvela interne postupke za periodičnu provedbu objektivnih preispitivanja usklađenosti s navedenim zahtjevima. Izjavu kojom se potvrđuje da je samoprocjena dovršena mora potpisati rukovoditelj ili drugi ovlašteni predstavnik organizacije barem jednom godišnje i dostaviti je pojedincima na njihov zahtjev ili u kontekstu istrage ili pritužbe zbog neusklađenosti.

d. Ako organizacija odabere vanjsko preispitivanje usklađenosti, takvom se provjerom mora dokazati da je njezina politika zaštite privatnosti osobnih informacija zaprimljenih iz EU-a točna, sveobuhvatna, lako dostupna, usklađena s Načelima i u potpunosti provedena (tj. da se postupa u skladu s njom). Mora se pokazati i da su pojedinci obaviješteni o mehanizmima u okviru kojih mogu podnositi pritužbe. Metode preispitivanja mogu bez ograničenja uključivati reviziju, nasumične provjere te uporabu „mamaca” ili prema potrebi tehnoloških sredstava. Izjavu kojom se potvrđuje da je vanjsko preispitivanje usklađenosti uspješno završeno treba potpisati voditelj preispitivanja, nadležni službenik ili neki drugi ovlašteni predstavnik organizacije najmanje jednom godišnje i dostaviti je pojedincima na njihov zahtjev ili u kontekstu istrage ili pritužbe zbog neusklađenosti.

e. Organizacije moraju čuvati evidencije o provedbi svoje prakse zaštite privatnosti u sklopu okvira EU-a i SAD-a za privatnost podataka i dostaviti ih na zahtjev u kontekstu istrage ili pritužbe zbog neusklađenosti neovisnom tijelu za rješavanje sporova odgovornom za istraživanje pritužbi ili agenciji koja je nadležna za nepoštenu i prijevarnu praksu. Organizacije isto tako moraju bez odlaganja odgovoriti na upite i druge zahtjeve Ministarstva trgovine za informacije povezane s njihovim pridržavanjem Načela.

8. **Pristup**

a. Načelo pristupa u praksi

i. U skladu s Načelima pravo pristupa od temeljne je važnosti za zaštitu privatnosti. Ono u prvom redu omogućuje pojedincima da provjere točnost informacija koje se čuvaju o njima. Načelo pristupa znači da pojedinci imaju pravo:

1. na to da od organizacije dobiju potvrdu o tome obrađuje li ona osobne podatke koji se odnose na njih ([14]);

2. na to da im se ti podaci priopće kako bi mogli provjeriti njihovu točnost i zakonitost obrade; i

3. na ispravljanje, mijenjanje ili brisanje netočnih podataka ili podataka koji se obrađuju u suprotnosti s Načelima.

ii. Pojedinci ne moraju obrazlagati zahtjeve za pristup svojim osobnim podacima. Kad odgovaraju na zahtjeve pojedinaca za pristup, organizacije bi se prvenstveno trebale voditi pitanjima zbog kojih su zahtjevi uopće podneseni. Na primjer, ako je zahtjev za pristup nejasan ili preširok, organizacija može razgovarati s pojedincem kako bi bolje razumjela motive za zahtjev i dala povratnu informaciju. Organizacija može pitati pojedinca s kojim je njezinim dijelovima kontaktirao i/ili za koju vrstu informacija traži pristup te za što će ih upotrebljavati.

iii. U skladu s osnovnom prirodom pristupa, organizacije bi uvijek trebale u dobroj vjeri nastojati omogućiti pristup. Na primjer, ako određene informacije treba zaštititi, a mogu se lako izdvojiti od ostalih osobnih informacija za koje se traži pristup, organizacija bi trebala ispustiti zaštićene informacije i otkriti ostale informacije. Ako organizacija utvrdi da treba uskratiti pristup u nekom određenom slučaju, trebala bi pojedincu koji traži pristup objasniti zašto je to utvrdila i uputiti ga na kontaktnu točku za sve daljnje upite.

b. Teret ili trošak omogućivanja pristupa

i. Pravo pristupa osobnim podacima može biti ograničeno u iznimnim okolnostima ako bi bila povrijeđena legitimna prava drugih osoba ili ako bi teret ili trošak omogućivanja pristupa bio nerazmjeran rizicima za privatnost pojedinca u okolnostima slučaja. Trošak i teret važni su čimbenici i trebali bi se uzeti u obzir, ali nisu presudni u odlučivanju o tome je li omogućivanje pristupa razumno.

ii. Na primjer, ako se osobne informacije upotrebljavaju za odluke koje će znatno utjecati na pojedinca (npr. uskraćenje ili odobrenje važnih pogodnosti, kao što su osiguranje, hipoteka ili posao), u skladu s ostalim odredbama ovih Dodatnih načela organizacija bi morala otkriti informacije čak i ako ih je relativno teško ili skupo pružiti. Ako tražene osobne informacije nisu osjetljive ili se ne upotrebljavaju za odluke koje će znatno utjecati na pojedinca, nego su lako dostupne i nije ih skupo pružiti, organizacija će morati omogućiti pristup tim informacijama.

c. Povjerljive poslovne informacije

i. Povjerljive poslovne informacije informacije su koje je organizacija zaštitila od otkrivanja jer bi se njihovim otkrivanjem pomoglo konkurentu na tržištu. Organizacije mogu uskratiti ili ograničiti pristup ako bi se odobravanjem potpunog pristupa razotkrile njihove povjerljive poslovne informacije, kao što su zaključci povezani s tržištem ili klasifikacije koje je uspostavila organizacija, ili tuđe povjerljive poslovne informacije koje podliježu ugovornoj obvezi o povjerljivosti.

([14]) Organizacija bi trebala odgovoriti na zahtjeve pojedinca u pogledu svrha obrade, kategorija predmetnih osobnih podataka i primatelja ili kategorija primatelja kojima se otkrivaju osobni podaci.

ii. Ako se povjerljive poslovne informacije mogu lako izdvojiti od ostalih osobnih informacija za koje se traži pristup, organizacija bi trebala ispustiti povjerljive poslovne informacije i otkriti informacije koje nisu povjerljive.

d. Organizacija baza podataka

i. Pristup se može omogućiti na način da organizacija otkrije pojedincu relevantne osobne informacije, za što pojedinac ne mora pristupiti njezinoj bazi podataka.

ii. Pristup treba omogućiti samo ako organizacija pohranjuje osobne informacije. Načelo pristupa samo po sebi ne stvara obvezu zadržavanja, održavanja, reorganiziranja ili restrukturiranja datoteka s osobnim informacijama.

e. Kad pristup može biti ograničen

i. Budući da organizacije uvijek moraju u dobroj vjeri nastojati pojedincima omogućiti pristup njihovim osobnim podacima, ograničene su okolnosti u kojima organizacije mogu ograničiti taj pristup i moraju postojati konkretni razlozi za ograničavanje pristupa. Kako je propisano OUZP-om, organizacija može ograničiti pristup informacijama ako je vjerojatno da će otkrivanje narušiti zaštitu bitnih prevladavajućih javnih interesa, kao što su nacionalna sigurnost, obrana ili javna sigurnost. Osim toga, pristup se može uskratiti ako se osobne informacije obrađuju isključivo u istraživačke ili statističke svrhe. Ostali su razlozi za uskraćivanje ili ograničavanje pristupa:

1. ometanje izvršenja ili provedbe zakona ili tužbe podignute iz privatnih razloga, uključujući sprečavanje, istraživanje ili otkrivanje kaznenih djela ili pravo na pošteno suđenje;

2. otkrivanje podataka kojim bi se povrijedila legitimna prava ili važni interesi drugih osoba;

3. povreda obveze čuvanja pravne ili druge profesionalne tajne ili obveze;

4. ugrožavanje sigurnosnih istraga zaposlenika ili žalbenih postupaka ili postupaka povezanih s planiranjem zamjene zaposlenika odnosno reorganizacije poduzeća; ili

5. narušavanje tajnosti koja je nužna za praćenje, inspekciju ili regulatorne zadaće povezane s dobrim upravljanjem odnosno za buduće ili aktualne pregovore u kojima organizacija sudjeluje.

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

f. Pravo na dobivanje potvrde i naplaćivanje naknade za pokrivanje troškova omogućivanja pristupa

i. Pojedinac ima pravo dobiti potvrdu o tome posjeduje li određena organizacija osobne podatke koji se odnose na njega. Ima pravo i na to da mu se priopće osobni podaci koji se odnose na njega. Organizacija smije naplatiti naknadu koja nije pretjerana.

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

iii. Pristup se ne može uskratiti zbog troška ako pojedinac ponudi da će pokriti troškove.

g. Opetovani ili zlonamjerni zahtjevi za pristup

i. Organizacija može u razumnoj mjeri ograničiti broj zahtjeva za pristup istog pojedinca kojima će udovoljiti u određenom razdoblju. Pri određivanju takvih ograničenja trebala bi uzeti u obzir čimbenike kao što su učestalost ažuriranja informacija, svrha uporabe podataka i priroda informacija.

h. Lažni zahtjevi za pristup

i. Organizacija ne mora omogućiti pristup ako nema dovoljno informacija na temelju kojih može provjeriti identitet osobe koja podnosi zahtjev.

i. Rokovi za odgovore

i. Organizacije bi trebale odgovoriti na zahtjeve za pristup u razumnom roku, na razuman način i u obliku koji pojedinac razumije. Organizacija koja ispitanicima redovito pruža informacije može udovoljiti pojedinačnom zahtjevu za pristup redovitim otkrivanjem tih informacija ako to ne bi dovelo do pretjeranog kašnjenja.

9. **Podaci o ljudskim resursima**

a. Obuhvaćenost okvirom EU-a i SAD-a za privatnost podataka

i. Ako organizacija u EU-u prenosi osobne informacije o svojim (bivšim ili sadašnjim) zaposlenicima prikupljene u kontekstu radnog odnosa matičnom, povezanom ili nepovezanom pružatelju usluga u SAD-u koji sudjeluje u okviru EU-a i SAD-a za privatnost podataka, taj se okvir primjenjuje na prijenos. Prikupljanje informacija i njihova obrada prije prijenosa u takvim slučajevima podliježu nacionalnim zakonima države članice EU-a u kojoj su prikupljene i moraju se poštovati svi uvjeti ili ograničenja njihova prijenosa u skladu s tim zakonima.

ii. Načela su relevantna samo ako se prenose evidencije u kojima je identitet pojedinca utvrđen ili se može utvrditi ili ako se pristupa tim evidencijama. Statističko izvješćivanje utemeljeno na agregiranim podacima o zaposlenima, pri kojem se ne navode osobni podaci niti se upotrebljavaju anonimizirani podaci, ne ugrožava privatnost.

b. Primjena načela obavješćivanja i izbora

i. Američka organizacija koja je primila informacije o zaposlenicima iz EU-a u skladu s okvirom EU-a i SAD-a za privatnost podataka može ih otkriti trećim stranama ili upotrijebiti u druge svrhe samo u skladu s načelima obavješćivanja i izbora. Na primjer, ako organizacija namjerava upotrebljavati osobne informacije prikupljene tijekom radnog odnosa u svrhe koje nisu povezane s radnim odnosom, kao što su promidžbeni sadržaji, američka organizacija mora pojedincima na koje se podaci odnose ponuditi izbor prije nego što to učini, osim ako su oni već odobrili uporabu informacija u takve svrhe. Takva uporaba ne smije biti u suprotnosti sa svrhom u koju su osobne informacije prikupljene ili za koju je pojedinac naknadno dao odobrenje. Nadalje, takve se mogućnosti izbora ne smiju upotrebljavati za ograničavanje prilika za zapošljavanje ili poduzimanje kaznenih mjera protiv tih zaposlenika.

ii. Treba napomenuti da određeni općenito primjenjivi uvjeti za prijenos iz nekih država članica EU-a mogu isključivati druge vrste uporabe tih informacija čak i nakon prijenosa izvan EU-a, i ti se uvjeti moraju poštovati.

iii. Osim toga, poslodavci bi trebali u razumnoj mjeri poštovati želje zaposlenika u pogledu privatnosti. To na primjer može uključivati ograničavanje pristupa osobnim podacima, anonimizaciju određenih podataka ili dodjeljivanje šifri ili pseudonima kad stvarna imena nisu potrebna za postojeću svrhu upravljanja.

iv. U onoj mjeri i u onom razdoblju koji su potrebni da se ne dovede u pitanje njezina sposobnost za donošenje odluka o unapređenjima, imenovanjima i sličnih odluka o zaposlenju, organizacija ne mora nuditi obavješćivanje i mogućnost izbora.

c. Primjena načela pristupa

i. Dodatno načelo o pristupu sadržava smjernice o razlozima zbog kojih može biti opravdano uskratiti ili ograničiti zahtjev za pristup u kontekstu ljudskih resursa. Naravno, poslodavci u EU-u moraju poštovati lokalne propise i pobrinuti se za to da zaposlenici iz EU-a imaju pristup tim informacijama u skladu s pravom njihove matične zemlje, neovisno o mjestu obrade i pohrane podataka. Okvirom EU-a i SAD-a za privatnost podataka zahtijeva se da organizacija koja obrađuje takve podatke u SAD-u izravno ili preko poslodavca iz EU-a surađuje u omogućivanju pristupa.

d. Provedba

i. Ako se osobne informacije upotrebljavaju samo u kontekstu radnog odnosa, glavnu odgovornost za podatke u odnosu na zaposlenika snosi organizacija u EU-u. Iz toga proizlazi da europske zaposlenike koji podnose pritužbe o povredama svojih prava na zaštitu podataka i nisu zadovoljni rezultatima internih postupaka preispitivanja, pritužbi i žalbi (ili nekog žalbenog postupka koji se primjenjuje na temelju ugovora sa sindikatom) treba uputiti državnom ili nacionalnom tijelu za zaštitu podataka ili tijelu za radno pravo nadležnom za područje u kojem zaposlenici rade. To uključuje slučajeve kad je za navodno nepravilno postupanje s njihovim osobnim informacijama odgovorna američka organizacija koja je primila informacije od poslodavca i stoga je riječ o navodnoj povredi Načela. To će biti najučinkovitiji način da se uzmu u obzir prava i obveze propisani lokalnim radnim pravom i kolektivnim ugovorima te pravom o zaštiti podataka, koji se često preklapaju.

ii. Američka organizacija koja sudjeluje u okviru EU-a i SAD-a za privatnost podataka i upotrebljava podatke o ljudskim resursima iz EU-a prenesene iz EU-a u kontekstu radnog odnosa, a želi da takvi prijenosi budu obuhvaćeni tim okvirom, mora se obvezati na suradnju u istragama i postupanje u skladu sa savjetima nadležnih tijela EU-a u takvim slučajevima.

e. Primjena načela odgovornosti za daljnji prijenos

i. U slučaju da organizacija uključena u okvir za privatnost podataka ima povremene operativne potrebe povezane s radnim odnosom za osobnim podacima prenesenima u skladu s okvirom EU-a i SAD-a za privatnost podataka, kao što su rezervacija leta, hotelske sobe ili ugovaranje osiguranja, osobni podaci manjeg broja zaposlenika mogu se prenijeti voditeljima obrade bez primjene načela pristupa ili sklapanja ugovora s voditeljem obrade koji je treća strana, kako je propisano u skladu s načelom odgovornosti za daljnji prijenos, pod uvjetom da organizacija uključena u okvir za privatnost podataka postupa u skladu s načelima obavješćivanja i izbora.

10. **Obvezni ugovori za daljnje prijenose**

a. Ugovori o obradi podataka

i. Kad se osobni podaci iz EU-a prenose u SAD samo u svrhe obrade, bit će potreban ugovor neovisno o tome sudjeluje li izvršitelj obrade u okviru EU-a i SAD-a za privatnost podataka.

ii. Voditelji obrade podataka u EU-u uvijek su obvezni sklopiti ugovor kad se podaci prenose samo u svrhu obrade, neovisno o tome hoće li se obrada provesti unutar ili izvan EU-a i sudjeluje li izvršitelj obrade u okviru EU-a i SAD-a za privatnost podataka. Svrha je ugovora osigurati da izvršitelj obrade:

1. postupa samo prema uputama voditelja obrade;

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

3. uzimajući u obzir prirodu obrade, pomaže voditelju obrade da odgovori pojedincima koji ostvaruju svoja prava u skladu s Načelima.

iii. Budući da organizacije uključene u okvir za privatnost podataka pružaju primjerenu zaštitu, za ugovore s takvim organizacijama samo u svrhe obrade nije potrebno prethodno odobrenje.

b. Prijenosi unutar kontrolirane grupe poduzeća ili subjekata

i. Ako se osobne informacije prenose između dvaju voditelja obrade u kontroliranoj grupi poduzeća ili subjekata, u skladu s načelom odgovornosti za daljnji prijenos nije uvijek potreban ugovor. Voditelji obrade podataka u kontroliranoj grupi poduzeća ili subjekata mogu takve prijenose utemeljiti na drugim instrumentima, kao što su obvezujuća korporativna pravila EU-a ili drugi instrumenti unutar grupe (npr. programi usklađenosti i kontrole) kojima se osigurava kontinuitet zaštite osobnih informacija u skladu s Načelima. U slučaju takvih prijenosa organizacija uključena u okvir za privatnost podataka odgovorna je za usklađenost s Načelima.

c. Prijenosi između voditelja obrade

i. U slučaju prijenosa između voditelja obrade, voditelj obrade koji je primatelj ne mora biti organizacija uključena u okvir za privatnost podataka ni imati neovisan mehanizam pravne zaštite. Organizacija uključena u okvir za privatnost podataka mora sklopiti ugovor s voditeljem obrade koji je treća strana i primatelj i tim se ugovorom mora osigurati razina zaštite jednaka onoj koja je dostupna u skladu s okvirom EU-a i SAD-a za privatnost podataka, a ugovor ne treba uključivati zahtjev da voditelj obrade koji je treća strana mora biti organizacija uključena u okvir za privatnost podataka ili imati neovisan sustav pravne zaštite ako je dostupan istovjetni mehanizam.

11. **Rješavanje sporova i provedba**

a. Načelom pravne zaštite, provedbe i odgovornosti utvrđuju se zahtjevi za provedbu okvira EU-a i SAD-a za privatnost podataka. Načini ispunjenja zahtjeva iz točke (a) podtočke ii. Načela utvrđeni su u dodatnom načelu o provjeri. Ovo 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 mogu ispuniti te zahtjeve na sljedeće načine: i. usklađivanjem s programima zaštite privatnosti razvijenima u privatnom sektoru u čija su pravila ugrađena Načela i koji uključuju učinkovite mehanizme provedbe opisane u načelu pravne zaštite, provedbe i odgovornosti, ii. usklađivanjem sa zakonskim ili regulatornim nadzornim tijelima koja rješavaju pojedinačne pritužbe i sporove, ili iii. obvezivanjem na suradnju s tijelima za zaštitu podataka iz EU-a ili s njihovim ovlaštenim predstavnicima.

b. Ovaj bi popis trebao biti ogledan, a ne ograničavajući. Subjekti iz privatnog sektora mogu osmisliti dodatne mehanizme provedbe ako zadovoljavaju zahtjeve načela pravne zaštite, provedbe i odgovornosti i Dodatna načela. Treba imati na umu da su zahtjevi načela pravne zaštite, provedbe i odgovornosti dodatni uz zahtjev da se samoregulacija mora moći provesti u skladu s člankom 5. Zakona o FTC-u (glava 15. članak 45. Zakonika SAD-a), kojim se zabranjuje nepošteno ili prijevarno postupanje, glavom 49. člankom 41712. Zakonika SAD-a, kojim se prijevozniku ili posredniku u prodaji karata zabranjuje nepoštena ili prijevarna praksa u zračnom prijevozu ili prodaji usluga u zračnom prijevozu, ili u skladu s drugim zakonom ili propisom kojim se zabranjuje takvo postupanje.

c. Kako bi se osigurala usklađenost s njihovim obvezama iz okvira EU-a i SAD-a za privatnost podataka i pridonijelo upravljanju programom, organizacije i njihovi neovisni mehanizmi pravne zaštite na zahtjev Ministarstva trgovine moraju dostaviti informacije o okviru EU-a i SAD-a za privatnost podataka. Nadalje, organizacije moraju žurno odgovoriti na pritužbe u pogledu usklađenosti s Načelima koje su tijela za zaštitu podataka proslijedila Ministarstvu trgovine. U odgovoru bi trebalo biti navedeno je li pritužba osnovana i ako jest, kako će organizacija ispraviti problem. Ministarstvo trgovine štitit će povjerljivost zaprimljenih informacija u skladu s američkim pravom.

d. Mehanizmi pravne zaštite

i. Pojedince treba poticati da podnose pritužbe protiv relevantne organizacije prije nego što prijeđu na neovisne mehanizme pravne zaštite. Organizacije moraju odgovoriti pojedincu u roku od 45 dana od primitka pritužbe. Neovisnost mehanizma pravne zaštite činjenično je pitanje i može se dokazati nepristranošću, transparentnom strukturom i financiranjem te dokazanim iskustvom. U skladu s načelom pravne zaštite, provedbe i odgovornosti pravna zaštita koja je na raspolaganju pojedincima mora biti lako dostupna i besplatna. Neovisna tijela za rješavanje sporova trebala bi razmotriti sve pritužbe koje zaprime od pojedinaca, osim ako su očigledno neutemeljene ili neozbiljne. To ne sprečava neovisno tijelo za rješavanje sporova koje upravlja mehanizmom pravne zaštite da utvrdi zahtjeve prihvatljivosti, ali takvi bi zahtjevi trebali biti transparentni i opravdani (npr. ne trebaju uključivati pritužbe koje nisu obuhvaćene područjem primjene programa ili koje se razmatraju na drugom sudu) i ne bi smjeli umanjivati obvezu razmatranja opravdanih pritužbi. Osim toga, kad pojedinci podnesu pritužbu, u okviru mehanizama pravne zaštite trebali bi dobiti potpune i lako dostupne informacije o funkcioniranju postupka rješavanja sporova. U skladu s Načelima takve informacije trebale bi sadržavati obavijest o praksi zaštite privatnosti u okviru mehanizma. Trebali bi surađivati i na razvoju resursa, kao što su standardni obrasci pritužbi, kako bi se olakšao postupak rješavanja pritužbi.

ii. Na javnim internetskim stranicama neovisnih mehanizama pravne zaštite moraju se nalaziti informacije o Načelima i uslugama koje pružaju u skladu s okvirom EU-a i SAD-a za privatnost podataka. Te informacije moraju uključivati: 1. informacije o zahtjevima Načela za neovisne mehanizme pravne zaštite ili poveznicu na te zahtjeve, 2. poveznicu na internetske stranice Ministarstva trgovine za okvir za privatnost podataka, 3. objašnjenje da su njihove usluge rješavanja sporova u skladu s okvirom EU-a i SAD-a za privatnost podataka besplatne za pojedince, 4. opis načina na koji se može podnijeti pritužba koja se odnosi na Načela, 5. rok obrade takvih pritužbi i 6. opis mogućih pravnih sredstava.

iii. Neovisni mehanizmi pravne zaštite moraju objaviti godišnje izvješće s agregiranim statističkim podacima o njihovim uslugama rješavanja sporova. Godišnje izvješće mora sadržavati: 1. ukupan broj pritužbi koje se odnose na Načela i zaprimljene su u izvještajnoj godini, 2. vrste zaprimljenih pritužbi, 3. mjere za osiguranje kvalitete rješavanja sporova, kao što je trajanje obrade pritužbi, i 4. ishode zaprimljenih pritužbi, posebno broj i vrstu pravnih sredstava ili izrečenih sankcija.

iv. Kako je navedeno u Prilogu I., pojedincu je dostupna mogućnost arbitraže kojom se za preostale zahtjeve može utvrditi je li organizacija uključena u okvir za privatnost podataka povrijedila svoje obveze u skladu s Načelima u odnosu na tog pojedinca i je li to potpuno ili djelomično ispravljeno. Ta je mogućnost dostupna samo u navedene svrhe. Nije, na primjer, dostupna za izuzeća od Načela ([15]) ili navode o primjerenosti okvira EU-a i SAD-a za privatnost podataka. U skladu s tom mogućnošću arbitraže „odbor za okvir EU-a i SAD-a za privatnost podataka” (koji se sastoji od jednog ili tri arbitra, ovisno o dogovoru stranki) ima ovlasti utvrditi pojedinačnu nenovčanu pravičnu naknadu (kao što je pristup, ispravak, brisanje ili vraćanje predmetnih podataka pojedinca) koja je potrebna za ispravljanje povrede Načela samo u odnosu na pojedinca. Pojedinci i organizacije uključene u okvir za privatnost podataka moći će na temelju Saveznog zakona o arbitraži tražiti sudsko preispitivanje i provedbu arbitražnih odluka u skladu s američkim pravom.

e. Pravna sredstva i sankcije

i. Rezultat bilo kojeg pravnog sredstva koje nudi tijelo za rješavanje sporova trebao bi biti takav da organizacija poništi ili ispravi učinke neusklađenosti ako je to izvedivo i da obrada koju organizacija provodi u budućnosti bude u skladu s Načelima te da se prema potrebi prestanu obrađivati osobni podaci pojedinca koji je podnio pritužbu. Sankcije trebaju biti dovoljno stroge da bi se osigurala usklađenost organizacije s Načelima. Niz sankcija različite težine omogućit će tijelima za rješavanje sporova da na

([15]) Načela, „Pregled”, točka 5.

odgovarajući način reagiraju na različite stupnjeve neusklađenosti. Sankcije trebaju uključivati objavljivanje informacija o utvrđenoj neusklađenosti i zahtjev da se podaci u određenim okolnostima obrišu ([16]). Ostale sankcije mogu uključivati suspenziju i oduzimanje pečata, nadoknadu gubitaka koje su pojedinci pretrpjeli kao posljedicu neusklađenosti i izdavanje sudskog naloga. Neovisna tijela za rješavanje sporova iz privatnog sektora i samoregulatorna tijela moraju obavijestiti vladino tijelo primjenjive nadležnosti ili prema potrebi sudove i Ministarstvo trgovine da organizacije uključene u okvir za privatnost podataka ne postupaju u skladu s njihovim odlukama.

f. Mjere FTC-a

i. FTC se obvezao davati prednost preispitivanju upućenih predmeta o navodnoj neusklađenosti s Načelima koje mu podnose: i. samoregulatorna tijela za zaštitu privatnosti i druga neovisna tijela za rješavanje sporova, ii. države članice EU-a, i iii. Ministarstvo trgovine, kako bi utvrdio je li povrijeđen članak 5. Zakona o FTC-u kojim se zabranjuje nepošteno ili prijevarno postupanje ili trgovačka praksa. Ako FTC zaključi da postoji opravdana sumnja da je povrijeđen članak 5., može riješiti predmet traženjem da se izda upravni nalog za obustavu spornih radnji ili podnošenjem pritužbe saveznom okružnom sudu koja, ako bude uspješno riješena, može dovesti do saveznog sudskog naloga s istim učinkom. To uključuje lažne izjave o pridržavanju Načela okvira EU-a i SAD-a za privatnost podataka ili o sudjelovanju u njemu koje iznose organizacije koje više nisu na popisu organizacija uključenih u okvir za privatnost podataka ili se nikada nisu samocertificirale Ministarstvu trgovine. FTC može ishoditi građanskopravnu kaznu za povrede upravnog naloga za zabranu i može pokrenuti građansku parnicu ili kazneni postupak zbog povrede naloga saveznog suda. Obavijestit će Ministarstvo trgovine o poduzimanju takvih mjera. Ministarstvo trgovine potiče ostala vladina tijela da ga obavijeste o konačnoj presudi o takvim upućenim predmetima ili o drugim odlukama u kojima se utvrđuje pridržavanje Načela.

g. Ustrajna neusklađenost

i. Ako organizacija ustrajno ne postupa u skladu s Načelima, više nema pravo na to da se okvir EU-a i SAD-a za privatnost podataka primjenjuje na nju. Ministarstvo trgovine uklonit će organizacije koje ustrajno ne postupaju u skladu s Načelima s popisa organizacija uključenih u okvir za privatnost podataka i one moraju vratiti ili izbrisati osobne informacije zaprimljene u skladu s okvirom EU-a i SAD-a za privatnost podataka.

ii. Ustrajna neusklađenost s Načelima nastaje kad organizacija koja se samocertificirala Ministarstvu trgovine odbije postupiti u skladu s konačnom odlukom samoregulatornog tijela za zaštitu privatnosti, neovisnog tijela za rješavanje sporova ili vladina tijela, ili ako takvo tijelo, uključujući Ministarstvo trgovine, utvrdi da organizacija često ne postupa u skladu s Načelima do mjere u kojoj njezina izjava o tome da je usklađena više nije vjerodostojna. Ako takvu odluku donese neko tijelo osim Ministarstva trgovine, organizacija o tome mora odmah obavijestiti to ministarstvo. Ako to ne učini, može biti kažnjena u skladu sa Zakonom o davanju lažnog iskaza (glava 18. članak 1001. Zakonika SAD-a). Povlačenje organizacije iz samoregulatornog programa za zaštitu privatnosti ili neovisnog mehanizma rješavanja sporova iz privatnog sektora ne znači da ona više nije obvezna postupati u skladu s Načelima, nego to predstavlja ustrajnu neusklađenost.

iii. Ministarstvo trgovine uklonit će organizaciju s popisa organizacija uključenih u okvir za privatnost podataka zbog ustrajne neusklađenosti, među ostalim na temelju obavijesti o neusklađenosti koju primi od same organizacije, samoregulatornog tijela za zaštitu privatnosti ili drugog neovisnog tijela za rješavanje sporova, ili od vladina tijela, ali tek nakon što joj da rok od 30 dana i priliku za odgovor ([17]). U skladu s tim na popisu organizacija uključenih u okvir za privatnost podataka koji vodi Ministarstvo trgovine bit će jasno navedeno na koje se organizacije primjenjuje okvir EU-a i SAD-a za privatnost podataka, a na koje se više ne primjenjuje.

iv. Organizacija koja se prijavi za sudjelovanje u samoregulatornom tijelu kako bi ponovno stekla uvjete za članstvo u okviru EU-a i SAD-a za privatnost podataka mora tom tijelu dostaviti sve informacije o svojem prijašnjem sudjelovanju u tom okviru.

([16]) Neovisna 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 o tome hoće li biti potrebno brisati podatke, a drugi je činjenica je li organizacija prikupila, upotrebljavala ili otkrila informacije u očitoj suprotnosti s Načelima.

([17]) Ministarstvo trgovine u obavijesti će navesti koliko vremena organizacija ima za odgovor, a to nužno mora biti manje od 30 dana.

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

a. Općenito je svrha načela izbora osigurati da načini uporabe i otkrivanja osobnih informacija budu u skladu s očekivanjima i izborima pojedinca. Pojedinac bi stoga trebao imati mogućnost izbora da u bilo kojem trenutku zatraži izuzeće od uporabe njegovih osobnih informacija u svrhe izravnog marketinga uz primjenu razumnih ograničenja koja je odredila organizacija, kao što je davanje organizaciji vremena da izuzeće stupi na snagu. Organizacija može tražiti i dovoljno informacija da bi potvrdila identitet pojedinca koji traži izuzeće. Pojedinci u SAD-u možda će moći iskoristiti tu mogućnost u okviru središnjeg programa izuzeća. U svakom slučaju, pojedincu treba ponuditi lako dostupan i pristupačan mehanizam za korištenje te mogućnosti.

b. Slično tomu, organizacija može upotrebljavati informacije u određene svrhe izravnog marketinga kad nije praktično ponuditi pojedincu mogućnost da zatraži izuzeće prije njihove uporabe ako mu odmah ponudi mogućnost da ujedno (na zahtjev u bilo kojem trenutku i besplatno) odbije nastaviti primati izravne marketinške sadržaje i postupi u skladu s njegovim željama.

13. **Putne informacije**

a. Podaci o rezervaciji zrakoplovne karte i ostale putne informacije, kao što su informacije o programima vjernosti ili hotelskim rezervacijama i posebnim potrebama, na primjer obroci u skladu s vjerskim zahtjevima ili pružanje fizičke pomoći, mogu se u različitim okolnostima prenositi organizacijama izvan EU-a. U skladu s OUZP-om, ako nije donesena odluka o primjerenosti, osobni se podaci mogu prenijeti trećoj zemlji ako su predviđene odgovarajuće mjere za zaštitu podataka iz članka 46. OUZP-a ili u posebnim situacijama ako je ispunjen jedan od uvjeta iz članka 49. OUZP-a (npr. ako je ispitanik izričito pristao na prijenos). Američke organizacije koje sudjeluju u okviru EU-a i SAD-a za privatnost podataka osiguravaju primjerenu zaštitu osobnih podataka i stoga mogu primati podatke prenesene iz EU-a na temelju članka 45. OUZP-a a da ne moraju uvesti instrument za prijenos iz članka 46. OUZP-a ili ispuniti uvjete iz članka 49. OUZP-a. Budući da okvir EU-a i SAD-a za privatnost podataka uključuje posebna pravila za osjetljive informacije, takve informacije (koje se možda moraju prikupiti npr. jer je korisnicima potrebna fizička pomoć) mogu biti uključene u prijenose organizacijama uključenima u okvir za privatnost podataka. Međutim, organizacija koja prenosi informacije u svim slučajevima mora poštovati pravo države članice EU-a u kojoj djeluje, koje među ostalim može sadržavati posebne uvjete za postupanje s osjetljivim podacima.

14. **Farmaceutski i medicinski proizvodi**

a. Primjena prava EU-a/države članice ili Načela

i. Pravo EU-a/države članice primjenjuje se na prikupljanje osobnih podataka i na obradu koja se obavlja prije prijenosa u SAD. Načela se primjenjuju na podatke nakon njihova prijenosa u SAD. Podatke koji se upotrebljavaju za farmaceutska istraživanja i ostale svrhe prema potrebi treba anonimizirati.

b. Buduća znanstvena istraživanja

i. Osobni podaci u određenim medicinskim ili farmaceutskim istraživačkim studijama često imaju vrijednu ulogu u budućim znanstvenim istraživanjima. Ako se osobni podaci prikupljeni za jednu istraživačku studiju prenose američkoj organizaciji u skladu s okvirom EU-a i SAD-a za privatnost podataka, ta organizacija može upotrebljavati te podatke za nova znanstvena istraživanja ako je prvotno dostavljena odgovarajuća obavijest i ponuđena mogućnost izbora. Takva obavijest trebala bi sadržavati informacije o svim budućim posebnim uporabama podataka, primjerice za potrebe periodičnog praćenja, povezanih studija ili marketinga.

ii. Podrazumijeva se da sve buduće uporabe podataka ne mogu biti točno navedene jer nova istraživanja mogu proizaći iz novih saznanja o izvornim podacima, novih medicinskih otkrića i napretka te promjena u javnom zdravstvu i regulatornih promjena. Obavijest stoga prema potrebi treba uključivati objašnjenje da je moguće da će se osobni podaci upotrebljavati u budućim medicinskim i farmaceutskim istraživanjima koja nisu predviđena. Ako uporaba nije u skladu s općom istraživačkom svrhom u koju su osobni podaci izvorno prikupljeni ili za koju je pojedinac naknadno dao odobrenje, mora se pribaviti nova suglasnost.

c. Povlačenje iz kliničkog ispitivanja

i. Sudionici se mogu u bilo kojem trenutku odlučiti povući iz kliničkog ispitivanja ili se to od njih može tražiti. Svi osobni podaci prikupljeni prije povlačenja i dalje se mogu obraditi zajedno s ostalim podacima prikupljenima u okviru kliničkog ispitivanja ako je u obavijesti to bilo jasno navedeno kad je pojedinac pristao sudjelovati u njemu.

d. Prijenosi u regulatorne i nadzorne svrhe

i. Poduzeća koja proizvode lijekove i medicinske proizvode smiju davati osobne podatke iz kliničkih ispitivanja provedenih u EU-u regulatornim tijelima u SAD-u u regulatorne i nadzorne svrhe. Slični prijenosi dopušteni su drugim strankama, kao što su podružnice poduzeća i drugi 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 o tome koju terapiju dobiva koji sudionik. Otkrivanjem tih informacija ugrozila bi se valjanost studije i rezultata. Sudionicima u takvim kliničkim ispitivanjima (poznatima kao „slijepe" studije) ne mora se omogućiti pristup podacima o njihovoj terapiji tijekom ispitivanja ako je to ograničenje objašnjeno kad je sudionik pristao sudjelovati u studiji i ako bi se otkrivanjem takvih informacija ugrozio integritet istraživanja.

ii. Pristanak na sudjelovanje u ispitivanju u tim uvjetima razuman je razlog za odricanje od prava pristupa. Nakon završetka ispitivanja i analize rezultata sudionici bi trebali imati pristup svojim podacima ako to zatraže. Trebali bi ga prvenstveno tražiti od liječnika ili drugog zdravstvenog djelatnika koji im je davao terapiju u okviru kliničkog ispitivanja ili od organizacije koja je pokrovitelj ispitivanja.

f. Sigurnost proizvoda i praćenje učinkovitosti

i. Poduzeće koje proizvodi farmaceutske ili medicinske proizvode ne mora primjenjivati načela obavješćivanja, izbora, odgovornosti za daljnji prijenos i pristupa u svojim aktivnostima praćenja sigurnosti i učinkovitosti proizvoda, uključujući izvješćivanje o neželjenim učincima i praćenju pacijenata/osoba koji uzimaju određene lijekove ili upotrebljavaju medicinske proizvode ako se zbog pridržavanja Načela ne mogu ispuniti regulatorni zahtjevi. To se odnosi i na izvješća, na primjer pružatelja zdravstvene skrbi poduzećima koja proizvode lijekove i medicinske proizvode i na izvješća poduzeća koja proizvode lijekove i medicinske proizvode vladinim agencijama, kao što je Uprava za hranu i lijekove.

g. Šifrirani podaci

i. Glavni istraživač uvijek na početku zaštićuje podatke o istraživanju jedinstvenom šifrom kako se ne bi mogao otkriti identitet pojedinačnih ispitanika. Farmaceutska poduzeća koja su pokrovitelji tih istraživanja ne dobivaju šifru. Jedinstvenu šifru ima samo istraživač kako bi mogao identificirati sudionika istraživanja u posebnim okolnostima (npr. ako je potrebno praćenje liječenja). Na prijenos tako šifriranih podataka, koji se prema pravu EU-a smatraju osobnim podacima, iz EU-a u SAD primjenjivala bi se Načela.

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

a. Organizacija mora primjenjivati načela sigurnosti, cjelovitosti podataka i ograničenja svrhe te načela pravne zaštite, provedbe i odgovornosti na osobne podatke iz javno dostupnih izvora. Ta načela primjenjuju se i na osobne podatke prikupljene iz javnih evidencija (tj. iz evidencija koje vode vladine agencije ili tijela na bilo kojoj razini i koje su općenito otvorene na uvid javnosti).

b. Načela obavješćivanja, izbora ili odgovornosti za daljnji prijenos ne moraju se primjenjivati na informacije iz javne evidencije ako se ne pojavljuju u kombinaciji s informacijama iz evidencije koja nije javna i ako se poštuju uvjeti za ostvarivanje uvida koje je utvrdilo nadležno tijelo. Općenito nije nužno ni primjenjivati načela obavješćivanja, izbora ili odgovornosti za daljnji prijenos na javno dostupne informacije, osim ako europski prenositelj navede da takve informacije podliježu ograničenjima zbog kojih organizacija mora primjenjivati ta načela za namjeravane uporabe. Organizacije neće snositi odgovornost za način na koji te informacije upotrebljavaju oni koji ih dobiju iz objavljenih materijala.

c. Ako se utvrdi da je organizacija namjerno objavila osobne informacije u suprotnosti s Načelima kako bi ona ili netko drugi ostvario korist od tih iznimki, na tu se organizaciju više neće primjenjivati okvir EU-a i SAD-a za privatnost podataka.

d. Načelo pristupa nije nužno primjenjivati na informacije iz javne evidencije ako nisu kombinirane s drugim osobnim informacijama (osim malih količina informacija koje se upotrebljavaju za indeksaciju ili organizaciju informacija iz javne evidencije), ali moraju se poštovati svi uvjeti za ostvarivanje uvida koje je utvrdilo nadležno tijelo. Međutim, ako su podaci iz javne evidencije kombinirani s drugim informacijama iz evidencije koja nije javna (osim kako je prethodno navedeno), organizacija mora omogućiti pristup svim takvim informacijama, uz pretpostavku da se na njih ne odnose druge dopuštene iznimke.

e. Kao što je slučaj s informacijama iz javne evidencije, nije potrebno omogućiti pristup informacijama koje su već dostupne široj javnosti, osim ako su kombinirane s informacijama iz evidencije koja nije javna. Organizacije koje se bave prodajom javno dostupnih informacija mogu naplatiti svoju uobičajenu naknadu kad odgovaraju na zahtjev za pristup. Druga je mogućnost da pojedinci traže pristup svojim informacijama od organizacije koja je izvorno prikupila podatke.

16. **Zahtjevi javnih tijela za pristup**

a. Kako bi osigurale transparentnost u pogledu zakonitih zahtjeva javnih tijela za pristup osobnim informacijama, organizacije uključene u okvir za privatnost podataka mogu dobrovoljno izdavati periodična izvješća o transparentnosti u kojima navode broj zahtjeva za osobne informacije koje su zaprimile od javnih tijela iz razloga povezanih s kaznenim progonom ili nacionalnom sigurnošću ako je takvo otkrivanje dopušteno u skladu s primjenjivim pravom.

b. Informacije koje su organizacije uključene u okvir za privatnost podataka navele u tim izvješćima zajedno s informacijama koje je objavila obavještajna zajednica i drugim informacijama mogu se upotrebljavati za periodično zajedničko preispitivanje funkcioniranja okvira EU-a i SAD-a za privatnost podataka u skladu s Načelima.

c. Izostanak obavijesti u skladu s točkom (a) podtočkom xii. načela obavješćivanja ne sprečava niti dovodi u pitanje sposobnost organizacije da odgovori na svaki zakonit zahtjev.

PRILOG I.: MODEL ARBITRAŽE

U ovom Prilogu I. navedeni su uvjeti pod kojima su organizacije uključene u okvir EU-a i SAD-a za privatnost podataka obvezne provoditi arbitražu u skladu s načelom pravne zaštite, provedbe i odgovornosti. Mogućnost obvezujuće arbitraže koja je opisana u nastavku primjenjuje se na određene „preostale" zahtjeve u pogledu podataka obuhvaćenih okvirom EU-a i SAD-a za privatnost podataka. Svrha je te mogućnosti pojedincima pružiti brz, neovisan i pošten mehanizam za rješavanje navodnih povreda Načela koje nisu riješene ostalim mehanizmima okvira EU-a i SAD-a za privatnost podataka.

A. **Područje primjene**

Mogućnost arbitraže dostupna je pojedincu kako bi za preostale zahtjeve mogao utvrditi je li organizacija uključena u okvir za privatnost podataka povrijedila svoje obveze u skladu s Načelima u pogledu pojedinca i je li ta povreda potpuno ili djelomično ispravljena. Ta je mogućnost dostupna samo u navedene svrhe. Nije, na primjer, dostupna za izuzeća od Načela ([1]) ili navode o primjerenosti okvira EU-a i SAD-a za privatnost podataka.

B. **Dostupna pravna sredstva**

U skladu s tom mogućnošću arbitraže „odbor za okvir EU-a i SAD-a za privatnost podataka" (koji se sastoji od jednog ili tri arbitra, ovisno o dogovoru stranki) ima ovlasti utvrditi pojedinačnu nenovčanu pravičnu naknadu (kao što je pristup, ispravak, brisanje ili vraćanje predmetnih podataka pojedinca) koja je potrebna za ispravljanje povrede Načela samo u odnosu na pojedinca. To su jedine ovlasti koje navedeni odbor ima u pogledu pravnih sredstava. Kad razmatra pravna sredstva, odbor za okvir EU-a i SAD-a za privatnost podataka mora uzeti u obzir druga pravna sredstva koja su već određena drugim mehanizmima u sklopu okvira EU-a i SAD-a za privatnost podataka. Nisu dostupne odštete, nadoknade troškova, naknade ili druga pravna sredstva. Svaka stranka snosi vlastite troškove odvjetnika.

C. **Zahtjevi prije pokretanja arbitražnog postupka**

Pojedinac koji odluči zatražiti pokretanje arbitraže mora poduzeti sljedeće korake prije podnošenja zahtjeva za taj postupak: 1. izravno obavijestiti organizaciju o navodnoj povredi i dati joj priliku da riješi pitanje u roku utvrđenom u točki (d) podtočki i. dodatnog načela o rješavanju sporova i provedbi; 2. iskoristiti besplatni neovisni mehanizam pravne zaštite u skladu s Načelima; i 3. obratiti se Ministarstvu trgovine preko svojeg tijela za zaštitu podataka i dati mu priliku da pokuša besplatno riješiti pitanje u rokovima iz dopisa Uprave za međunarodnu trgovinu Ministarstva trgovine.

Pojedinac ne može zatražiti pokretanje arbitraže 1. ako je ista navodna povreda Načela prethodno bila predmet obvezujuće arbitraže; 2. ako je bila predmet konačne presude donesene u sudskom postupku u kojem je taj pojedinac bio stranka; ili 3. ako su je stranke prethodno riješile. Nadalje, ta se mogućnost ne može iskoristiti ako tijelo za zaštitu podataka 1. ima ovlasti u skladu s dodatnim načelom o ulozi tijela za zaštitu podataka ili dodatnim načelom o podacima o ljudskim resursima; ili 2. ima ovlasti riješiti navodnu povredu izravno s organizacijom. Samim ovlastima tijela za zaštitu podataka za rješavanje istog zahtjeva za arbitražu protiv voditelja obrade podataka iz EU-a ne isključuje se mogućnost pokretanja arbitražnog postupka protiv druge pravne osobe koju ne obvezuju ovlasti tijela za zaštitu podataka.

D. **Obvezujuća priroda odluka**

Odluka pojedinca da zatraži obvezujuću arbitražu u potpunosti je dobrovoljna. Arbitražna odluka bit će obvezujuća za sve stranke u arbitražnom postupku. Kad pojedinac iskoristi tu mogućnost, odriče se mogućnosti traženja pravne zaštite za istu navodnu povredu na drugom sudu, ali ako se nenovčanom pravičnom naknadom ne ostvaruje potpuna nadoknada navodne povrede, pojedinac može podnijeti zahtjev za odštetu koji se inače može podnijeti na sudu čak i ako je iskoristio mogućnost pokretanja arbitražnog postupka.

([1]) Načela, „Pregled", točka 5.

E. **Preispitivanje i provedba**

Pojedinci i organizacije uključene u okvir za privatnost podataka moći će na temelju Saveznog zakona o arbitraži tražiti sudsko preispitivanje i provedbu arbitražnih odluka u skladu s američkim pravom ([2]). Takvi se postupci moraju pokrenuti pred saveznim okružnim sudom koji je mjesno nadležan za glavno mjesto poslovanja organizacije uključene u okvir za privatnost podataka.

Svrha je te mogućnosti arbitraže rješavanje pojedinačnih sporova, a arbitražne odluke ne moraju biti uvjerljivi ili obvezujući presedani u pitanjima povezanima s drugim strankama, među ostalim u budućim arbitražnim postupcima, na europskim ili američkim sudovima ili u postupcima FTC-a.

F. **Arbitražno vijeće**

Stranke će izabrati arbitre za odbor za okvir EU-a i SAD-a za privatnost podataka s popisa arbitara navedenog u nastavku.

U skladu s primjenjivim pravom, Ministarstvo trgovine i Komisija sastavit će popis od najmanje 10 arbitara koji se biraju na temelju neovisnosti, integriteta i stručnosti. Na taj se postupak primjenjuje sljedeće:

Arbitri:

1. ostaju na popisu na razdoblje od tri godine, osim u iznimnim okolnostima ili u slučaju razrješenja iz opravdanih razloga, koje Ministarstvo trgovine uz prethodnu obavijest Komisiji može produljiti na još tri godine;

2. ne primaju upute od stranke, organizacije uključene u okvir za privatnost podataka, SAD-a, EU-a, države članice EU-a ili drugog vladina tijela, javnog tijela ili izvršnog tijela i nisu s njima povezani; i

3. moraju biti odvjetnici u SAD-u i stručnjaci za američko pravo o zaštiti privatnosti, s posebnim stručnim znanjem u području prava EU-a o zaštiti podataka.

([2]) U poglavlju 2. Saveznog zakona o arbitraži (*Federal Arbitration Act* – FAA) propisano 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, uključujući transakciju, ugovor ili sporazum opisan u [članku 2. FAA-a] primjenjuje Konvencija [o priznavanju i provedbi stranih arbitražnih odluka od 10. lipnja 1958., glava 21. članak 2519. Međunarodnih ugovora i sporazuma SAD-a (U.S.T.), Zbirka sporazuma i drugih međunarodnih ugovora (T.I.A.S.) br. 6997 (dalje u tekstu ‚Konvencija iz New Yorka')]." (glava 9. članak 202. Zakonika SAD-a). U FAA-u je dalje propisano da se „sporazum ili odluka proizašli iz tog odnosa u kojem isključivo sudjeluju državljani SAD-a ne smatraju obuhvaćenima 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 postoji neka druga razumna poveznica s jednom ili više stranih država." *(vidjeti prethodno upućivanje)*. U skladu s poglavljem 2. „svaka stranka u arbitraži na temelju ovog poglavlja može podnijeti zahtjev bilo kojem nadležnom sudu 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]." *(vidjeti prethodno upućivanje,* članak 207.). U poglavlju 2. propisano je i da su „okružni sudovi SAD-a […] nadležni za […] mjeru ili postupak [u skladu s Konvencijom iz New Yorka], neovisno o spornom iznosu." *(vidjeti prethodno upućivanje,* članak 203.).
U poglavlju 2. propisano je i 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 ju je ratificirao SAD." *(vidjeti prethodno upućivanje,* članak 208.). S druge strane, u poglavlju 1. propisano je da je „pisana odredba u […] ugovoru kao dokaz poslovne transakcije za rješavanje spora arbitražom koja proizlazi iz takvog ugovora ili transakcije ili odbijanja izvršavanja cijelog ili dijela tog ugovora ili transakcije, ili pisani sporazum o pokretanju arbitražnog postupka zbog postojećeg spora koji proizlazi iz takvog ugovora, transakcije ili odbijanja, važeća, neponištiva i izvršiva, osim na osnovama koje postoje u pravu ili pravnom lijeku za raskid ugovora." *(vidjeti prethodno upućivanje,* članak 2.). U poglavlju 1. dalje je predviđeno da „svaka stranka u arbitražnom postupku može od za to određenog suda tražiti nalog kojim se potvrđuje odluka i sud ga potom mora odobriti, osim ako je odluka poništena, izmijenjena ili ispravljena kako je propisano u člancima 10. i 11. [FAA-a]". *(vidjeti prethodno upućivanje,* članak 9.).

G. **Arbitražni postupci**

Ministarstvo trgovine i Komisija u skladu s primjenjivim pravom dogovorili su se da će donijeti arbitražne propise kojima se uređuju postupci pred odborom za okvir EU-a i SAD-a za privatnost podataka ([3]). Ako bude potrebno mijenjati propise kojima se uređuju postupci, Ministarstvo trgovine i Komisija dogovorit će se da prema potrebi izmijene te propise ili primijene drugi skup postojećih i dokazanih arbitražnih postupaka SAD-a, uz ispunjavanje svih uvjeta u nastavku:

1. Pojedinac može pokrenuti obvezujuću arbitražu u skladu s prethodno navedenim zahtjevima prije pokretanja arbitražnog postupka dostavljanjem obavijesti organizaciji. Obavijest sadržava sažetak koraka poduzetih u skladu s odjeljkom C za rješavanje zahtjeva, opis navedene potvrde i, ako pojedinac tako želi, prateće dokumente i materijale i/ili pregled prava koje se odnosi na navodni zahtjev.

2. Osmislit će se postupci kojima će se osigurati da pojedinac 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 predstavnik SAD-a, EU-a, države članice EU-a ili drugog vladina tijela, javnog tijela ili izvršnog tijela ako na zahtjev pojedinca iz EU-a tijela za zaštitu podataka mogu pružati pomoć samo u pripremi obavijesti, ali ne smiju imati pristup otkrivenim dokazima ili drugim materijalima povezanima s arbitražnim postupkom.

5. Arbitraža se provodi u SAD-u, a pojedinac može odlučiti sudjelovati videokonferencijom ili telefonom, što će mu se besplatno omogućiti. Osobna nazočnost neće biti obavezna.

6. Jezik arbitraže bit će engleski, osim ako se stranke dogovore drukčije. Na razuman zahtjev i ovisno o tome zastupa li pojedinca odvjetnik na arbitražnoj se raspravi osiguravaju besplatne usluge usmenog prevođenja i prijevoda arbitražnih materijala, osim ako odbor za okvir EU-a i SAD-a za privatnost podataka odluči da bi s obzirom na okolnosti određenog arbitražnog postupka time nastali neopravdani ili nerazmjerni troškovi.

7. Materijali dostavljeni arbitrima smatrat će se povjerljivima i upotrebljavati samo u vezi s arbitražnim postupkom.

8. Otkrivanje dokaza koji se odnose na pojedinca dopušteno je prema potrebi, a stranke će te dokaze smatrati povjerljivima i upotrebljavati ih samo u vezi s arbitražnim postupkom.

9. Arbitražni bi se postupci trebali dovršiti u roku od 90 dana od dostavljanja obavijesti predmetnoj organizaciji, osim ako se stranke dogovore drukčije.

([3]) Ministarstvo trgovine odabralo je Međunarodni centar za rješavanje sporova (ICDR) Američkog udruženja za arbitražu (AAA) za vođenje arbitraža u skladu s Prilogom I. Načelima i za upravljanje arbitražnim fondom utvrđenim u tom prilogu. Ministarstvo trgovine i Komisija dogovorili su se 15. rujna 2017. da će donijeti propise o arbitraži kojima se uređuju obvezujući arbitražni postupci opisani u Prilogu I. Načelima te kodeks ponašanja za arbitre koji je u skladu s općeprihvaćenim etičkim normama za trgovačke arbitre i s Prilogom I. Načelima. Dogovorili su se da će prilagoditi propise o arbitraži i kodeks ponašanja kako bi bili u skladu s ažuriranim okvirom EU-a i SAD-a za privatnost podataka, a Ministarstvo trgovine i Međunarodni centar za rješavanje sporova Američkog udruženja za arbitražu zajedno će ih ažurirati.

H. **Troškovi**

Arbitri bi trebali poduzeti razumne korake kako bi smanjili troškove ili naknade za arbitražne postupke.

U skladu s primjenjivim pravom Ministarstvo trgovine uspostavit će fond u koji će organizacije uključene u okvir za privatnost podataka morati uplaćivati doprinos koji se djelomično temelji na veličini organizacije, a obuhvaćat će troškove arbitražnog postupka, uključujući naknade za arbitre, do najvećih iznosa („gornje granice”). Fondom će upravljati treća strana, koja će redovito izvješćivati Ministarstvo trgovine o radu fonda. Ministarstvo trgovine surađivat će s trećom stranom na periodičnom preispitivanju funkcioniranja fonda, među ostalim kad je riječ o potrebi da se prilagodi iznos doprinosa ili gornjih granica troškova arbitražnog postupka, te će među ostalim uzeti u obzir broj provedenih arbitražnih postupaka, njihove troškove i rokove, pri čemu se podrazumijeva da to neće uključivati pretjerano financijsko opterećenje za organizacije uključene u okvir za privatnost podataka. Ministarstvo trgovine obavijestit će Komisiju o ishodu takvih preispitivanja s trećom stranom i dostaviti joj prethodnu obavijest o eventualnim prilagodbama iznosa doprinosa. Troškovi odvjetnika nisu obuhvaćeni ovom odredbom ni bilo kojim fondom iz ove odredbe.

PRILOG II.

MINISTARSTVO TRGOVINE SJEDINJENIH AMERIČKIH DRŽAVA
Ministrica trgovine
Washington, D.C. 20230

6. srpnja 2023.

Poštovani g. Didier Reynders
Povjerenik za pravosuđe
Europska komisija
Rue de la Loi/Westraat 200
1049 Bruxelles
Belgija

Poštovani povjereniče Reynders,

zadovoljstvo mi je u ime Sjedinjenih Američkih Država ovim Vam putem dostaviti paket materijala o okviru EU-a i SAD-a za privatnost podataka, koji je, zajedno s Izvršnim nalogom br. 14086 o poboljšanju zaštitnih mjera u američkim aktivnostima elektroničkog izviđanja, i glavom 28. odjeljkom 201. Kodeksa saveznih propisa, kojim se izmjenjuju propisi Ministarstva pravosuđa o osnivanju Žalbenog suda za zaštitu podataka, potvrda važnih i detaljnih pregovora o jačanju oblika zaštite privatnosti i građanskih sloboda. Rezultat su tih pregovora nove zaštitne mjere kojima se osigurava nužnost i proporcionalnost američkih aktivnosti elektroničkog izviđanja za ostvarenje utvrđenih ciljeva u području nacionalne sigurnosti i novi mehanizam pravne zaštite za pojedince iz Europske unije koji smatraju da su bili predmet aktivnosti elektroničkog izviđanja u suprotnosti sa zakonom, a njihovom će se kombinacijom zaštititi privatnost osobnih podataka iz EU-a. Okvir EU-a i SAD-a za privatnost podataka pridonijet će uključivom i konkurentnom digitalnom gospodarstvu. Oboje bismo trebali biti ponosni na poboljšanja vidljiva u tom okviru, kojim će se povećati zaštita privatnosti u cijelom svijetu. Ovaj je paket, zajedno s Izvršnim nalogom, propisima i drugim materijalima dostupnima iz javnih izvora, vrlo čvrsta osnova za novi zaključak Europske komisije o primjerenosti ([1]).

Priloženi su sljedeći materijali:

— Načela okvira EU-a i SAD-a za privatnost podataka, uključujući Dodatna načela (zajedno „Načela”) i Prilog I. Načelima (tj. prilog u kojem su navedeni uvjeti u skladu s kojima su organizacije uključene u okvir za privatnost podataka obvezne provoditi arbitražne postupke za određene preostale zahtjeve u pogledu osobnih podataka obuhvaćenih Načelima),

— dopis Uprave za međunarodnu trgovinu Ministarstva trgovine, koja upravlja programom za okvir za privatnost podataka, u kojem su opisane obveze koje je naše ministarstvo preuzelo u cilju osiguranja učinkovitog funkcioniranja okvira EU-a i SAD-a za privatnost podataka,

— dopis Savezne trgovinske komisije u kojem je opisana njezina provedba Načela,

— dopis Ministarstva prometa u kojem je opisana njegova provedba Načela,

— dopis koji je pripremio Ured direktora za nacionalna obavještajna pitanja u vezi sa zaštitnim mjerama i ograničenjima koja se primjenjuju na američka tijela za nacionalnu sigurnost, i

— dopis koji je pripremilo Ministarstvo pravosuđa u vezi sa zaštitnim mjerama i ograničenjima pristupa američke vlade u svrhe kaznenog progona i javnih interesa.

([1]) Ako se odluka Komisije o primjerenosti zaštite koju pruža okvir EU-a i SAD-a za privatnost podataka primjenjuje na Island, Lihtenštajn i Norvešku, paket okvira EU-a i SAD-a za privatnost podataka obuhvatit će Europsku uniju i tri navedene zemlje.

Cijeli paket okvira EU-a i SAD-a za privatnost podataka objavit će se na internetskim stranicama Ministarstva trgovine za okvir za privatnost podataka, a Načela i Prilog I. Načelima stupit će na snagu na datum stupanja na snagu odluke Europske komisije o primjerenosti.

Uvjeravam Vas da Sjedinjene Američke Države te obveze shvaćaju ozbiljno. S nestrpljenjem očekujemo suradnju u provedbi okvira EU-a i SAD-a za privatnost podataka dok zajednički ulazimo u sljedeću fazu ovog postupka.

S poštovanjem

Gina M. RAIMONDO

PRILOG III.

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

12. prosinca 2022.

Poštovani g. Didier Reynders
Povjerenik za pravosuđe
Europska komisija
Rue de la Loi/Westraat 200
1049 Bruxelles
Belgija

Poštovani povjereniče Reynders,

u ime Uprave za međunarodnu trgovinu zadovoljstvo mi je opisati obveze koje je Ministarstvo trgovine u okviru svojeg upravljanja programom za okvir za privatnost podataka i njegova nadzora preuzelo radi zaštite osobnih podataka. Dovršetak okvira EU-a i SAD-a za privatnost podataka važno je postignuće za zaštitu privatnosti i za poduzeća s obje strane Atlantika jer će se pojedincima iz EU-a zajamčiti da će njihovi podaci biti zaštićeni i da će na raspolaganju imati pravna sredstva u slučaju bilo kakvih dvojbi o svojim podacima, a tisućama poduzeća omogućit će se da nastave ulagati i obavljati ostale oblike trgovinske djelatnosti preko Atlantika, u korist naših gospodarstava i građana. Okvir EU-a i SAD-a za privatnost podataka rezultat je godina napornog rada i suradnje s Vama i Vašim kolegama u Europskoj komisiji. Veselimo se daljnjoj suradnji s Komisijom kako bi naš zajednički trud urodio plodom.

Okvir EU-a i SAD-a za privatnost podataka donijet će znatne prednosti pojedincima i poduzećima. Prvo, on pruža važne oblike zaštite privatnosti podataka pojedinaca iz EU-a prenesenih u SAD. Njime se od američkih organizacija uključenih u okvir zahtijeva da izrade usklađenu politiku zaštite privatnosti, da se javno obvežu da će poštovati Načela okvira EU-a i SAD-a za privatnost podataka, uključujući Dodatna načela (zajedno „Načela") i Prilog I. Načelima (tj. prilog u kojem su navedeni uvjeti u skladu s kojima su organizacije uključene u okvir EU-a i SAD-a za privatnost podataka obvezne provoditi arbitražne postupke za određene preostale zahtjeve u pogledu osobnih podataka obuhvaćenih Načelima), kako bi ta obveza postala provediva u skladu s američkim pravom ([1]), da svake godine ponovno certificiraju svoju usklađenost pri Ministarstvu trgovine, da omoguće besplatno, neovisno rješavanje sporova pojedincima iz EU-a, i da podliježu istražnim i provedbenim ovlastima američkog zakonskog tijela navedenog u Načelima (npr. Savezna trgovinska komisija, FTC ili Ministarstvo prometa) ili američkog zakonskog tijela navedenog u budućem prilogu Načelima. Iako organizacija dobrovoljno donosi odluku o samocertificiranju, kad se javno obveže sudjelovati u okviru EU-a i SAD-a za privatnost podataka, ta je obveza provediva u skladu s američkim pravom i mogu je provesti FTC, Ministarstvo prometa ili drugo američko zakonsko tijelo, ovisno o tome koje je tijelo nadležno za organizaciju uključenu u okvir za privatnost podataka. Drugo, okvir EU-a i SAD-a za privatnost podataka omogućit će poduzećima u SAD-u i tamošnjim podružnicama europskih poduzeća da primaju osobne podatke iz Europske unije kako bi se pojednostavnio protok podataka koji

([1]) Organizacije koje su samocertificiranjem preuzele obvezu usklađivanja s Načelima europsko-američkog sustava zaštite privatnosti i žele ostvariti pogodnosti iz okvira EU-a i SAD-a za privatnost podataka moraju se uskladiti s Načelima okvira EU-a i SAD-a za privatnost podataka. Ta obveza usklađivanja s Načelima okvira EU-a i SAD-a za privatnost podataka mora se što prije uvrstiti u politike zaštite privatnosti tih organizacija, a u svakom slučaju najkasnije tri mjeseca nakon datuma stupanja na snagu Načela okvira EU-a i SAD-a za privatnost podataka. (Vidjeti odjeljak (e) dodatnog načela o samocertificiranju).

olakšava transatlantsku trgovinu. Protok podataka između SAD-a i Europske unije najveći je na svijetu i pridonosi američko-europskom gospodarskom odnosu koji je vrijedan 7,1 bilijun USD i omogućuje milijune radnih mjesta s obje strane Atlantika. Poduzeća koja se oslanjaju na transatlantski protok podataka potječu iz svih industrijskih sektora i uključuju velika poduzeća s popisa 500 najuspješnijih časopisa Fortune te brojna mala i srednja poduzeća. Transatlantski protok podataka omogućuje američkim organizacijama da obrađuju podatke koji su potrebni kako bi se Europljanima mogle ponuditi roba, usluge i prilike za zapošljavanje.

Ministarstvo trgovine spremno je na blisku i produktivnu suradnju s našim kolegama iz EU-a radi učinkovitog upravljanja programom za okvir za privatnost podataka i njegova nadzora. Ta se spremnost očituje u činjenici da Ministarstvo trgovine razvija i kontinuirano usavršava razna sredstva za pomoć organizacijama u postupku samocertificiranja, izrađuje internetske stranice za pružanje ciljanih informacija dionicima, surađuje s Komisijom i europskim tijelima za zaštitu podataka na razvoju smjernica kojima se pojašnjavaju važni elementi okvira EU-a i SAD-a za privatnost podataka, provodi aktivnosti informiranja organizacija da bi bolje razumjele svoje obveze zaštite podataka te nadzire i prati usklađenost organizacija sa zahtjevima programa.

Zahvaljujući stalnoj suradnji s našim cijenjenim partnerima iz EU-a Ministarstvo trgovine osigurat će djelotvorno funkcioniranje okvira EU-a i SAD-a za privatnost podataka. Vlada SAD-a dugo surađuje s Komisijom na promicanju zajedničkih načela zaštite podataka, čime se premošćuju razlike u našim pravnim pristupima, a ujedno potiču trgovina i gospodarski rast u Europskoj uniji i SAD-u. Smatramo da će Komisija na temelju okvira EU-a i SAD-a za privatnost podataka, koji je primjer te suradnje, moći objaviti novu odluku o primjerenosti zahvaljujući kojoj će organizacije moći primjenjivati taj okvir za prijenos osobnih podataka iz Europske unije u SAD u skladu sa zakonodavstvom EU-a.

Upravljanje programom za okvir za privatnost podataka i njegov nadzor koje provodi Ministarstvo trgovine

Ministarstvo trgovine odlučno se zalaže za djelotvorno upravljanje programom za okvir za privatnost podataka i njegov nadzor te će u to uložiti odgovarajući trud i resurse. Ministarstvo trgovine vodit će i objavljivati obvezujući popis američkih organizacija koje su se samocertificirale tom ministarstvu i izjavile da će se pridržavati Načela („popis organizacija uključenih u okvir za privatnost podataka”), a ažurirat će ga na temelju godišnjih prijava za ponovno certificiranje organizacija uključenih u okvir za privatnost podataka i ukloniti organizacije s popisa kad se one dobrovoljno povuku, kad ne ispune obvezu godišnjeg ponovnog certificiranja u skladu s postupcima Ministarstva trgovine ili ako se utvrdi da ustrajno ne postupaju u skladu s Načelima. Nadalje, Ministarstvo trgovine vodit će i objavljivati obvezujuću evidenciju američkih organizacija koje su uklonjene s popisa organizacija uključenih u okvir za privatnost podataka i za svaku navesti razlog zbog kojeg je to učinjeno. Prethodno spomenuti obvezujući popis i evidencija bit će javno dostupni na internetskim stranicama Ministarstva trgovine za okvir za privatnost podataka. Na tim će internetskim stranicama na istaknutom mjestu biti objašnjeno da svaka organizacija koja je uklonjena s popisa organizacija uključenih u okvir za privatnost podataka mora prestati izjavljivati da sudjeluje u okviru EU-a i SAD-a za privatnost podataka ili da je usklađena s njim te da može primati osobne informacije u skladu s tim okvirom. Takva organizacija ipak mora nastaviti primjenjivati Načela na osobne informacije koje je primila dok je sudjelovala u okviru EU-a i SAD-a za privatnost podataka sve dok čuva takve informacije. Kako bi se nastavilo sveobuhvatno i kontinuirano zalagati za djelotvorno upravljanje programom za okvir za privatnost podataka i njegov nadzor, Ministarstvo trgovine izričito se obvezuje da će provoditi sljedeće aktivnosti:

Provjera zahtjeva za samocertificiranje

— Prije dovršetka izvornog samocertificiranja ili godišnjeg ponovnog certificiranja određene organizacije (zajedno „samocertificiranje”) i njezina uvrštavanja na popis organizacija uključenih u okvir za privatnost podataka ili zadržavanja na tom popisu, Ministarstvo trgovine provjerit će je li organizacija ispunila barem relevantne zahtjeve iz dodatnog načela o samocertificiranju koji se odnose na informacije koje organizacija mora navesti u svojoj prijavi za samocertificiranje Ministarstvu trgovine i je li u prikladnom trenutku uvela relevantnu politiku zaštite privatnosti kojom se pojedinci informiraju o svih 13 elemenata navedenih u načelu obavješćivanja. Ministarstvo trgovine provjerit će je li organizacija:

— navela ime organizacije koja podnosi prijavu za samocertificiranje, kao i imena svih njezinih subjekata ili podružnica u SAD-u koji se isto tako pridržavaju Načela i koje organizacija želi obuhvatiti svojim samocertificiranjem,

— navela potrebne podatke za kontakt za organizaciju (npr. podatke za kontakt za određene pojedince i/ili urede organizacije koja se samocertificira odgovorne za rješavanje pritužbi, zahtjeva za pristup i svih ostalih pitanja povezanih s okvirom EU-a i SAD-a za privatnost podataka),

— opisala svrhe u koje će organizacija prikupljati i koristiti osobne informacije koje je zaprimila od Europske unije,

— navela koje će osobne informacije zaprimiti od Europske unije u skladu s okvirom EU-a i SAD-a za privatnost podataka i time obuhvatiti samocertificiranjem,

— na svojim javnim internetskim stranicama, ako ih ima, navela internetsku adresu na kojoj je lako dostupna relevantna politika zaštite privatnosti ili je li dostavila Ministarstvu trgovine primjerak relevantne politike zaštite privatnosti te navela gdje tu politiku mogu pročitati pojedinci na koje se osobne informacije odnose (tj. poslodavci ako je riječ o politici zaštite privatnosti podataka o ljudskim resursima ili javnost ako nije riječ o takvoj politici),

— u svoju relevantnu politiku zaštite privatnosti u prikladnom trenutku (tj. na početku samo u njezin nacrt priložen prijavi ako je riječ o izvornoj prijavi za samocertificiranje, a kasnije u konačnu i prema potrebi objavljenu politiku zaštite privatnosti) uključila izjavu da se pridržava Načela i poveznicu na internetske stranice Ministarstva trgovine za okvir za privatnost podataka ili internetsku adresu na kojoj se on nalazi (npr. početna stranica ili internetska stranica s popisom organizacija uključenih u okvir za privatnost podataka),

— u svoju relevantnu politiku zaštite privatnosti u prikladnom trenutku uključila preostalih 12 elemenata navedenih u načelu obavješćivanja (npr. mogućnost da pojedinac iz EU-a na kojeg se odnose informacije u određenim okolnostima zatraži obvezujuću arbitražu, obveza otkrivanja osobnih informacija u odgovoru na zakonite zahtjeve javnih tijela, među ostalim da bi se ispunili zahtjevi u pogledu nacionalne sigurnosti ili kaznenog progona i vlastita odgovornost u slučajevima daljnjih prijenosa trećim stranama),

— odredila posebno zakonsko tijelo koje je nadležno rješavati pritužbe protiv organizacije zbog moguće nepoštene ili prijevarne prakse i povreda zakona ili propisa o zaštiti privatnosti (i koje je navedeno u Načelima ili budućem prilogu Načelima),

— navela program za zaštitu privatnosti u kojem organizacija sudjeluje kao članica,

— utvrdila je li relevantna metoda (tj. postupci praćenja koje mora primijeniti) za provjeru njezine usklađenosti s Načelima „samoprocjena” (tj. interna provjera) ili „vanjsko preispitivanje usklađenosti” (tj. provjera koju provodi treća strana) i ako je riječ o potonjem, je li navela i koja je treća strana provela preispitivanje usklađenosti,

— odabrala prikladan neovisni mehanizam pravne zaštite koji je dostupan za rješavanje pritužbi podnesenih u skladu s Načelima i omogućila pojedincu na kojeg se informacije odnose besplatan pristup prikladnoj pravnoj zaštiti.

— Ako je organizacija odabrala neovisan mehanizam pravne zaštite koji pruža tijelo za alternativno rješavanje sporova iz privatnog sektora, u svoju je relevantnu politiku zaštite privatnosti uključila poveznicu na internetske stranice ili adresu relevantnih internetskih stranica ili obrazac za podnošenje pritužbi mehanizma koji je dostupan za istragu neriješenih pritužbi podnesenih u skladu s Načelima.

— Ako je organizacija obvezna (u slučaju podataka o ljudskim resursima prenesenih iz Europske unije u kontekstu radnog odnosa) ili je odabrala surađivati s prikladnim tijelima za zaštitu podataka na istraživanju i rješavanju pritužbi podnesenih u skladu s Načelima, izjavila je da se obvezuje na takvu suradnju s tijelima za zaštitu podataka i postupanje u skladu s njihovim relevantnim savjetima kako bi poduzela određenu radnju za usklađivanje s Načelima.

— Ministarstvo trgovine provjerit će i je li prijava organizacije za samocertificiranje u skladu s njezinim relevantnim politikama zaštite privatnosti. Ako organizacija koja se samocertificira želi obuhvatiti svoje subjekte ili podružnice u SAD-u koji imaju zasebne relevantne politike zaštite privatnosti, Ministarstvo trgovine preispitat će i relevantne politike zaštite privatnosti takvih obuhvaćenih subjekata ili podružnica kako bi osiguralo da sadržavaju sve potrebne elemente iz načela obavješćivanja.

— Ministarstvo trgovine surađivat će sa zakonskim tijelima (npr. FTC i Ministarstvo prometa) kako bi provjerilo podliježu li organizacije nadležnosti relevantnog zakonskog tijela utvrđenog u njihovoj prijavi za samocertificiranje ako ima razloga sumnjati u to da podliježu toj nadležnosti.

— Ministarstvo trgovine surađivat će s tijelima za alternativno rješavanje sporova iz privatnog sektora kako bi provjerilo jesu li organizacije aktivno registrirane za neovisni mehanizam pravne zaštite naveden u njihovim prijavama za samocertificiranje i, ako tijela nude obje vrste usluga, jesu li organizacije aktivno registrirane za vanjsko preispitivanje usklađenosti navedeno u tim prijavama.

— Ako su organizacije odabrale tijela za zaštitu podataka kao relevantni neovisni mehanizam pravne zaštite, Ministarstvo trgovine surađivat će s trećom stranom koju je odabralo za čuvara sredstava prikupljenih naplatom naknade za odbor tijela za zaštitu podataka (godišnja naknada namijenjena za pokrivanje operativnih troškova tog odbora) kako bi provjerilo jesu li organizacije platile naknadu za relevantnu godinu.

— Ministarstvo trgovine surađivat će s trećom stranom koju je odabralo za vođenje arbitraža u skladu s Prilogom I. Načelima i za upravljanje arbitražnim fondom utvrđenim u tom prilogu kako bi provjerilo jesu li organizacije uplatile doprinos tom fondu.

— Ako Ministarstvo trgovine u svojem preispitivanju prijava organizacija za samocertificiranje utvrdi bilo kakve probleme, obavijestit će ih da moraju riješiti te probleme u prikladnom roku koji to ministarstvo odredi ([2]). Obavijestit će ih i da će se, ako odgovor izostane u roku koji je odredilo Ministarstvo trgovine ili se na drugi način ne ispune obveze samocertificiranja u skladu s postupcima Ministarstva trgovine, smatrati da su organizacije odustale od tih prijava za samocertificiranje te da svako lažno prikazivanje sudjelovanja organizacije u samocertificiranje te da svako lažno prikazivanje sudjelovanja organizacije u okviru EU-a i SAD-a za privatnost podataka ili o njezinoj usklađenosti s njim može biti predmet provedbenih mjera FTC-a, Ministarstva prometa ili drugog relevantnog vladina tijela. Ministarstvo trgovine obavijestit će organizacije s pomoću kontaktnih podataka koje su mu one dostavile.

Olakšavanje suradnje s tijelima za alternativno rješavanje sporova koja pružaju usluge povezane s Načelima

— Ministarstvo trgovine surađivat će s tijelima za alternativno rješavanje sporova iz privatnog sektora koja pružaju usluge neovisnih mehanizama pravne zaštite, koji su dostupni za istragu neriješenih pritužbi podnesenih u skladu s Načelima, kako bi provjerilo ispunjavaju li barem zahtjeve utvrđene u dodatnom načelu o rješavanju sporova i provedbi. Ministarstvo trgovine provjerit će jesu li:

  — na njihovim javnim internetskim stranicama navedene informacije o Načelima i uslugama koje pružaju u skladu s okvirom EU-a i SAD-a za privatnost podataka, što mora uključivati: 1. informacije o zahtjevima Načela za neovisne mehanizme pravne zaštite ili poveznicu na te zahtjeve, 2. poveznicu na internetske stranice Ministarstva trgovine za okvir za privatnost podataka, 3. objašnjenje da su njihove usluge rješavanja sporova u skladu s okvirom EU-a i SAD-a za privatnost podataka besplatne za pojedince, 4. opis načina na koji se može podnijeti pritužba koja se odnosi na Načela, 5. rok obrade takvih pritužbi i 6. opis mogućih pravnih sredstava. Ministarstvo trgovine pravodobno će obavijestiti tijela o značajnim promjenama programa tog ministarstva za upravljanje programom za okvir za privatnost podataka i njegov nadzor ako se te promjene događaju uskoro ili su se već dogodile, a relevantne su za ulogu koju tijela imaju u skladu s okvirom EU-a i SAD-a za privatnost podataka,

([2]) Npr. očekuje se da organizacije riješe sve probleme povezane s ponovnim certificiranjem u roku od 45 dana, osim ako Ministarstvo trgovine odredi drugi prikladan rok.

— objaviti godišnje izvješće s agregiranim statističkim podacima o svojim uslugama rješavanja sporova, što mora uključivati: 1. ukupan broj pritužbi koje se odnose na Načela i zaprimljene su u izvještajnoj godini, 2. vrste zaprimljenih pritužbi, 3. mjere za osiguranje kvalitete rješavanja sporova, kao što je trajanje obrade pritužbi, i 4. ishode zaprimljenih pritužbi, posebno broj i vrstu pravnih sredstava ili izrečenih sankcija. Ministarstvo trgovine tijelima će dostaviti precizne dodatne smjernice o tome koje bi informacije trebala navesti u tim godišnjim izvješćima, u kojima će objasniti te zahtjeve (npr. navesti posebne kriterije koje pritužba mora ispunjavati kako bi je se za potrebe godišnjeg izvješća smatralo pritužbom koja se odnosi na Načela) i navesti ostale informacije koje bi trebalo dostaviti (npr. ako tijelo pruža i usluge provjere povezane s Načelima, opis načina na koji izbjegava stvarne ili moguće sukobe interesa u situacijama kad organizaciji pruža usluge provjere i rješavanja sporova). U dodatnim smjernicama Ministarstva trgovine bit će naveden i datum do kojeg bi trebalo objaviti godišnja izvješća tijela za relevantno izvještajno razdoblje.

Praćenje organizacija koje žele biti uklonjene ili su uklonjene s popisa organizacija uključenih u okvir za privatnost podataka

— Ako se organizacija želi povući iz okvira EU-a i SAD-a za privatnost podataka, Ministarstvo trgovine tražit će od nje da iz relevantnih politika zaštite privatnosti ukloni sva upućivanja na taj okvir iz kojih bi se moglo zaključiti da i dalje sudjeluje u njemu te da može primati osobne podatke u skladu s tim okvirom (vidjeti opis obveze traženja lažnih izjava o sudjelovanju koju je preuzelo Ministarstvo trgovine). Ministarstvo trgovine zahtijevat će od organizacije i da mu dostavi ispunjen odgovarajući upitnik u kojem će potvrditi:

  — svoju želju da se povuče,

  — što će od sljedećih mogućnosti učiniti s osobnim podacima koje je primila u skladu s okvirom EU-a i SAD-a za privatnost podataka dok je sudjelovala u njemu: (a) zadržati te podatke, nastaviti primjenjivati Načela na njih i svake godine potvrditi Ministarstvu trgovine da se obvezuje i dalje primjenjivati Načela na njih, (b) zadržati takve podatke i osigurati njihovu „primjerenu” zaštitu drugim odobrenim sredstvima, ili (c) vratiti ili izbrisati sve takve podatke do određenog datuma, i

  — tko će u organizaciji biti stalna kontaktna točka za pitanja koja se odnose na Načela.

— Ako organizacija odabere prethodno opisanu opciju (a), Ministarstvo trgovine zahtijevat će i da mu svake godine nakon povlačenja (tj. do prve godišnjice povlačenja i na svaku sljedeću, osim ako i sve dok ne osigura „primjerenu” zaštitu tih podataka drugim odobrenim sredstvima ili vrati ili izbriše sve takve podatke te o tome obavijesti Ministarstvo trgovine) dostavi ispunjen odgovarajući upitnik u kojem potvrđuje što je učinila s tim osobnim podacima, što će učiniti s onima koje je zadržala i tko će u organizaciji biti stalna kontaktna točka za pitanja koja se odnose na Načela.

— Ako je samocertificiranje organizacije isteklo (tj. nije ispunila obvezu godišnjeg ponovnog certificiranja za pridržavanje Načela, a nije ni uklonjena s popisa organizacija uključenih u okvir za privatnost podataka zbog nekog drugog razloga, kao što je povlačenje), Ministarstvo trgovine zatražit će da mu dostavi ispunjen odgovarajući upitnik u kojem potvrđuje želi li se povući ili ponovno certificirati:

  — ako se želi povući, treba dodatno potvrditi što će učiniti s osobnim podacima koje je primila u skladu s okvirom EU-a i SAD-a za privatnost podataka dok je sudjelovala u njemu (vidjeti prethodni opis toga što organizacija mora potvrditi ako se želi povući),

  — ako se namjerava ponovno certificirati, treba dodatno potvrditi da je u razdoblju kad je certifikat istekao primjenjivala Načela na osobne podatke primljene u skladu s okvirom EU-a i SAD-a za privatnost podataka i pojasniti koje će korake poduzeti da riješi otvorena pitanja zbog kojih je odgodila ponovno certificiranje.

— Ako je organizacija uklonjena s popisa organizacija uključenih u okvir za privatnost podataka zbog nekog od sljedećih razloga: (a) povlačenje iz okvira EU-a i SAD-a za privatnost podataka, (b) propust da se dovrši godišnje ponovno certificiranje za pridržavanje Načela (tj. pokrenula je, ali nije pravodobno dovršila postupak godišnjeg ponovnog certificiranja ili ga uopće nije pokrenula), ili (c) „ustrajna neusklađenost”, Ministarstvo trgovine poslat će obavijest kontaktima iz prijave organizacije za samocertificiranje, u kojoj će navesti razlog uklanjanja i objasniti da organizacija mora prestati izravno ili neizravno izjavljivati da sudjeluje u okviru EU-a i SAD-a za privatnost podataka ili da je usklađena s njim te da može primati osobne podatke u skladu s tim okvirom. Obavijest može uključivati i drugi sadržaj povezan s razlogom za uklanjanje, a u njoj će se navesti da organizacije koje lažno prikazuju svoje sudjelovanje u okviru EU-a i SAD-a za privatnost podataka ili usklađenost s njim, među ostalim i ako navode da sudjeluju u tom okviru nakon što su uklonjene s popisa organizacija uključenih u okvir za privatnost podataka, mogu biti predmet provedbenih mjera FTC-a, Ministarstva prometa ili drugog relevantnog vladina tijela.

Traženje i uklanjanje lažnih izjava o sudjelovanju

— Ako se organizacija: (a) povuče iz okvira EU-a i SAD-a za privatnost podataka, (b) ne dovrši godišnje ponovno certificiranje za pridržavanje Načela (tj. pokrenula je, ali nije pravodobno dovršila postupak godišnjeg ponovnog certificiranja ili ga uopće nije pokrenula), (c) ukloni kao sudionica iz okvira EU-a i SAD-a za privatnost podataka, prije svega zbog „ustrajne neusklađenosti”, ili (d) ne pobrine za izvorno samocertificiranje za pridržavanje Načela (tj. pokrenula je, ali nije pravodobno dovršila postupak izvornog samocertificiranja), Ministarstvo trgovine redovito će po službenoj dužnosti provjeravati da relevantne objavljene politike zaštite privatnosti organizacije ne sadržavaju upućivanja na okvir EU-a i SAD-a za privatnost podataka iz kojih bi se moglo zaključiti da sudjeluje u njemu te da može primati osobne podatke u skladu s tim okvirom. Ako Ministarstvo trgovine utvrdi da takva upućivanja postoje, obavijestit će organizaciju da će prema potrebi uputiti predmet relevantnoj agenciji radi mogućeg izricanja provedbene mjere ako organizacija nastavi lažno prikazivati da sudjeluje u okviru EU-a i SAD-a za privatnost podataka. Ministarstvo trgovine obavijestit će organizaciju s pomoću kontaktnih podataka koje mu je ona dostavila ili prema potrebi drugim prikladnim sredstvima. Ako organizacija ne ukloni upućivanja ili ne provede samocertificiranje usklađenosti s okvirom EU-a i SAD-a za privatnost podataka u skladu s postupcima Ministarstva trgovine, to će ministarstvo po službenoj dužnosti uputiti predmet FTC-u, Ministarstvu prometa ili drugoj odgovarajućoj agenciji za provedbu zakona ili će poduzeti druge odgovarajuće mjere za osiguranje primjerene uporabe certifikacijske oznake okvira EU-a i SAD-a za privatnost podataka.

— Ministarstvo trgovine i na druge će načine nastojati otkriti lažne izjave o sudjelovanju u okviru EU-a i SAD-a za privatnost podataka i neprimjerenu uporabu certifikacijske oznake tog okvira, među ostalim i u organizacijama koje za razliku od onih navedenih u prethodnoj točki nisu nikad započele postupak samocertificiranja (npr. pretraživanjem interneta radi provjere upućuje li se u politikama zaštite privatnosti organizacija na okvir EU-a i SAD-a za privatnost podataka). Ako Ministarstvo trgovine na taj način otkrije lažne izjave o sudjelovanju u okviru EU-a i SAD-a za privatnost podataka i neprimjerenu uporabu certifikacijske oznake tog okvira, obavijestit će organizaciju da će prema potrebi uputiti predmet relevantnoj agenciji radi mogućeg izricanja provedbene mjere ako organizacija nastavi lažno prikazivati da sudjeluje u okviru EU-a i SAD-a za privatnost podataka. Ministarstvo trgovine obavijestit će organizaciju s pomoću kontaktnih podataka koje mu je ona dostavila, ako postoje, ili prema potrebi drugim prikladnim sredstvima. Ako organizacija ne ukloni upućivanja ili ne provede samocertificiranje usklađenosti s okvirom EU-a i SAD-a za privatnost podataka u skladu s postupcima Ministarstva trgovine, to će ministarstvo po službenoj dužnosti uputiti predmet FTC-u, Ministarstvu prometa ili drugoj odgovarajućoj agenciji za provedbu zakona ili će poduzeti druge odgovarajuće mjere za osiguranje primjerene uporabe certifikacijske oznake okvira EU-a i SAD-a za privatnost podataka.

— Ministarstvo trgovine odmah će preispitati i riješiti konkretne, ozbiljne pritužbe o lažnim izjavama o sudjelovanju u okviru EU-a i SAD-a za privatnost podataka koje zaprimi (npr. pritužbe koje dostave tijela za zaštitu podataka, neovisni mehanizmi pravne zaštite koje pružaju tijela za alternativno rješavanje sporova iz privatnog sektora, ispitanici, europska i američka poduzeća i druge vrste trećih strana).

— Ministarstvo trgovine može poduzeti druge odgovarajuće korektivne mjere. Lažno prikazivanje Ministarstvu trgovine kažnjivo je u skladu sa Zakonom o davanju lažnog iskaza (*False Statements Act*, glava 18. članak 1001. Zakonika SAD-a).

Provedba periodičnih preispitivanja usklađenosti po službenoj dužnosti i ocjena programa za okvir za privatnost podataka

— Ministarstvo trgovine redovito će pratiti postupaju li organizacije uključene u okvir EU-a i SAD-a za privatnost podataka stvarno u skladu s okvirom kako bi utvrdilo jesu li za neka pitanja potrebne daljnje mjere. Osobito će po službenoj dužnosti provoditi redovite terenske provjere nasumično odabranih organizacija uključenih u okvir EU-a i SAD-a za privatnost podataka i ad hoc terenske provjere određenih organizacija uključenih u taj okvir kad se utvrde mogući problemi s usklađenosti (npr. ako Ministarstvo trgovine o njima obavijeste treće strane) kako bi provjerilo: (a) jesu li dostupne kontaktne točke odgovorne za rješavanje pritužbi, zahtjeva za pristup i ostalih pitanja povezanih s okvirom EU-a i SAD-a za privatnost podataka, (b) prema potrebi, je li javna politika zaštite privatnosti organizacije lako dostupna na njezinim javnim internetskim stranicama i na poveznici s popisa organizacija uključenih u okvir za privatnost podataka, (c) je li politika zaštite privatnosti organizacije i dalje u skladu sa zahtjevima za samocertificiranje opisanima u Načelima, i (d) je li neovisni mehanizam pravne zaštite koji je organizacija odabrala dostupan za rješavanje pritužbi podnesenih u skladu s okvirom EU-a i SAD-a za privatnost podataka. Ministarstvo trgovine aktivno će pratiti i navode li se u vijestima uvjerljivi dokazi o neusklađenosti organizacija uključenih u okvir EU-a i SAD-a za privatnost podataka.

— Ministarstvo trgovine u okviru preispitivanja usklađenosti zahtijevat će da mu organizacija uključena u okvir EU-a i SAD-a za privatnost podataka dostavi ispunjen detaljni upitnik ako: (a) Ministarstvo trgovine primi konkretne, ozbiljne pritužbe o usklađenosti organizacije s Načelima, (b) organizacija ne odgovori na zadovoljavajući način na upite Ministarstva trgovine o informacijama u vezi s okvirom EU-a i SAD-a za privatnost podataka, ili (c) postoje uvjerljivi dokazi da organizacija ne ispunjava svoje obveze u skladu s okvirom EU-a i SAD-a za privatnost podataka. Ako Ministarstvo trgovine pošalje takav detaljan upitnik organizaciji, a ona ne odgovori na njega na zadovoljavajući način, obavijestit će je da će prema potrebi uputiti predmet relevantnoj agenciji radi mogućeg izricanja provedbene mjere ako mu organizacija pravodobno ne dostavi zadovoljavajući odgovor. Ministarstvo trgovine obavijestit će organizaciju s pomoću kontaktnih podataka koje mu je ona dostavila ili prema potrebi drugim prikladnim sredstvima. Ako organizacija pravodobno ne dostavi zadovoljavajući odgovor, Ministarstvo trgovine po službenoj će dužnosti uputiti predmet FTC-u, Ministarstvu prometa ili drugoj odgovarajućoj agenciji za provedbu zakona ili će poduzeti druge odgovarajuće mjere za osiguranje usklađenosti. Ministarstvo trgovine prema potrebi se o takvim preispitivanjima usklađenosti savjetuje s tijelima za zaštitu podataka.

— Ministarstvo trgovine periodično će preispitivati upravljanje programom za okvir za privatnost podataka i njegov nadzor kako bi se pobrinulo za to da je praćenje koje provodi, među ostalim primjenom alata za pretraživanje (npr. radi provjere funkcioniraju li poveznice na politike zaštite privatnosti organizacija uključenih u okvir EU-a i SAD-a za privatnost podataka), prikladno za rješavanje postojećih i novih problema.

Prilagođavanje internetskih stranica okvira za privatnost podataka ciljanoj publici

Ministarstvo trgovine prilagodit će internetske stranice okvira za privatnost podataka sljedećoj ciljanoj publici: pojedincima i poduzećima iz EU-a, američkim poduzećima te tijelima za zaštitu podataka. Uključivanje materijala izravno usmjerenih na pojedince i poduzeća iz EU-a na različite će načine olakšati transparentnost. Na internetskim će se stranicama pojedincima iz EU-a jasno objasniti: 1. prava koja im pruža okvir EU-a i SAD-a za privatnost podataka, 2. mehanizmi pravne zaštite koji su im dostupni kad smatraju da je organizacija povrijedila svoju obvezu postupanja u skladu s Načelima, i 3. kako pronaći informacije koje se odnose na samocertificiranje organizacije za sudjelovanje u okviru EU-a i SAD-a za privatnost podataka. Poduzeća iz EU-a lakše će moći provjeriti: 1. sudjeluje li organizacija u okviru EU-a i SAD-a za privatnost podataka, 2. vrste informacija obuhvaćene samocertificiranjem organizacije za sudjelovanje u okviru EU-a i SAD-a za privatnost podataka, 3. politiku zaštite privatnosti koja se primjenjuje na obuhvaćene informacije, i 4. metodu koju organizacija upotrebljava za provjeru svojeg pridržavanja Načela. Američkim će se poduzećima jasno objasniti: 1. pogodnosti sudjelovanja u okviru EU-a i SAD-a za privatnost podataka, 2. način na koji se mogu uključiti u okvir EU-a i SAD-a za privatnost podataka, ponovno certificirati i povući iz tog okvira, i 3. način na koji SAD upravlja okvirom EU-a i SAD-a za privatnost podataka i provodi taj okvir. Uključivanje materijala izravno usmjerenih na tijela za zaštitu podataka (npr. informacije o kontaktnoj točki Ministarstva trgovine za tijela za zaštitu podataka i poveznica na sadržaj povezan s Načelima na internetskim stranicama FTC-a) olakšat će suradnju i transparentnost. Ministarstvo trgovine na *ad hoc* osnovi surađivat će s Komisijom i Europskim odborom za zaštitu podataka (EDPB) na izradi dodatnih, tematskih materijala (npr. odgovori na često postavljena pitanja) koji će se upotrebljavati na internetskim stranicama okvira za privatnost podataka ako bi takve informacije pridonijele učinkovitom upravljanju programom za okvir za privatnost podataka i njegovu nadzoru.

Olakšavanje suradnje s tijelima za zaštitu podataka

Kako bi se povećale prilike za suradnju s tijelima za zaštitu podataka, Ministarstvo trgovine uspostavit će posebnu kontaktnu točku za vezu s tim tijelima. U slučajevima kad tijelo za zaštitu podataka smatra da organizacija uključena u okvir EU-a i SAD-a za privatnost podataka ne postupa u skladu s Načelima, među ostalim na temelju pritužbe pojedinca iz EU-a, to će se tijelo moći obratiti posebnoj kontaktnoj točki u Ministarstvu trgovine koje će uputiti organizaciju na daljnje preispitivanje. Ministarstvo trgovine nastojat će olakšati rješavanje pritužbe s organizacijom uključenom u okvir EU-a i SAD-a za privatnost podataka. U roku od 90 dana od primitka pritužbe obavijestit će tijelo za zaštitu podataka o napretku. Posebna kontaktna točka primat će i sve upućene predmete o organizacijama koje iznose lažne izjave o sudjelovanju u okviru EU-a i SAD-a za privatnost podataka. Pratit će sve predmete koje tijela za zaštitu podataka upute Ministarstvu trgovine, a to će ministarstvo u godišnje preispitivanje koje je opisano u nastavku uključiti izvješće s analizom ukupnog broja pritužbi koje zaprima svake godine. Pomagat će tijelima za zaštitu podataka koja traže informacije o samocertificiranju određene organizacije ili njezinu prethodnom sudjelovanju u okviru EU-a i SAD-a za privatnost podataka i odgovarati na upite tih tijela u vezi s provedbom posebnih zahtjeva okvira EU-a i SAD-a za privatnost podataka. Ministarstvo trgovine surađivat će s Komisijom i EDPB-om na postupovnim i administrativnim aspektima odbora tijela za zaštitu podataka, među ostalim na uspostavljanju prikladnih postupaka za raspodjelu sredstava prikupljenih naplatom naknade za taj odbor. Razumijemo da će Komisija surađivati s Ministarstvom trgovine da olakša rješavanje eventualnih poteškoća koje se pojave u vezi s tim postupcima. Osim toga, Ministarstvo trgovine tijelima za zaštitu podataka dostavit će materijale o okviru EU-a i SAD-a za privatnost podataka koje će ta tijela uključiti na svoje internetske stranice u cilju povećanja transparentnosti za pojedince i poduzeća iz EU-a. Informiranost o okviru EU-a i SAD-a za privatnost podataka i pravima i odgovornostima koji iz njega proizlaze trebala bi olakšati prepoznavanje problema čim nastanu kako bi ih se na odgovarajući način riješilo.

Ispunjavanje obveza iz Priloga I. Načelima

Ministarstvo trgovine ispunit će svoje obveze iz Priloga I. Načelima, među ostalim u pogledu vođenja popisa arbitara koje zajedno s Komisijom bira na temelju neovisnosti, integriteta i stručnosti te će prema potrebi poduprijeti treću stranu koju je odabralo za vođenje arbitraža u skladu s Prilogom I. Načelima i za upravljanje arbitražnim fondom utvrđenim u tom prilogu ([3]). Ministarstvo trgovine surađivat će s trećom stranom među ostalim kako bi provjerilo održava li ona internetske stranice sa smjernicama o postupku arbitraže, uključujući: 1. način na koji se pokreću postupci i dostavljaju dokumenti, 2. popis arbitara koji vodi Ministarstvo trgovine i način na koji se biraju arbitri s tog popisa, 3. arbitražne postupke koji su na snazi i kodeks ponašanja za arbitre koji su donijeli Ministarstvo trgovine i Komisija ([4]), i 4. prikupljanje i plaćanje naknade za arbitre. Nadalje, Ministarstvo trgovine surađivat će s trećom stranom na periodičnom preispitivanju funkcioniranja arbitražnog fonda, uključujući preispitivanje potrebe da se prilagodi iznos doprinosa ili gornjih granica (najvećih iznosa) troškova arbitraže, i uzeti u obzir, među ostalim, broj provedenih arbitražnih postupaka te njihove troškove i rokove, pri čemu se podrazumijeva da to neće uključivati pretjerano financijsko opterećenje za organizacije uključene u okvir EU-a i SAD-a za privatnost podataka. Ministarstvo trgovine obavijestit će Komisiju o ishodu takvih preispitivanja s trećom stranom i dostaviti joj prethodnu obavijest o eventualnim prilagodbama iznosa doprinosa.

Zajedničko preispitivanje funkcioniranja okvira EU-a i SAD-a za privatnost podataka

Ministarstvo trgovine i prema potrebi druge agencije održavat će redovite sastanke s Komisijom, zainteresiranim tijelima za zaštitu podataka i odgovarajućim predstavnicima EDPB-a na kojima će ih Ministarstvo trgovine obavješćivati o napretku okvira EU-a i SAD-a za privatnost podataka. Na sastancima će se raspravljati o aktualnim pitanjima povezanima s funkcioniranjem, provedbom, nadzorom i ostvarivanjem programa za okvir za privatnost podataka. Na sastancima se prema potrebi može raspravljati o povezanim temama, kao što su drugi mehanizmi za prijenos podataka na koje se primjenjuju zaštitne mjere u skladu s okvirom EU-a i SAD-a za privatnost podataka.

([3]) Ministarstvo trgovine odabralo je Međunarodni centar za rješavanje sporova (ICDR) Američkog udruženja za arbitražu (AAA) za vođenje arbitraža u skladu s Prilogom I. Načelima i za upravljanje arbitražnim fondom utvrđenim u tom prilogu.

([4]) Ministarstvo trgovine i Komisija dogovorili su se 15. rujna 2017. da će donijeti propise o arbitraži kojima se uređuju obvezujući arbitražni postupci opisani u Prilogu I. Načelima te kodeks ponašanja za arbitre koji je u skladu s općeprihvaćenim etičkim normama za trgovačke arbitre i s Prilogom I. Načelima. Dogovorili su se da će prilagoditi propise o arbitraži i kodeks ponašanja kako bi bili u skladu s ažuriranim okvirom EU-a i SAD-a za privatnost podataka, a Ministarstvo trgovine i Međunarodni centar za rješavanje sporova Američkog udruženja za arbitražu zajedno će ih ažurirati.

Ažuriranje zakonâ

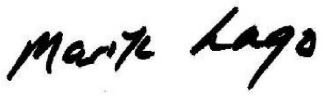
Ministarstvo trgovine u razumnoj će mjeri nastojati obavijestiti Komisiju o bitnim promjenama američkog prava koje su relevantne za okvir EU-a i SAD-a za privatnost podataka u području zaštite privatnosti podataka te o ograničenjima i zaštitnim mjerama koji se primjenjuju na pristup američkih tijela osobnim podacima i njihovu daljnju uporabu.

Pristup američke vlade osobnim podacima

SAD je objavio Izvršni nalog br. 14086 o poboljšanju zaštitnih mjera u američkim aktivnostima elektroničkog izviđanja, i glavu 28. članak 201. Kodeksa saveznih propisa o izmjeni propisa Ministarstva pravosuđa radi osnivanja Žalbenog suda za zaštitu podataka (Data Protection Review Court – DPRC), kojima se osigurava visok stupanj zaštite osobnih podataka kad je riječ o pristupu vlade tim podacima u svrhe nacionalne sigurnosti. Ta zaštita uključuje jačanje zaštitnih mjera u pogledu privatnosti i građanskih sloboda kako bi se osigurala nužnost i proporcionalnost američkih aktivnosti elektroničkog izviđanja za ostvarenje utvrđenih ciljeva u području nacionalne sigurnosti, uspostavu novog neovisnog mehanizma pravne zaštite koji ima obvezujuće ovlasti i poboljšanje postojećeg strogog i višerazinskog nadzora američkih aktivnosti elektroničkog izviđanja. Pojedinci iz EU-a zahvaljujući tim oblicima zaštite mogu tražiti pravnu zaštitu u okviru novog višerazinskog mehanizma koji uključuje neovisni DPRC, koji će biti sastavljen od odabranih pojedinaca koji nisu dio američke vlade i imaju pune ovlasti odlučivanja o zahtjevima i prema potrebi izricanja korektivnih mjera. Ministarstvo trgovine vodit će evidenciju pojedinaca iz EU-a koji podnesu pritužbu koja ispunjava uvjete u skladu s Izvršnim nalogom br. 14086 i glavom 28. člankom 201. Kodeksa saveznih propisa. Pet godina nakon ovog dopisa i svakih pet godina nakon toga Ministarstvo trgovine kontaktirat će s relevantnim agencijama kako bi provjerilo jesu li informacije koje se odnose na preispitivanje pritužbi koje ispunjavaju uvjete ili na molbe za preispitivanje podnesene DPRC-u deklasificirane. Ako jesu, Ministarstvo trgovine surađivat će s relevantnim tijelom za zaštitu podataka da o tome obavijesti pojedinca iz EU-a. Ta poboljšanja potvrđuju da će se s osobnim podacima iz EU-a prenesenima u SAD postupati na način koji je u skladu s pravnim zahtjevima EU-a kad je riječ o vladinu pristupu podacima.

Na temelju Načela, Izvršnog naloga br. 14086, glave 28. članka 201. Kodeksa saveznih propisa te popratnih dopisa i materijala, uključujući obveze koje je Ministarstvo trgovine preuzelo u pogledu upravljanja programom za okvir za privatnost podataka i njegova nadzora, očekujemo da će Komisija utvrditi da okvir EU-a i SAD-a za privatnost podataka osigurava primjerenu razinu zaštite za potrebe prava EU-a i da će se podaci iz Europske unije nastaviti prenositi organizacijama koje sudjeluju u tom okviru. Očekujemo i da će uvjeti tih dogovora olakšati prijenos podataka američkim organizacijama u skladu sa standardnim ugovornim klauzulama EU-a ili obvezujućim korporativnim pravilima EU-a.

S poštovanjem



Marisa LAGO

PRILOG IV.

SJEDINJENE AMERIČKE DRŽAVE
Savezna trgovinska komisija
WASHINGTON, D.C. 20580

Ured predsjednice

9. lipnja 2023.

Didier Reynders
Povjerenik za pravosuđe
Europska komisija
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgija

Poštovani povjereniče Reynders,

Savezna trgovinska komisija Sjedinjenih Američkih Država (FTC) zahvaljuje na prilici da objasni svoju provedbenu ulogu u vezi s Načelima okvira EU-a i SAD-a za privatnost podataka. FTC je već dugo posvećen prekograničnoj zaštiti potrošača i privatnosti te provedbi aspekata tog okvira povezanih s trgovinskim sektorom. Od 2000. obavlja tu ulogu u vezi s okvirom EU-a i SAD-a „sigurne luke", a u novije vrijeme, odnosno od 2016., u vezi s okvirom europsko-američkog sustava zaštite privatnosti ([1]). Sud Europske Unije („Sud") 16. srpnja 2020. proglasio je nevaljanom odluku Europske komisije o primjerenosti na kojoj se temeljio okvir europsko-američkog sustava zaštite privatnosti zbog razloga koji nisu povezani s trgovačkim načelima za čiju je provedbu FTC zadužen. SAD i Europska komisija u međuvremenu su uspostavili dogovor o novom okviru EU-a i SAD-a za privatnost podataka u kojem se uvažava ta presuda Suda.

Ovim putem želim potvrditi predanost FTC-a odlučnoj provedbi Načela okvira EU-a i SAD-a za privatnost podataka. Posebno potvrđujemo predanost trima ključnim područjima, a to su: 1. davanje prednosti upućenim predmetima i istrage, 2. ishođenje i praćenje naloga, i 3. suradnja u području provedbe s tijelima za zaštitu podataka iz EU-a.

I. **Uvod**

a. **Osiguranje provedbe privatnosti i rad u području politike FTC-a**

FTC ima široke građanske provedbene ovlasti promicanja zaštite potrošača i tržišnog natjecanja u području trgovine. U okviru svojeg mandata zaštite potrošača FTC provodi brojne zakone za zaštitu privatnosti i sigurnosti potrošača i njihovih podataka. Glavnim zakonom koji FTC provodi, Zakonom o FTC-u, zabranjuje se „nepošteno" ili „prijevarno" postupanje ili

([1]) Dopis predsjednice FTC-a Edith Ramirez povjerenici Europske komisije za pravosuđe, zaštitu potrošača i ravnopravnost spolova Věri Jourovoj, u kojem je opisano kako Savezna trgovinska komisija provodi novi okvir europsko-američkog sustava zaštite privatnosti (29. veljače 2016.), dostupan na https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. FTC se prethodno obvezao i na provedbu europsko-američkog programa „sigurne luke". Dopis predsjednika FTC-a Roberta Pitofskyja direktoru GU-a Europske komisije za unutarnje tržište Johnu Moggu (14. srpnja 2000.), dostupan na: https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Ovim se dopisom zamjenjuju te ranije preuzete obveze.

praksa u trgovini ili koji utječu na trgovinu ([2]). FTC provodi i ciljane zakone kojima se štite informacije o zdravlju, kreditnoj sposobnosti i drugim financijskim pitanjima te informacije o djeci na internetu i donio je propise o provedbi svakog od njih ([3]).

FTC u posljednje vrijeme provodi i brojne inicijative za poboljšanje zaštite privatnosti. U kolovozu 2022. najavio je da radi na izradi propisa za obračunavanje sa štetnom praksom u području komercijalnog nadzora i nedovoljnom razinom sigurnosti podataka ([4]). Cilj je projekta sastaviti pouzdanu javnu evidenciju na temelju koje će se odlučiti treba li FTC izdati propise koji se odnose na praksu u području komercijalnog nadzora i sigurnosti podataka te kako bi ti propisi potencijalno trebali izgledati. Pozdravljamo komentare dionika iz EU-a o toj i drugim inicijativama.

Vodeći istraživači i dalje sudjeluju na našim konferencijama o privatnosti pod nazivom „PrivacyCon" kako bi raspravljali o najnovijim istraživanjima i trendovima povezanima sa zaštitom privatnosti potrošača i sigurnosti podataka. Povećali smo i sposobnost svoje agencije da održi korak s razvojem tehnologije na kojem je utemeljena većina našeg rada u području zaštite privatnosti te kontinuirano povećavamo svoj tim tehnoloških stručnjaka i interdisciplinarnih istraživača. Kao što znate, najavili smo dijalog s Vama i Vašim kolegama u Europskoj komisiji, što uključuje razmatranje tema povezanih s privatnošću, kao što su sučelja osmišljena da prevare korisnike (*dark patterns*) i poslovni modeli koje karakterizira kontinuirano prikupljanje podataka ([5]). Nedavno smo objavili i izvješće Kongresu u kojem upozoravamo na opasnosti povezane s uporabom umjetne inteligencije za suzbijanje prijetnji na internetu koje je utvrdio Kongres. U tom se izvješću upozorava na netočnost, pristranost, diskriminaciju i sve veću raširenost komercijalnog nadzora ([6]).

b. **Oblici pravne zaštite u SAD-u koji koriste potrošačima iz EU-a**

Okvir EU-a i SAD-a za privatnost podataka dio je šireg okoliša zaštite privatnosti u kojem su i potrošači iz EU-a zaštićeni na brojne načine. Zabrana nepoštenog ili prijevarnog postupanja ili prakse iz Zakona o FTC-u nije ograničena na zaštitu američkih potrošača od američkih poduzeća jer uključuje praksu 1. zbog koje nastaje ili bi mogla nastati razumno predvidiva šteta u SAD-u ili 2. koja uključuje postupanje u SAD-u kojim se krši ta zabrana. Nadalje, FTC za zaštitu stranih potrošača može upotrijebiti sva pravna sredstva dostupna za zaštitu domaćih potrošača ([7]).

FTC provodi i druge ciljane zakone kojima se štite i potrošači izvan SAD-a, kao što je Zakon o zaštiti privatnosti djece na internetu (*Children's Online Privacy Protection Act* – COPPA). Tim je zakonom propisano, među ostalim, da operateri internetskih stranica i internetskih usluga usmjerenih na djecu ili stranica za opću publiku koji svjesno prikupljaju osobne informacije od djece mlađe od 13 godine moraju obavijestiti roditelje o tome i zatražiti njihovu provjerljivu suglasnost. Američke internetske stranice i usluge na koje se primjenjuje taj zakon i koje prikupljaju podatke od djece iz inozemstva

([2]) Glava 15. članak 45. točka (a) Zakonika SAD-a. FTC nije nadležan za kazneni progon ni za pitanja nacionalne sigurnosti. FTC ne može utjecati ni na većinu drugih vladinih mjera. Nadalje, postoje iznimke od nadležnosti FTC-a u području tržišnih aktivnosti, među ostalim u odnosu na banke, zračne prijevoznike, djelatnost osiguranja i zajedničke operaterske aktivnosti pružatelja telekomunikacijskih usluga. FTC nije nadležan ni za većinu neprofitnih organizacija, ali jest za lažne dobrotvorne ili druge neprofitne organizacije koje zapravo ostvaruju dobit. FTC je nadležan i za neprofitne organizacije koje posluju kako bi njihovi članovi ostvarili dobit, među ostalim osiguravanjem znatne gospodarske koristi tim članovima. Nadležnost FTC-a u nekim se slučajevima preklapa s nadležnošću drugih agencija kaznenog progona. Imamo dobru suradnju sa saveznim i državnim tijelima te blisko surađujemo s njima u koordinaciji istraga ili prema potrebi u upućivanju predmeta.

([3]) Vidjeti smjernice FTC-a o privatnosti i sigurnosti, https://www.ftc.gov/business-guidance/privacy-security.

([4]) V*idjeti* priopćenje za medije „FTC razmatra uvođenje propisa za obračunavanje sa štetnim praksama komercijalnog nadzora i nedovoljnom razinom sigurnosti podataka" (11. kolovoza 2022.) https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices

([5]) V*idjeti* zajedničku izjavu za medije Didiera Reyndersa, povjerenika Europske komisije za pravosuđe, i Lise Khan, predsjednice američke Savezne trgovinske komisije (30. ožujka 2022.), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) V*idjeti* priopćenje za medije „FTC u svojem izvješću upozorava na opasnosti uporabe umjetne inteligencije za rješavanje problema na internetu" (16. lipnja 2022.), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) Glava 15. članak 45. točka (a)(4)(B) Zakonika SAD-a. Nadalje, pojam „nepošteno ili prijevarno postupanje ili praksa" uključuje postupanje ili praksu i. zbog kojih nastaje ili bi mogla nastati razumno predvidiva šteta u SAD-u ili ii. koje uključuju postupanje u SAD-u kojim se krši zabrana takvog postupanja (glava 15. članak 45. točka (a)(4)(A) Zakonika SAD-a).

moraju postupati u skladu s njim. Internetske stranice i usluge iz inozemstva moraju postupati u skladu s tim zakonom ako su usmjerene na djecu u SAD-u ili ako svjesno prikupljaju osobne informacije od tamošnje djece. Nadalje, osim američkih saveznih zakona koje provodi FTC, potrošačima iz EU-a mogu se osigurati dodatne pogodnosti na temelju drugih saveznih i državnih zakona o zaštiti potrošača, povredi podataka i zaštiti privatnosti.

c. **Provedbene aktivnosti FTC-a**

FTC je pokretao postupke u skladu s europsko-američkim okvirom „sigurne luke" i europsko-američkim okvirom za sustav zaštite privatnosti, a nastavio je provoditi potonji i nakon što je Sud proglasio nevaljanom odluku o primjerenosti na kojoj je taj sustav bio utemeljen ([8]). U nekoliko novijih pritužbi koje je FTC zaprimio navodi se da su poduzeća povrijedila odredbe europsko-američkog sustava zaštite privatnosti, među ostalim u postupcima protiv poduzeća Twitter ([9]), CafePress ([10]) i Flo ([11]). FTC je u provedbenim mjerama protiv Twittera od tog poduzeća osigurao iznos od 150 milijuna USD zbog povrede ranijeg naloga FTC-a postupcima koji su utjecali na više od 140 milijuna klijenata, među ostalim povredom načela br. 5. (cjelovitost podataka i ograničavanje svrhe) europsko-američkog sustava zaštite privatnosti. Nadalje, tim se nalogom od Twittera zahtijeva da dopusti korisnicima primjenu sigurnih metoda višerazinske autentifikacije za koje nije potreban telefonski broj.

FTC je u predmetu *CafePress* naveo da to poduzeće nije zaštitilo osjetljive podatke potrošača, da je zataškalo ozbiljan slučaj povrede podataka i povrijedilo načela br. 2 (izbor), br. 4 (sigurnost) i br. 6 (pristup) sustava zaštite privatnosti. U nalogu FTC-a od poduzeća se zahtijeva da zamijeni neprikladne mjere autentifikacije višerazinskom autentifikacijom, znatno ograniči količinu podataka koje prikuplja i zadržava, šifrira brojeve socijalnog osiguranja te da treća strana ocijeni njegove programe u području informacijske sigurnosti i dostavi FTC-u primjerak koji se može objaviti.

FTC je u predmetu *Flo* naveo da je aplikacija za praćenje plodnih dana podijelila zdravstvene informacije korisnika s trećom stranom koja pruža usluge analize podataka, iako se obvezala na čuvanje privatnosti tih informacija. U pritužbi FTC-a konkretno je navedeno da je poduzeće Flo poslovalo s potrošačima iz EU-a i povrijedilo načela br. 1 (obavijest), br. 2 (izbor), br. 3 (odgovornost za daljnji prijenos) i br. 5 (cjelovitost podataka i ograničavanje svrhe) europsko-američkog sustava zaštite privatnosti. Nalogom FTC-a od poduzeća Flo među ostalim se zahtijeva da obavijesti korisnike čije su osobne informacije otkrivene i naloži trećoj strani koja je primila zdravstvene informacije korisnika da uništi te podatke. Važno je istaknuti da se nalozima FTC-a štite svi potrošači u cijelom svijetu koji posluju s američkim poduzećem, a ne samo oni koji su podnijeli pritužbe.

Brojni predmeti u kojima su izrečene provedbene mjere u vezi s europsko-američkim okvirom „sigurne luke" i europsko-američkim sustavom zaštite privatnosti u prošlosti su uključivali organizacije koje su se izvorno samocertificirale Ministarstvu trgovine, ali nisu provele godišnje ponovno samocertificiranje, a nastavile su se predstavljati kao članice. Drugi predmeti odnosili su se na lažne izjave o sudjelovanju organizacija koje se nikad nisu izvorno samocertificirale Ministarstvu trgovine. Očekujemo da ćemo u budućnosti usmjeriti provedbene mjere na vrste materijalnih povreda Načela okvira EU-a i SAD-a za privatnost podataka na koje se odnose predmeti kao što su Twitter, CafePress i Flo. Ministarstvo trgovine u međuvremenu će upravljati programom za postupak samocertificiranja i nadzirati ga, voditi obvezujući popis organizacija sudionica okvira EU-a i SAD-a za privatnost podataka i posvetiti se drugim pitanjima povezanima s izjavama o sudjelovanju u programu ([12]). Važno je istaknuti da će organizacije koje izjave da sudjeluju u okviru EU-a i SAD-a za privatnost podataka možda morati osigurati materijalnu provedbu Načela tog okvira čak i ako se ne uspiju samocertificirati ili ponovno samocertificirati Ministarstvu trgovine.

([8]) Vidjeti Prilog A za popis predmeta koje je FTC pokrenuo u skladu s okvirom „sigurne luke" i sustava zaštite privatnosti.

([9]) *Vidjeti* priopćenje za medije „FTC optužio Twitter za prijevarnu uporabu sigurnosnih podataka računa za prodaju ciljanih oglasa" (25. svibnja 2022.), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) *Vidjeti* priopćenje za medije „FTC pokrenuo postupak protiv CafePressa zbog pokušaja zataškavanja povrede podataka" (15. ožujka 2022.), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) *Vidjeti* priopćenje za medije „FTC izdao nalog u postupku protiv aplikacije za praćenje plodnih dana Flo Health koja je dijelila osjetljive podatke s Facebookom, Googleom i drugima" (22. lipnja 2021.), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Dopis Marise Lago, zamjenice američke ministrice za međunarodnu trgovinu, Didieru Reyndersu, povjereniku Europske komisije za pravosuđe (12. prosinca 2022.).

II. **Davanje prednosti upućenim predmetima i istrage**

Jednako kao u slučaju europsko-američkog okvira „sigurne luke" i europsko-američkog sustava zaštite privatnosti, FTC se obvezuje da će dati prednost predmetima povezanima s Načelima okvira EU-a i SAD-a za privatnost podataka koje su uputili Ministarstvo trgovine i države članice EU-a. Dat ćemo prednost i razmatranju predmeta o neusklađenosti s Načelima okvira EU-a i SAD-a za privatnost podataka koje su nam uputile samoregulatorne organizacije za zaštitu privatnosti i druga neovisna tijela za rješavanje sporova.

Kako bi olakšao upućivanja predmeta iz država članica EU-a u skladu s okvirom EU-a i SAD-a za privatnost podataka, FTC je uveo standardizirani postupak upućivanja i objavio smjernice državama članicama EU-a o vrsti informacija koje bi mu najviše koristile u istrazi upućenog predmeta. U tu je svrhu odredio kontaktnu točku u agenciji kojoj države članice EU-a mogu upućivati predmete. Najkorisnije je kad tijelo koje upućuje predmet prethodno istraži navodnu povredu i može surađivati s FTC-om u istrazi.

Po primitku takvog upućenog predmeta od Ministarstva trgovine, države članice EU-a ili samoregulatorne organizacije ili drugih neovisnih tijela za rješavanje sporova FTC može poduzeti niz mjera za rješavanje navedenih problema. Na primjer, možemo preispitati politike zaštite privatnosti organizacije, pribaviti dodatne informacije izravno od organizacije ili od trećih strana, konzultirati se s tijelom koje je uputilo predmet, ocijeniti postoji li obrazac povreda i je li pogođen velik broj potrošača, utvrditi odnose li se upućeni predmeti na pitanja u nadležnosti Ministarstva trgovine, ocijeniti bi li bilo korisno dodatno obavijestiti sudionike na tržištu i prema potrebi pokrenuti ovršni postupak.

Osim davanja prednosti predmetima povezanima s Načelima okvira EU-a i SAD-a za privatnost podataka koje su uputili Ministarstvo trgovine, države članice EU-a i samoregulatorne organizacije za zaštitu privatnosti ili druga neovisna tijela za rješavanje sporova ([13]), FTC će nastaviti istraživati bitne povrede tih načela uporabom raznih sredstava, prema potrebi na vlastitu inicijativu. FTC u okviru svojeg programa za istragu pitanja zaštite privatnosti i sigurnosti koja uključuju komercijalne organizacije redovito ispituje je li predmetni subjekt davao izjave u pogledu europsko-američkog sustava zaštite privatnosti. Ako jest i ako su se istragom utvrdile očite povrede Načela europsko-američkog sustava zaštite privatnosti, FTC je u svoje provedbene mjere uključivao navode o povredama tih načela. Nastavit ćemo primjenjivati taj proaktivni pristup i na Načela okvira EU-a i SAD-a za privatnost podataka.

III. **Ishođenje i praćenje naloga**

FTC potvrđuje i svoju obvezu da će ishoditi i pratiti provedbene naloge kako bi osigurao usklađenost s Načelima okvira EU-a i SAD-a za privatnost podataka. Zahtijevat ćemo usklađenost s tim načelima na temelju niza odgovarajućih odredbi o sudskim nalozima u budućim nalozima FTC-a u vezi s Načelima okvira EU-a i SAD-a za privatnost podataka. Za povrede upravnih naloga FTC-a mogu se izreći građanskopravne sankcije i naplatiti kazne do 50 120 USD po povredi ili po danu za trajne povrede ([14]), što može iznositi milijune dolara u slučaju prakse koja utječe na brojne potrošače. Svaki ukaz o suglasnosti sadržava i odredbe o izvješćivanju i usklađenosti. Subjekti na koje se ukaz odnosi moraju na određeni broj godina zadržati dokumente kojima dokazuju usklađenost. Ukazi se moraju dostaviti i zaposlenicima koji su odgovorni za osiguravanje usklađenosti s ukazom.

FTC sustavno prati usklađenost s postojećim nalozima u pogledu Načela europsko-američkog sustava zaštite privatnosti, što čini sa svim svojim nalozima, te prema potrebi poduzima mjere za njihovu provedbu ([15]). Važno je istaknuti da će se nalozima FTC-a i dalje štititi svi potrošači u cijelom svijetu koji posluju s poduzećem, a ne samo oni koji su podnijeli pritužbe. Naposljetku, FTC će na internetu voditi popis poduzeća na koja se primjenjuju nalozi povezani s provedbom Načela okvira EU-a i SAD-a za privatnost podataka ([16]).

([13]) Iako FTC ne rješava pojedinačne pritužbe potrošača niti u njima posreduje, potvrđuje da će davati prednost predmetima povezanima s Načelima okvira EU-a i SAD-a za privatnost podataka koje su uputila tijela za zaštitu podataka iz EU-a. Osim toga, FTC upotrebljava pritužbe u svojoj bazi podataka o potrošačima „Consumer Sentinel", kojoj mogu pristupiti brojne druge agencije kaznenog progona, kako bi utvrdio trendove i odredio prioritete za provedbu te utvrdio moguće predmete istrage. Pojedinci iz EU-a za podnošenje pritužbe FTC-u mogu upotrijebiti isti sustav koji je dostupan američkim potrošačima na https://reportfraud.ftc.gov/. Međutim, za pojedinačne pritužbe u pogledu Načela okvira EU-a i SAD-a za privatnost podataka pojedincima iz EU-a najkorisnije bi bilo podnijeti pritužbe tijelu za zaštitu privatnosti u njihovoj državi članici ili neovisnom tijelu za rješavanje sporova.

([14]) Glava 15. članak 45. točka (m) Zakonika SAD-a; glava 16. članak 1.98. Kodeksa saveznih propisa. Taj se iznos periodično prilagođava s obzirom na inflaciju.

([15]) FTC je prošle godine donio odluku o pojednostavnjenju postupka istrage višestrukih prijestupnika. *Vidjeti* priopćenje za medije „FTC odobrio istragu ključnih prioriteta za tijela kaznenog progona" (1. srpnja 2021.), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Vidjeti* europsko-američki sustav zaštite privatnosti, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Suradnja u području provedbe s tijelima za zaštitu podataka iz EU-a**

FTC prepoznaje važnu ulogu koju tijela za zaštitu podataka iz EU-a mogu imati u pogledu usklađenosti s Načelima okvira EU-a i SAD-a za privatnost podataka i poziva ih da produbе suradnju u području savjetovanja i provedbe. Sve je važnije koordinirano pristupiti problemima koji nastaju zbog razvoja digitalnog tržišta i poslovnih modela u kojima se upotrebljavaju velike količine podataka. FTC će u skladu sa zakonima o povjerljivosti i ograničenjima razmjenjivati informacije o upućenim predmetima s tijelima kaznenog progona koja su ih uputila, među ostalim o statusu upućenih predmeta. Ako je to izvedivo s obzirom na broj i vrstu zaprimljenih upućenih predmeta, dostavljene informacije sadržavat će evaluaciju upućenih pitanja, uključujući opis važnih postavljenih pitanja i mjera poduzetih za otklanjanje povreda zakona u nadležnosti FTC-a. FTC će tijelu koje je uputilo predmet dostaviti i povratne informacije o vrstama zaprimljenih upućenih predmeta kako bi se što djelotvornije suzbilo nezakonito postupanje. Ako tijelo koje je uputilo predmet želi znati koji je status određenog upućenog predmeta u svrhu vlastitih postupaka provedbe, FTC će odgovoriti uzimajući u obzir broj upućenih predmeta koje razmatra, uz primjenu zahtjeva povjerljivosti i ostalih pravnih zahtjeva.

FTC će pružati pomoć u provedbi tijelima za zaštitu podataka iz EU-a. To bi u odgovarajućim slučajevima moglo uključivati razmjenu informacija i pomoć u istrazi u skladu s američkim Zakonom o sigurnom internetu (SAFE WEB), kojim se FTC ovlašćuje za pružanje pomoći stranim agencijama kaznenog progona kad provode zakone kojima se zabranjuje praksa koja je u bitnom slična praksi zabranjenoj zakonima koje provodi FTC ([17]). FTC u okviru te pomoći može razmjenjivati informacije prikupljene u vezi sa svojom istragom, pokrenuti obvezni postupak u ime tijela za zaštitu podataka iz EU-a koje provodi vlastitu istragu i tražiti usmeno svjedočenje svjedoka ili tuženika u vezi s postupkom provedbe tijela za zaštitu podataka, u skladu sa zahtjevima američkog zakona SAFE WEB. FTC redovito upotrebljava te ovlasti za pomoć tijelima iz cijelog svijeta u predmetima povezanima sa zaštitom privatnosti i potrošača.

Osim savjetovanja o pitanjima povezanima s određenim predmetom s tijelima za zaštitu podataka iz EU-a koja su ga uputila, FTC će sudjelovati na periodičnim sastancima s imenovanim predstavnicima Europskog odbora za zaštitu podataka (EDPB) radi općenitih razgovora o mogućnostima poboljšanja suradnje u području provedbe. FTC će zajedno s Ministarstvom trgovine, Europskom komisijom i predstavnicima EDPB-a periodično preispitivati provedbu okvira EU-a i SAD-a za privatnost podataka. FTC potiče i razvoj resursa za poboljšanje suradnje u području provedbe s tijelima za zaštitu podatka iz EU-a te s drugim tijelima za provedbu zaštite privatnosti u cijelom svijetu. FTC sa zadovoljstvom potvrđuje svoju predanost provedbi aspekata okvira EU-a i SAD-a za privatnost podataka povezanih s trgovinskim sektorom. Smatramo da je naše partnerstvo s kolegama iz EU-a ključno za zaštitu privatnosti naših i vaših građana.

S poštovanjem

Lina M. KHAN
Predsjednica, Savezna trgovinska komisija

([17]) Kad utvrđuje treba li izvršavati svoje ovlasti u skladu s američkim zakonom SAFE WEB, FTC među ostalim razmatra sljedeće: „(A) je li agencija koja podnosi zahtjev pristala pružiti ili će pružiti uzajamnu pomoć Komisiji, (B) hoće li se postupanjem u skladu sa zahtjevom dovesti u pitanje javni interes SAD-a, i (C) odnosi li se istraga ili postupak provedbe agencije koja podnosi zahtjev na postupanje ili praksu kojima se nanosi ili bi se mogla nanijeti šteta velikom broju osoba" (glava 15. članak 46. točka (j)(3) Zakonika SAD-a). Ta se ovlast ne primjenjuje na provedbu zakona o tržišnom natjecanju.

Dodatak A

Provedba sustava zaštite privatnosti i programa „sigurne luke”

	Broj predmeta/dokumenta FTC-a	Predmet	Poveznica
1	Dokument FTC-a br. 2023062 Predmet br. 3:22-cv-03070 (Sjeverni okrug Kalifornije)	SAD protiv **Twitter, Inc.**	Twitter
2	Dokument FTC-a br. 192 3209	U predmetu Residual Pumpkin Entity, LLC, ranija tvrtka: **CafePress**, i PlanetArt, LLC, druga tvrtka: **CafePress**	CafePress
3	Dokument FTC-a br. 192 3133 Broj predmeta: C-4747	U predmetu **Flo Health, Inc.**	Flo Health
4	Dokument FTC-a br. 192 3050 Broj predmeta: C-4723	U predmetu **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	Dokument FTC-a br. 192 3092 Broj predmeta: C-4709	U predmetu **T&M Protection, LLC**	T&M Protection
6	Dokument FTC-a br. 192 3084 Broj predmeta: C-4704	U predmetu **TDARX, Inc.**	TDARX
7	Dokument FTC-a br. 192 3093 Broj predmeta: C-4706	U predmetu **Global Data Vault, LLC**	Global Data
8	Dokument FTC-a br. 192 3078 Broj predmeta: C-4703	U predmetu **Incentive Services, Inc.**	Incentive Services
9	Dokument FTC-a br. 192 3090 Broj predmeta: C-4705	U predmetu **Click Labs, Inc.**	Click Labs
10	Dokument FTC-a br. 182 3192 Broj predmeta: C-4697	U predmetu **Medable, Inc.**	Medable
11	Dokument FTC-a br. 182 3189 Broj predmeta: 9386	U predmetu NTT Global Data Centers Americas, Inc., sljednik poduzeća **RagingWire Data Centers, Inc.**	RagingWire
12	Dokument FTC-a br. 182 3196 Broj predmeta: C-4702	U predmetu **Thru, Inc.**	Thru
13	Dokument FTC-a br. 182 3188 Broj predmeta: C-4698	U predmetu **DCR Workforce, Inc.**	DCR Workforce
14	Dokument FTC-a br. 182 3194 Broj predmeta: C-4700	U predmetu **LotaData, Inc.**	LotaData
15	Dokument FTC-a br. 182 3195 Broj predmeta: C-4701	U predmetu **EmpiriStat, Inc.**	EmpiriStat

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

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

55	Dokument FTC-a br. 142 3025 Broj predmeta: C-4468	U predmetu **PDB Sports, Ltd.**, druga tvrtka: Denver Broncos Football Club, LLP	Broncos
56	Dokument FTC-a br. 142 3030 Broj predmeta: C-4471	U predmetu **Reynolds Consumer Products, Inc.**	Reynolds
57	Dokument FTC-a br. 142 3031 Broj predmeta: C-4472	U predmetu **Receivable Management Services Corporation**	Receivable Mgmt
58	Dokument FTC-a br. 142 3032 Broj predmeta: C-4473	U predmetu **Tennessee Football, Inc.**	Tennessee Football
59	Dokument FTC-a br. 102 3058 Broj predmeta: C-4369	U predmetu **Myspace LLC**	Myspace
60	Dokument FTC-a br. 092 3184 Broj predmeta: C-4365	U predmetu **Facebook, Inc.**	Facebook
61	Dokument FTC-a br. 092 3081 Građanski postupak br. 09-CV-5276 (C.D. Cal.)	FTC protiv Javiana Karnanija i **Balls of Kryptonite, LLC**, druge tvrtke: Bite Size Deals, LLC i Best Priced Brands, LLC	Balls of Kryptonite
62	Dokument FTC-a br. 102 3136 Broj predmeta: C-4336	U predmetu **Google, Inc.**	Google
63	Dokument FTC-a br. 092 3137 Broj predmeta: C-4282	U predmetu **World Innovators, Inc.**	World Innovators
64	Dokument FTC-a br. 092 3141 Broj predmeta: C-4271	U predmetu **Progressive Gaitways LLC**	Progressive Gaitways
65	Dokument FTC-a br. 092 3139 Broj predmeta: C-4270	U predmetu **Onyx Graphics, Inc.**	Onyx Graphics
66	Dokument FTC-a br. 092 3138 Broj predmeta: C-4269	U predmetu **ExpatEdge Partners, LLC**	ExpatEdge
67	Dokument FTC-a br. 092 3140 Broj predmeta: C-4281	U predmetu **Directors Desk LLC**	Directors Desk
68	Dokument FTC-a br. 092 3142 Broj predmeta: C-4272	U predmetu **Collectify LLC**	Collectify

PRILOG V.

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6. srpnja 2023.

Povjerenik Didier Reynders
Europska komisija
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgija

Poštovani povjereniče Reynders,

Ministarstvo prometa Sjedinjenih Američkih Država zahvaljuje na prilici da opiše svoju ulogu u provedbi Načela okvira EU-a i SAD-a za privatnost podataka. Okvir EU-a i SAD-a za privatnost podataka ima ključnu ulogu u zaštiti osobnih podataka koji se razmjenjuju u poslovnim transakcijama u sve povezanijem svijetu. Okvir će omogućiti poduzećima da obavljaju važne poslove u globalnom gospodarstvu i ujedno osigurati da potrošači iz EU-a zadrže važne oblike zaštite privatnosti.

Ministarstvo prometa prvi se put javno obvezalo na provedbu europsko-američkog okvira „sigurne luke" u dopisu poslanu Europskoj komisiji prije više od 22 godine, a te su obveze ponovljene i proširene u dopisu iz 2016. koji se odnosio na okvir europsko-američkog sustava zaštite privatnosti. Naše se ministarstvo tim dopisima obvezalo da će odlučno provoditi Načela europsko-američkog programa sigurne luke, a zatim i europsko-američkog sustava zaštite privatnosti. Proširujemo tu obvezu na Načela okvira EU-a i SAD-a za privatnost podataka, a ovim se dopisom ta obveza trajno bilježi.

Ministarstvo prometa osobito potvrđuje svoje obveze u sljedećim ključnim područjima: 1. davanje prednosti istrazi navodnih povreda Načela okvira EU-a i SAD-a za privatnost podataka, 2. prikladne provedbene mjere protiv subjekata koji navode lažne ili prijevarne izjave o članstvu u tom okviru, i 3. praćenje i objava provedbenih naloga koji se odnose na povrede tog okvira. Sve su te obveze opisane u nastavku, a u svrhu pružanja nužnog konteksta navedene su i osnovne informacije o ulozi Ministarstva prometa u zaštiti privatnosti potrošača i provedbi Načela okvira za privatnost podataka.

1. **Kontekst**

A. Ovlasti Ministarstva prometa za zaštitu privatnosti

Ministarstvo prometa snažno se zalaže za zaštitu privatnosti informacija koje potrošači daju zračnim prijevoznicima

i posrednicima u prodaji karata. Ovlasti Ministarstva prometa za postupanje u tom području propisane su u glavi 49. članku 41712. Zakonika SAD-a, kojim se prijevozniku ili posredniku u prodaji karata zabranjuje „nepoštena ili prijevarna praksa" u zračnom prijevozu ili prodaji usluga u zračnom prijevozu. Članak 41712.

sastavljen je po uzoru na članak 5. Zakona o FTC-u (glava 15. članak 45. Zakonika SAD-a). Ministarstvo prometa nedavno je objavilo propise u kojima se definira nepoštena i prijevarna praksa u skladu s prethodnim definicijama tog ministarstva i FTC-a. (glava 14. članak 399.79 Kodeksa saveznih propisa). Točnije, praksa je „nepoštena" ako zbog nje nastaje ili bi mogla nastati znatna šteta koju nije moguće razumno izbjeći i čiji štetni učinak ne nadoknađuju pogodnosti

za potrošače ili tržišno natjecanje. Praksa je „prijevarna" za potrošače ako bi mogla zavarati potrošača koji u pogledu značajnog pitanja postupa razumno s obzirom na okolnosti. Pitanje je značajno ako je moglo utjecati na ponašanje potrošača ili odluku u pogledu proizvoda ili usluge. Osim tih općenitih načela, Ministarstvo prometa tumači članak 41712. na način da se njime prijevozniku ili posredniku u prodaji karata zabranjuje: 1. povreda uvjeta svoje politike zaštite privatnosti, 2. povreda bilo kojeg pravila koje je objavilo Ministarstvo prometa na temelju kojeg se utvrđuje da je određena praksa zaštite privatnosti nepoštena ili prijevarna, 3. povreda Zakona o zaštiti privatnosti djece na internetu (*Children's Online Privacy Protection Act* – COPPA) ili propisa FTC-a o provedbi tog zakona, ili 4. propust da kao sudionici okvira EU-a i SAD-a za privatnost podataka postupaju u skladu s Načelima tog okvira ([1]).

Kao što je prethodno navedeno, u skladu sa saveznim pravom Ministarstvo prometa ima isključivu ovlast regulirati praksu zaštite privatnosti zračnih prijevoznika, a dijeli nadležnost s FTC-om za praksu zaštite privatnosti posrednika u prodaji karata za usluge zračnog prijevoza.

Kad se prijevoznik ili prodavač usluga zračnog prijevoza javno obveže poštovati Načela okvira EU-a i SAD-a za privatnost podataka, Ministarstvo prometa može upotrijebiti svoje zakonske ovlasti iz članka 41712. da osigura usklađenost s tim načelima. Dakle, kad putnik da informacije prijevozniku ili posredniku u prodaji karata koji se obvezao poštovati Načela okvira EU-a i SAD-a za privatnost podataka, svako ponašanje prijevoznika ili posrednika koje nije u skladu s tim načelima smatralo bi se povredom članka 41712.

B. Provedbena praksa

Ured Ministarstva prometa za zaštitu potrošača u zračnom prometu (*Office of Aviation Consumer Protection* – OACP) ([2]) istražuje i kazneno progoni predmete u skladu s glavom 49. člankom 41712. Zakonika SAD-a. On provodi zakonsku zabranu nepoštene i prijevarne prakse iz članka 41712. uglavnom pregovorima, pripremom naloga za obustavu i izradom naloga u kojima se određuju građanskopravne sankcije. Ured saznaje za moguće povrede većinom iz pritužbi koje zaprima od pojedinaca, putnih agenata, zračnih prijevoznika te američkih i stranih vladinih agencija. Potrošači mogu podnositi pritužbe na povrede privatnosti protiv zračnih prijevoznika i posrednika u prodaji karata na internetskim stranicama Ministarstva prometa ([3]).

Ako se u određenom predmetu ne postigne razumna i odgovarajuća nagodba, OACP je ovlašten pokrenuti provedbeni postupak koji uključuje izvođenje dokaza pred upravnim sucem Ministarstva prometa. Upravni sudac ima ovlasti izdavati naloge za obustavu i građanskopravne sankcije. Povrede članka 41712. mogu dovesti do izdavanja naloga za obustavu i izricanja građanskopravnih sankcija u iznosu do 37 377 USD za svaku povredu tog članka.

Ministarstvo prometa nema ovlasti dodijeliti odštetu ili novčanu naknadu pojedinačnim podnositeljima pritužbi. Međutim, ima ovlasti odobriti nagodbe sklopljene nakon istraga OACP-a koje izravno koriste potrošačima (npr. gotovina, vaučeri) za prijeboj novčanih kazni koje bi inače trebalo platiti američkoj vladi. To se dogodilo u prošlosti, a može se dogoditi i u kontekstu Načela okvira EU-a i SAD-a za privatnost podataka ako to bude opravdano zbog okolnosti. Ako zračni prijevoznik opetovano krši članak 41712., dovela bi se u pitanje njegova spremnost na usklađivanje, što bi u vrlo ozbiljnim situacijama moglo dovesti do zaključka da prijevoznik više nije sposoban obavljati djelatnost i stoga bi izgubio odobrenje za njezino obavljanje.

Ministarstvo prometa do danas je zaprimilo razmjerno malo pritužbi koje se odnose na navodne povrede privatnosti posrednika u prodaji karata ili zračnih prijevoznika. Kad dođe do tih povreda, one se istražuju u skladu s prethodno navedenim načelima.

C. Oblici pravne zaštite Ministarstva prometa koji se primjenjuju na potrošače iz EU-a

U skladu s člankom 41712. zabrana nepoštene ili prijevarne prakse u zračnom prijevozu ili prodaji usluga zračnog prijevoza primjenjuje se na američke i strane zračne prijevoznike i na posrednike u prodaji karata. Ministarstvo prometa često poduzima mjere protiv američkih i stranih zračnih prijevoznika zbog prakse koja utječe na strane i američke potrošače na temelju činjenice da je zračni prijevoznik primjenjivao tu praksu tijekom pružanja usluga prijevoza iz SAD-a ili u SAD. Ministarstvo prometa upotrebljava i nastavit će upotrebljavati sva pravna sredstva koja su dostupna za zaštitu stranih i američkih potrošača od nepoštene ili prijevarne prakse reguliranih subjekata u zračnom prijevozu.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Ranije poznat kao Ured za provedbu i postupke u području zrakoplovstva (Office of Aviation Enforcement and Proceedings).
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

Kad je riječ o zračnim prijevoznicima, Ministarstvo provodi i druge ciljane zakone kojima se štite potrošači izvan SAD-a, kao što je Zakon o zaštiti privatnosti djece na internetu (*Children's Online Privacy Act* – COPPA). Tim je zakonom propisano, među ostalim, da operateri internetskih stranica i internetskih usluga usmjerenih na djecu ili stranica za opću publiku koji svjesno prikupljaju osobne informacije od djece mlađe od 13 godine moraju obavijestiti roditelje o tome i zatražiti njihovu provjerljivu suglasnost. Američke internetske stranice i usluge na koje se primjenjuje taj zakon i koje prikupljaju podatke od djece iz inozemstva moraju postupati u skladu s njim. Internetske stranice i usluge iz inozemstva moraju postupati u skladu s tim zakonom ako su usmjerene na djecu u SAD-u ili ako svjesno prikupljaju osobne informacije od tamošnje djece. Ako SAD ili strani prijevoznici koji posluju u toj državi krše taj zakon, Ministarstvo prometa bilo bi nadležno za poduzimanje provedbenih mjera.

II. **Provedba Načela okvira EU-a i SAD-a za privatnost podataka**

Ako zračni prijevoznik ili posrednik u prodaji karata odluči sudjelovati u okviru EU-a i SAD-a za privatnost podataka, a Ministarstvo prometa zaprimi pritužbu da je taj zračni prijevoznik ili posrednik u prodaji karata navodno povrijedio Načela tog okvira, poduzelo bi korake navedene u nastavku za njihovu odlučnu provedbu.

A. Davanje prednosti istrazi navodnih povreda

OACP Ministarstva prometa istražit će sve pritužbe o navodnim povredama Načela okvira EU-a i SAD-a za privatnost podataka,

uključujući pritužbe koje zaprimi od tijela za zaštitu podataka iz EU-a, i poduzet će provedbene mjere kad postoje dokazi o povredi. Nadalje, OACP će surađivati s FTC-om i Ministarstvom trgovine i prvo će razmatrati navode da regulirani subjekti ne ispunjavaju obveze u pogledu privatnosti preuzete u skladu s okvirom EU-a i SAD-a za privatnost podataka.

Po primitku navoda o povredi Načela okvira EU-a i SAD-a za privatnost podataka OACP u okviru istrage može poduzeti niz mjera. Može na primjer preispitati politike zaštite privatnosti posrednika u prodaji karata ili zračnog prijevoznika, pribaviti dodatne informacije od posrednika u prodaji karata ili zračnog prijevoznika ili trećih strana, konzultirati se s tijelom koje je uputilo predmet, ocijeniti postoji li obrazac povreda i je li pogođen velik broj potrošača. Osim toga, utvrdio bi odnosi li se predmet na pitanja u nadležnosti Ministarstva trgovine ili FTC-a, ocijenio bi li bilo korisno obrazovati potrošače i poduzeća i prema potrebi bi pokrenuo postupak provedbe.

Ako Ministarstvo prometa sazna da su posrednici u prodaji karata povrijedili Načela okvira EU-a i SAD-a za privatnost podataka, surađivat će s FTC-om u tom pogledu. Savjetovat ćemo se i s FTC-om i Ministarstvom trgovine o ishodu svih provedbenih mjera u pogledu Načela okvira EU-a i SAD-a za privatnost podataka.

B. Suzbijanje lažnih ili prijevarnih izjava o sudjelovanju u okviru za privatnost podataka

Ministarstvo je i dalje predano istragama povreda Načela okvira EU-a i SAD-a za privatnost podataka, uključujući lažne ili prijevarne izjave o sudjelovanju u tom okviru. Davat ćemo prednost razmatranju predmeta koje je uputilo Ministarstvo trgovine u vezi s organizacijama za koje je utvrdilo da se neprimjereno predstavljaju kao sudionice okvira EU-a i SAD-a za privatnost podataka ili upotrebljavaju certifikacijske oznake tog okvira bez odobrenja.

Nadalje, napominjemo da, ako organizacija u svojoj politici zaštite privatnosti tvrdi da je usklađena s Načelima okvira EU-a i SAD-a za privatnost podataka, činjenica da se nije samocertificirala ili ponovno samocertificirala Ministarstvu trgovine sama po sebi vjerojatno ne znači da će biti oslobođena od toga da Ministarstvo prometa osigura provedbu tih obveza.

C. Praćenje i objava provedbenih naloga koji se odnose na povrede okvira EU-a i SAD-a za privatnost podataka

OACP potvrđuje svoju predanost praćenju provedbenih naloga prema potrebi kako bi se osigurala usklađenost s Načelima okvira EU-a i SAD-a za privatnost podataka. Točnije, ako ured izda nalog kojim se od zračnog prijevoznika ili posrednika u prodaji karata traži da obustavi daljnje povrede Načela okvira EU-a i SAD-a za privatnost podataka i članka 41712., on će pratiti usklađenost tog subjekta s odredbom o obustavi iz naloga. Nadalje, ured će osigurati da su nalozi doneseni u predmetima povezanima s Načelima okvira EU-a i SAD-a za privatnost podataka dostupni na njegovim internetskim stranicama.

Veselimo se daljnjoj suradnji s našim saveznim partnerima i dionicima iz EU-a na pitanjima povezanima s okvirom EU-a i SAD-a za privatnost podataka.

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

S poštovanjem

Pete BUTTIGIEG

PRILOG VI.

Ministarstvo pravosuđa SAD-a

Uprava za kazneno pravo

Ured pomoćnika Glavnog državnog odvjetnika

Washington, D.C. 20530

23. lipnja 2023.

Gđa Ana Gallego Torres
Glavna direktorica za pravosuđe i zaštitu potrošača
Europska komisija
Rue Montoyer/Montoyerstraat 59
1049 Bruxelles
Belgija

Poštovana direktorice Gallego Torres,

u ovom dopisu navodi se kratak pregled glavnih istražnih alata koji se upotrebljavaju za prikupljanje tržišnih podataka i ostalih informacija iz evidencije od poduzeća u SAD-u u svrhe kaznenog progona ili javnog interesa (građanske i regulatorne), uključujući ograničenja pristupa utvrđena u tim ovlastima ([1]). Svi su pravni postupci koji su opisani u ovom dopisu nediskriminirajući jer se upotrebljavaju za prikupljanje informacija od poduzeća u SAD-u, među ostalim od poduzeća koja će se samocertificirati u skladu s okvirom EU-a i SAD-a za privatnost podataka, bez obzira na državljanstvo ili boravište ispitanika. Nadalje, poduzeća protiv kojih je pokrenut sudski postupak u SAD-u mogu ga osporiti pred sudom na način opisan u nastavku ([2]).

Kad je riječ o zapljeni podataka koju obavljaju javna tijela, posebno treba spomenuti četvrti amandman Ustava SAD-a u kojem je propisano da se „ne smije povrijediti pravo osoba da se osjećaju sigurno te da su njihove kuće, dokumenti i imovina zaštićeni od nerazumnih pretraga i zapljena, a nalozi se smiju izdavati samo ako postoji opravdana sumnja potkrijepljena prisegom ili izjavom i u njima mora biti posebno opisano mjesto koje će se pretraživati i osobe ili stvari koje će se zaplijeniti.” Četvrti amandman američkog Ustava. Kako je Vrhovni sud SAD-a naveo u predmetu Berger protiv Države New Yorka, „osnovna je svrha tog amandmana, potvrđena u brojnim odlukama ovog Suda, zaštititi privatnost i sigurnost pojedinaca od proizvoljnog i neovlaštenog narušavanja privatnosti koje provode vladini dužnosnici.” 388 U.S. 41, 53 (1967.) (u kojem se citira predmet Camara protiv Općinskog suda u San Franciscu, 387 U.S. 523, 528 (1967.)). Četvrtim amandmanom općenito se zahtijeva da službenici tijela kaznenog progona u istragama u nacionalnim kaznenim postupcima prije pretrage ishode sudski nalog za pretragu. Vidjeti predmet Katz protiv SAD-a, 389 U.S. 347, 357 (1967.). Standardi za izdavanje naloga, kao što su osnovana sumnja te precizan opis predmeta za zapljenu i mjesta na kojem će se ona obaviti, primjenjuju se na naloge za fizičko pretraživanje i zapljenu, kao i na naloge za pohranjeni sadržaj elektroničke

([1]) Ovim pregledom nisu obuhvaćeni istražni alati u području nacionalne sigurnosti koje upotrebljavaju tijela kaznenog progona u slučaju istraga terorizma i drugih istraga povezanih s nacionalnom sigurnošću, što uključuje dopise o nacionalnoj sigurnosti za određene informacije koje se nalaze u izvješćima o kreditnoj sposobnosti, financijskim evidencijama i elektroničkim evidencijama o pretplatnicima i transakcijama, glava 12. članak 3414. Zakonika SAD-a; glava 15. članak 1681.u Zakonika SAD-a; glava 15. članak 1681.v Zakonika SAD-a; glava 18. članak 2709. Zakonika SAD-a; glava 50. članak 3162. Zakonika SAD-a, te za elektronički nadzor, naloge za pretragu, poslovne evidencije i drugo prikupljanje informacija na temelju Zakona o nadzoru stranih obavještajnih aktivnosti, glava 50. članak 1801. i dalje Zakonika SAD-a.

([2]) U ovom je dopisu riječ o saveznim tijelima kaznenog progona i regulatornim tijelima. Povrede državnih zakona istražuju državna tijela kaznenog progona i rješavaju ih pred državnim sudovima. Državna tijela kaznenog progona upotrebljavaju naloge za pretragu i sudske pozive u skladu s državnim zakonima na prethodno opisani način, ali na državni sudski postupak mogu se primjenjivati dodatni oblici zaštite iz državnih ustava ili zakona koji premašuju one iz američkog Ustava. Oblici zaštite pruženi u okviru državnih zakona moraju biti barem jednaki onima pruženima u okviru američkog Ustava, uključujući, ali ne ograničavajući se na četvrti amandman.

komunikacije izdane u skladu sa Zakonom o pohranjenoj komunikaciji kako je opisano u nastavku. Ako se ne primjenjuje zahtjev posjedovanja sudskog naloga, aktivnosti vlade ipak podliježu provjeri „opravdanosti" u skladu s četvrtim amandmanom. Stoga se samim Ustavom osigurava da američka vlada nema neograničene ili proizvoljne ovlasti da zaplijeni osobne informacije ([3]).

Tijela kaznenog progona:

Savezni tužitelji, koji su zaposlenici Ministarstva pravosuđa, i savezni agenti, uključujući agente Saveznog istražnog ureda (FBI), agencije kaznenog progona u okviru Ministarstva pravosuđa, mogu zahtijevati od poduzeća u SAD-u da dostave dokumente i ostale informacije iz evidencija u svrhe istrage u kaznenom postupku primjenom nekoliko vrsta obveznih zakonskih mjera, uključujući pozive velike porote, upravne sudske pozive i naloge za pretragu, te mogu tražiti druge podatke o komunikacijama u skladu sa saveznim ovlastima za prikupljanje podataka prislušnim uređajima i bilježenje izlaznih poziva.

Poziv velike porote ili sudski poziv: kazneni sudski pozivi upotrebljavaju se za potporu ciljanim istragama tijela kaznenog progona. Poziv velike porote službeni je zahtjev koji izdaje velika porota (obično na zahtjev saveznog tužitelja) za potporu istrazi koju velika porota provodi zbog sumnje na povredu kaznenog prava. Velika porota istražni je ogranak suda koji sastavlja sudac ili pomoćni sudac. U sudskom se pozivu može od nekoga tražiti da dostavi ili da na uvid poslovne evidencije, elektronički pohranjene informacije ili druge fizičke predmete. Informacije moraju biti relevantne za istragu i sudski poziv ne smije biti nerazuman jer je preopsežan, opresivan ili opterećujući. Primatelj na temelju toga može osporavati sudski poziv. Vidjeti Savezne propise o kaznenom postupku, propis br. 17. Sudski pozivi na dostavu dokumenata u ograničenim se okolnostima mogu upotrebljavati nakon što velika porota izda optužnicu.

Ovlast za izdavanje upravnog sudskog poziva: ovlasti za izdavanje upravnog sudskog poziva mogu se primjenjivati u istragama u kaznenim ili građanskopravnim postupcima. U kontekstu kaznenog progona postoji nekoliko saveznih zakona kojima se dopušta uporaba upravnih sudskih poziva na dostavu ili davanje na uvid poslovnih evidencija, elektronički pohranjenih informacija ili drugih fizičkih predmeta u istragama povezanima s prijevarom u zdravstvu, zlostavljanjem djece, zaštitom koju pruža Tajna služba i kontroliranim tvarima te istragama glavnog inspektora usmjerenima na vladine agencije. Ako vlada želi provesti upravni sudski poziv na sudu, primatelj takvog poziva, kao i primatelj sudskog poziva koji je izdala velika porota, može tvrditi da je taj sudski poziv nerazuman jer je preopsežan, opresivan ili opterećujući.

Sudski nalozi za uređaje za bilježenje ulaznih i izlaznih poziva: u skladu s kaznenim odredbama o uređajima za bilježenje ulaznih i izlaznih poziva tijela kaznenog progona mogu ishoditi sudski nalog za prikupljanje informacija o biranim brojevima, preusmjeravanju, adresiranju i signaliziranju bez sadržaja u stvarnom vremenu za telefonski broj ili e-adresu nakon potvrde da su dostavljene informacije relevantne za istragu u kaznenom postupku koja je u tijeku. Vidjeti glavu 18. članke od 3121. do 3127. Zakonika SAD-a. Nezakonita uporaba ili postavljanje takvog uređaja savezno je kazneno djelo.

Zakon o zaštiti privatnosti elektroničke komunikacije (ECPA): dodatna pravila primjenjuju se na vladin pristup informacijama o pretplatnicima, podacima o prometu i pohranjenom sadržaju komunikacije u posjedu pružatelja internetskih usluga, telefonskih operatera i ostalih pružatelja usluga koji su treća strana, u skladu s glavom II. ECPA-e, koja se naziva i Zakonom o pohranjenim komunikacijama (glava 18. članci od 2701. do 2712. Zakonika SAD-a). Tim je zakonom uspostavljen sustav zaštite prava na privatnost na temelju kojeg je pristup tijela kaznenog progona podacima o klijentima i pretplatnicima pružatelja internetskih usluga ograničen na ono što je propisano ustavnim pravom. Propisano je i da se razina zaštite privatnosti povećava razmjerno tomu koliko se prikupljanjem zadire u privatnost. Tijela kaznenog progona moraju ishoditi sudski poziv za prikupljanje informacija o registraciji pretplatnika, IP adresa i povezanih

([3]) Američki sudovi redovito primjenjuju prethodno navedena načela zaštite interesa u pogledu privatnosti i sigurnosti iz četvrtog amandmana na nove vrste istražnih alata koje su dostupne tijelima kaznenog progona zahvaljujući tehnološkom razvoju. Na primjer, Vrhovni sud odlučio je 2018. da činjenica da je vlada u okviru istrage tijela kaznenog progona dulje vrijeme prikupljala povijesne podatke o lokaciji baznih stanica od mobilnog mrežnog operatera čini „pretragu" na koju se primjenjuje zahtjev za nalog iz četvrtog amandmana. Carpenter protiv SAD-a, 138 S. Ct. 2206 (2018.).

vremenskih oznaka te informacija o naplati. Za većinu drugih pohranjenih informacija bez sadržaja, kao što su zaglavlja e-poruka bez predmeta, ta tijela moraju sucu iznijeti konkretne činjenice kojima se dokazuje da su tražene informacije relevantne i bitne za istragu u kaznenom postupku koja je u tijeku. Kako bi mogla dobiti pohranjeni sadržaj elektroničke komunikacije, tijela kaznenog progona u načelu moraju od suca ishoditi nalog na temelju osnovane sumnje da predmetni račun sadržava dokaze o kaznenom djelu. U Zakonu o pohranjenim komunikacijama propisane su građanskopravna odgovornost i kaznene sankcije ([4]).

Sudski nalozi za nadzor u skladu sa saveznim Zakonom o uporabi prislušnih uređaja: tijela kaznenog progona u svrhu istrage u kaznenom postupku mogu u stvarnom vremenu presretati telefonsku, usmenu ili elektroničku komunikaciju u skladu sa saveznim Zakonom o uporabi prislušnih uređaja. Vidjeti glavu 18. članke od 2510. do 2523. Zakonika SAD-a. Ta se ovlast dobiva samo na temelju sudskog naloga u kojem je sudac utvrdio, među ostalim, da postoji osnovana sumnja da će se prisluškivanjem ili elektroničkim presretanjem pronaći dokazi o saveznom kaznenom djelu ili o lokaciji bjegunca od kaznenog progona. U zakonu su predviđene građanskopravna odgovornost i kaznene sankcije za povrede odredbi o prisluškivanju

Nalog za pretragu – Savezni propisi o kaznenom postupku, propis br. 41: tijela kaznenog progona mogu fizički pretražiti prostorije u SAD-u ako sudac to dopusti. Ta tijela moraju dokazati sucu da postoji osnovana sumnja da je kazneno djelo počinjeno ili će biti počinjeno i da se predmeti povezani s tim kaznenim djelom vjerojatno nalaze na mjestu navedenom u nalogu. Ta se ovlast često upotrebljava kad policija mora fizički pretražiti prostorije jer postoji opasnost od uništavanja dokaza ako se poduzeću dostavi sudski poziv ili drugi nalog. Osoba koja je predmet pretrage ili čija je imovina· predmet pretrage može podnijeti prijedlog za odbijanje izvođenja dokaza pribavljenih nezakonitom pretragom ili izvedenih na temelju takve pretrage ako se ti dokazi iznesu protiv te osobe u kaznenom postupku. Vidjeti predmet Mapp protiv Ohija, 367 U.S. 643 (1961.). Kad je nositelj podataka dužan otkriti podatke na temelju naloga, on može ponajprije osporavati obvezu otkrivanja kao prekomjerno opterećenje. Vidjeti predmete In re Application of United States, 610 F.2d 1148, 1157 (3. okrug, 1979.) (utvrđeno je da je „postupanje […] zakonito samo ako se saslušanje o pitanju opterećenja održi prije nego što se telefonskog operatera obveže da pomogne" u izvršenju naloga za pretragu) i In re Application of United States, 616 F.2d 1122 (9. okrug, 1980.) (isti zaključak na temelju nadzorne ovlasti suda).

Smjernice i politike Ministarstva pravosuđa: osim tih ustavnih i zakonskih ograničenja vladina pristupa podacima i ograničenja utemeljenih na propisima glavni državni odvjetnik objavio je smjernice kojima se dodatno ograničava pristup tijela kaznenog progona podacima i koje sadržavaju i mjere za zaštitu privatnosti i građanskih sloboda. Na primjer, Smjernicama glavnog državnog odvjetnika za domaće operacije FBI-ja (rujan 2008.), koje su dostupne na http://www.justice.gov/archive/opa/docs/guidelines.pdf, utvrđena su ograničenja uporabe istražnih sredstava za traženje informacija povezanih s istragama saveznih kaznenih djela. Tim je smjernicama propisano da FBI mora upotrebljavati istražne metode kojima se najmanje zadire u privatnost uzimajući u obzir utjecaj na privatnost i građanske slobode i moguću štetu za ugled. Nadalje, u njima se navodi da se „podrazumijeva da FBI mora provoditi svoje istrage i druge aktivnosti na zakonit i razuman način kojim se poštuju sloboda i privatnost te izbjegava nepotrebno zadiranje u privatnost osoba koje poštuju zakone." (Smjernice glavnog državnog odvjetnika za FBI, točka 5.). FBI provodi te smjernice u okviru Vodiča FBI-ja za domaće istrage i operacije, dostupnog na https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29. Riječ je o opsežnom priručniku koji uključuje detaljna ograničenja uporabe istražnih alata i smjernice kojima se osigurava zaštita građanskih sloboda i privatnosti u svakoj istrazi. Dodatna pravila i politike u kojima su propisana ograničenja istražnih aktivnosti saveznih tužitelja navedeni su u Pravosudnom priručniku, koji je dostupan i na internetu na https://www.justice.gov/jm/justicemanual.

Građanska i regulatorna tijela (javni interes):

([4]) Osim toga, u članku 2705. točki (b) tog zakona vladu se ovlašćuje da ishodi sudski nalog na temelju dokazane potrebe za zaštitom od otkrivanja, a pružatelju komunikacijskih usluga zabranjuje se da dobrovoljno obavijesti korisnike o tome da je pokrenut postupak u skladu s tim zakonom. Zamjenik glavnog državnog odvjetnika Rod Rosenstein u listopadu 2017. uputio je memorandum odvjetnicima i agentima Ministarstva pravosuđa u kojem su navedene smjernice kako bi takvi nalozi za zaštitu bili prilagođeni posebnim činjenicama i pitanjima u okviru istrage i u kojem je utvrđena opća gornja granica od godine dana kao najdulje razdoblje na koje se molbom može tražiti odgoda obavijesti. Zamjenica glavnog državnog odvjetnika Lisa Monaco u svibnju 2022. objavila je dodatne smjernice o toj temi, kojima su među ostalim uvedeni interni zahtjevi Ministarstva pravosuđa za odobrenje molbi za produljenje trajanja naloga o zaštiti nakon početnog jednogodišnjeg razdoblja i kojima se zahtijeva ukidanje naloga za zaštitu nakon završetka istrage.

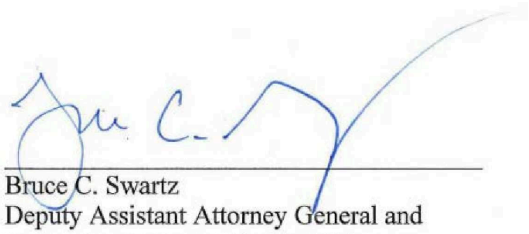
Postoje ozbiljna ograničenja i u pogledu pristupa građanskih i regulatornih tijela (pristup zbog „javnog interesa") podacima poduzeća u SAD-u. Agencije s građanskim i regulatornim nadležnostima mogu izdavati sudske pozive za poslovne evidencije, elektronički pohranjene informacije ili druge fizičke predmete poduzeća. Te agencije imaju ograničene ovlasti za dostavljanje upravnih ili građanskopravnih sudskih poziva ne samo na temelju svojih osnivačkih akata, već i zbog neovisnog sudskog preispitivanja sudskih poziva prije mogućeg sudskog izvršenja. Vidjeti npr. Savezne propise o građanskom postupku, propis br. 45. Agencije mogu tražiti pristup samo onim podacima koji su relevantni za pitanja u njihovoj nadležnosti. Nadalje, primatelj upravnog sudskog poziva može osporiti njegovo izvršenje na sudu dostavljanjem dokaza da agencija nije postupila u skladu s osnovnim standardima opravdanosti, kako je prethodno opisano.

Postoje i druge pravne osnove na temelju kojih poduzeća mogu osporavati zahtjeve upravnih agencija za podatke zbog posebnosti industrije u kojoj djeluju i vrste podataka koje posjeduju. Na primjer, financijske institucije mogu osporavati upravne sudske pozive kojima se traže određeni podaci jer ih smatraju povredom Zakona o bankarskoj tajni i njegovih provedbenih propisa (glava 31. članak 5318. Zakonika SAD-a; glava 31. poglavlje X. Kodeksa saveznih propisa). Druga poduzeća mogu se oslanjati na Zakon o poštenom izvješćivanju o kreditnoj sposobnosti (glava 15. članak 1681.b Zakonika SAD-a), ili niz drugih zakona usmjerenih na određene sektore. Zlouporaba ovlasti agencije za izdavanje sudskih poziva može dovesti do toga da agencija snosi odgovornost ili da njezini zaposlenici snose osobnu odgovornost. Vidjeti na primjer Zakon o pravu na privatnost financijskih podataka, glava 12. članci od 3401. do 3423. Zakonika SAD-a. Sudovi u SAD-u stoga su zaštitnici od nezakonitih regulatornih zahtjeva i osiguravaju neovisni nadzor aktivnosti saveznih agencija.

Naposljetku, zakonske ovlasti upravnih tijela za fizičku zapljenu evidencije poduzeća u SAD-u na temelju pregleda moraju biti u skladu sa zahtjevima iz četvrtog amandmana. Vidjeti predmet See protiv Grada Seattlea, 387 U.S. 541 (1967.).

Zaključak

Sve aktivnosti tijela kaznenog progona i regulatornih tijela u SAD-u moraju biti u skladu s primjenjivim pravom, uključujući američki Ustav, zakone, pravila i propise. Te aktivnosti moraju biti u skladu i s primjenjivim politikama, uključujući smjernice glavnog državnog odvjetnika kojima se uređuju aktivnosti saveznih tijela kaznenog progona. Prethodno opisanim pravnim okvirom ograničava se mogućnost američkih agencija kaznenog progona i regulatornih agencija da pribavljaju informacije od poduzeća u SAD-u, neovisno o tome odnose li se te informacije na američke državljane ili osobe koje nisu američki državljani, i dopušta sudsko preispitivanje svih vladinih zahtjeva za dostavljanje podataka u skladu s tim ovlastima.



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

PRILOG VII.

URED DIREKTORA ZA NACIONALNA OBAVJEŠTAJNA PITANJA, URED GLAVNOG PRAVNOG SAVJETNIKA

WASHINGTON, DC 20511

9. prosinca 2022.

Leslie B. Kiernan
Glavna pravna savjetnica
Ministarstvo trgovine SAD-
a, 1401 Constitution
Ave., NW Washington, DC 20230

Poštovana gđo Kiernan,

dana 7. listopada 2022. predsjednik Biden potpisao je Izvršni nalog br. 14086 o poboljšanju zaštitnih mjera u američkim aktivnostima elektroničkog izviđanja, kojim se jača strogi skup zaštitnih mjera u pogledu privatnosti i građanskih sloboda primjenjivih na američke aktivnosti elektroničkog izviđanja. Na temelju tih zaštitnih mjera aktivnosti elektroničkog izviđanja moraju ispunjavati navedene legitimne ciljeve, izričito je zabranjena provedba takvih aktivnosti za potrebe određenih zabranjenih ciljeva, uvedeni su novi postupci kojima se osigurava da se aktivnostima elektroničkog izviđanja promiču ti legitimni ciljevi te da se ne promiču oni zabranjeni, zahtijeva se da se aktivnosti elektroničkog izviđanja provode tek nakon što se, na temelju razumne procjene svih relevantnih čimbenika, utvrdi da su te aktivnosti nužne za ostvarenje potvrđenog obavještajnog prioriteta, i to samo u mjeri i na način koji su proporcionalni potvrđenom obavještajnom prioritetu za čije su ostvarenje odobrene, a od obavještajnih službi traži se da ažuriraju svoje politike i postupke kako bi se uzele u obzir zaštitne mjere u pogledu elektroničkog izviđanja koje se zahtijevaju Izvršnim nalogom. Najvažnije, Izvršnim se nalogom uvodi neovisan i obvezujući mehanizam koji pojedincima iz „država koje ispunjavaju uvjete", kako su utvrđene u tom nalogu, omogućuje traženje pravne zaštite ako smatraju da su bili predmet američkih aktivnosti elektroničkog izviđanja u suprotnosti sa zakonom, uključujući aktivnosti koje predstavljaju povredu oblika zaštite iz Izvršnog naloga.

Izdavanjem Izvršnog naloga br. 14086 predsjednika Bidena zaključeni su pregovori između predstavnika Europske komisije i SAD-a koji su trajali više od godinu dana i donesena je odluka o smjeru kojim će SAD krenuti u provedbi svojih obveza u skladu s okvirom EU-a i SAD-a za privatnost podataka. U skladu s duhom suradnje u kojem je nastao taj okvir, razumijem da ste od Europske komisije primili dva skupa pitanja o načinu na koji će obavještajne službe provoditi Izvršni nalog. U ovom ću dopisu rado odgovoriti na ta pitanja.

Članak 702. Zakona o nadzoru stranih obavještajnih aktivnosti iz 1978. (članak 702. FISA-e)

Prvi skup pitanja odnosi se na članak 702. FISA-e, u skladu s kojim se strane obavještajne informacije mogu, uz zakonski obveznu pomoć američkih pružatelja usluga elektroničke komunikacije, prikupljati ciljanim praćenjem osoba koji nisu američki državljani, a za koje se iz opravdanih razloga vjeruje da se nalaze izvan SAD-a. Točnije, pitanja se odnose na međudjelovanje te odredbe i Izvršnog naloga br. 14086 te drugih zaštitnih mjera koje se primjenjuju na aktivnosti koje se provode u skladu s člankom 702. FISA-e.

Za početak možemo potvrditi da će obavještajne službe primjenjivati zaštitne mjere iz Izvršnog naloga br. 14086 na aktivnosti koje se provode u skladu s člankom 702. FISA-e.

Osim toga, brojne druge zaštitne mjere primjenjuju se na vladinu primjenu članka 702. FISA-e. Na primjer, sve certifikate iz članka 702. FISA-e moraju potpisati glavni državni odvjetnik i direktor za nacionalna obavještajna pitanja, a vlada sve takve certifikate mora dostaviti na odobrenje Sudu za nadzor stranih obavještajnih aktivnosti (FISC), koji se sastoji od neovisnih sudaca s doživotnim mandatom imenovanih na sedmogodišnje mandatno razdoblje koje se ne može obnoviti. U certifikatima se navode kategorije stranih obavještajnih informacija, koje moraju odgovarati zakonskoj definiciji stranih obavještajnih informacija, a prikupljat će se ciljanim praćenjem osoba koje nisu američkih državljani, a za koje se iz opravdanih razloga vjeruje da se nalaze izvan SAD-a. Certifikati sadržavaju informacije o međunarodnom terorizmu i drugim temama, kao što je prikupljanje informacija o oružju za masovno uništenje. Svi godišnji certifikati moraju se podnijeti na odobrenje FISC-u u okviru molbe za certificiranje, koja uključuje certifikate glavnog državnog odvjetnika i direktora za nacionalna obavještajna pitanja, izjave pod prisegom određenih ravnatelja obavještajnih agencija te postupke ciljanog praćenja, smanjenja količine podataka i pretraživanja koji su obvezujući za vladu. Za postupke ciljanog praćenja obavještajne službe moraju na temelju svih okolnosti razumno procijeniti je li vjerojatno da će se ciljanim praćenjem prikupiti strane obavještajne informacije navedene u certifikatu u skladu s člankom 702. FISA-e.

Osim toga, kad obavještajne službe prikupljaju informacije u skladu s člankom 702. FISA-e, moraju: pisanim putem objasniti razloge na kojima je utemeljena ocjena da se u vrijeme ciljanog praćenja očekivalo da ciljana osoba posjeduje, da bi mogla primiti ili da će vjerojatno prenijeti strane obavještajne informacije navedene u certifikatu u skladu s člankom 702. FISA-e, potvrditi da je standard za ciljano praćenje utvrđen u postupcima ciljanog praćenja iz članka 702. FISA-e i dalje ispunjen i prestati s prikupljanjem ako standard više nije ispunjen. Vidjeti podnesak američke vlade Sudu za nadzor stranih obavještajnih aktivnosti, *2015 Summary of Notable Section 702 Requirements* (Sažetak iz 2015. o najvažnijim zahtjevima iz članka 702.), str. 2.–3. (15. srpnja 2015.).

Činjenica da obavještajne službe moraju u pisanom obliku zabilježiti svoju ocjenu da ciljane osobe iz članka 702. FISA-e ispunjavaju primjenjive standarde za ciljano praćenje i redovito potvrđivati valjanost te ocjene omogućuje FISC-u jednostavniji nadzor aktivnosti ciljanog praćenja koje provode obavještajne službe. Odvjetnici odgovorni za nadzor obavještajnih aktivnosti pri Ministarstvu pravosuđa svaka dva mjeseca preispituju svaku evidentiranu procjenu i obrazloženje za ciljano praćenje, a provode tu nadzornu funkciju neovisno o stranim obavještajnim operacijama. Odjel Ministarstva pravosuđa koji provodi tu funkciju zatim u skladu s davno uspostavljenim pravilom FISC-a ima odgovornost prijaviti FISC-u sve povrede primjenjivih postupaka. To prijavljivanje, zajedno s redovitim sastancima FISC-a i tog odjela Ministarstva pravosuđa u pogledu nadzora ciljanog praćenja iz članka 702. FISA-e, omogućuje FISC-u da osigura usklađenost s ciljanim praćenjem iz tog članka i drugim postupcima te da se na druge načine pobrine da su aktivnosti vlade zakonite. FISC to može činiti na razne načine, među ostalim donošenjem obvezujućih korektivnih odluka o obustavljanju ovlasti vlade da prikuplja podatke o određenoj ciljanoj osobi ili da se izmijeni ili odgodi prikupljanje podataka iz članka 702. FISA-e. FISC može tražiti od vlade i da ga dodatno izvijesti o svojoj usklađenosti s postupcima ciljanog praćenja i drugim postupcima ili zahtijevati od vlade da ih promijeni.

„Skupno" prikupljanje podataka elektroničkim izviđanjem

Drugi se skup pitanja odnosi na „skupno" prikupljanje podataka elektroničkim izviđanjem, definirano u Izvršnom nalogu br. 14086 kao „odobreno prikupljanje velike količine podataka elektroničkim izviđanjem koji su iz tehničkih ili operativnih razloga prikupljeni bez primjene razlikovnih čimbenika (npr. bez primjene posebnih identifikatora ili čimbenika za odabir)".

U tom pogledu napominjemo da skupno prikupljanje nije dopušteno u skladu s FISA-om ni u skladu s dopisima o nacionalnoj sigurnosti. Kad je riječ o FISA-i:

— Za glave I. i III., kojima se dopušta elektronički nadzor odnosno fizičke pretrage, potreban je sudski nalog (uz ograničen broj iznimaka, kao što su hitni slučajevi) i uvijek mora postojati osnovana sumnja da je ciljana osoba strana sila ili agent strane sile. Vidjeti glavu 50. članke 1805. i 1824. Zakonika SAD-a.

— Zakonom USA FREEDOM iz 2015. izmijenjena je glava IV. FISA-e, kojom se dopušta uporaba uređaja za bilježenje ulaznih i izlaznih poziva na temelju sudskog naloga (osim u hitnim slučajevima), na način da je uvedena obveza da zahtjevi vlade budu utemeljeni na „posebnom čimbeniku za odabir". Vidjeti glavu 50. članak 1842. točku (c)(3) Zakonika SAD-a.

— Za glavu V. FISA-e, kojom se FBI-ju dopušta pribavljanje određene poslovne evidencije, potreban je sudski nalog utemeljen na molbi u kojoj je utvrđeno da „postoje konkretne i razumljive činjenice koje su temelj opravdane sumnje da je osoba kojoj evidencije pripadaju strana sila ili agent strane sile". Vidjeti glavu 50. članak 1862. točku (b)(2)(B) Zakonika SAD-a ([1]).

— Konačno, člankom 702. FISA-e dopušteno je „ciljano praćenje osoba koje nisu američki državljani, a za koje se iz opravdanih razloga vjeruje da se nalaze izvan SAD-a kako bi prikupile strane obavještajne informacije". Vidjeti glavu 50. članak 188l.a točku (a) Zakonika SAD-a. Dakle, kako je primijetio Odbor za nadzor privatnosti i građanskih sloboda, prikupljanje podataka koje vlada provodi u skladu s člankom 702. FISA-e „u cijelosti se sastoji od ciljanog praćenja određenih osoba i pribavljanja komunikacija povezanih s tim osobama jer vlada smatra da je razumno očekivati da će od njih prikupiti određene oblike stranih obavještajnih informacija" te „program ne funkcionira na način da se skupno prikupljaju komunikacije". Odbor za zaštitu privatnosti i građanske slobode, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Izvješće o programu nadzora koji se provodi u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti), str. 103. (2. srpnja 2014.) ([2]).

Zakonom USA FREEDOM iz 2015. uvodi se zahtjev „posebnog čimbenika za odabir" za uporabu dopisa o nacionalnoj sigurnosti. Vidjeti glavu 12. članak 3414. točku (a)(2) Zakonika SAD-a; glavu 15. članak 1681.u Zakonika SAD-a; glavu 15. članak 1681.v točku (a) Zakonika SAD-a; glavu 18. članak 2709. točku (b) Zakonika SAD-a.

Nadalje, u Izvršnom nalogu br. 14086 propisano je da se „daje prednost ciljanom prikupljanju" i da je, kad obavještajne službe provode skupno prikupljanje, „skupno prikupljanje elektroničkim izviđanjem dopušteno samo ako se utvrdi […] da se informacije nužne za ostvarenje potvrđenog obavještajnog prioriteta iz opravdanih razloga ne mogu dobiti ciljanim prikupljanjem". Vidjeti članak 2. točku (c)(ii)(A) Izvršnog naloga br. 14086.

Osim toga, Izvršnim nalogom br. 14086 propisane su dodatne zaštitne mjere za slučajeve kad obavještajne službe utvrde da skupno prikupljanje ispunjava te uvjete. Točnije, u tom se nalogu zahtijeva da obavještajna zajednica pri skupnom prikupljanju mora „provesti razumne metode i tehničke mjere za ograničavanje prikupljanja samo na one podatke koji su nužni za ostvarenje potvrđenog obavještajnog prioriteta i na što manju količinu nerelevantnih informacija" *(vidjeti prethodno upućivanje)*. U Izvršnom nalogu navedeno je i da se „aktivnosti elektroničkog izviđanja", koje uključuju pretraživanje podataka dobivenih skupnim elektroničkim izviđanjem „provode tek nakon što se, na temelju razumne procjene svih relevantnih čimbenika, utvrdi da su te aktivnosti nužne za ostvarenje potvrđenog obavještajnog prioriteta" *(vidjeti prethodno upućivanje,* članak 2. točka (a)(ii)(A)). U tom se nalogu dodatno provodi navedeno načelo navođenjem da obavještajne službe mogu pretraživati samo podatke dobivene skupnim elektroničkim izviđanjem čija količina nije smanjena i koji su prikupljeni kako bi se ostvarilo šest dopuštenih ciljeva te da se takva pretraživanja moraju provoditi u skladu s politikama i postupcima „u kojima se u odgovarajućoj mjeri uzima u obzir utjecaj pretraživanja na privatnost i građanske slobode svih osoba neovisno o njihovu državljanstvu ili boravištu" *(vidjeti prethodno upućivanje,* članak 2. točka (c)(iii)(D)). Konačno, u Izvršnom nalogu propisani su način postupanja s prikupljenim podacima, njihova sigurnost i kontrola pristupa *(vidjeti prethodno upućivanje,* članak 2. točke (c)(iii)(A) i (c)(iii)(B)).

* * * * *

Nadamo se da su ova pojašnjenja bila korisna. Obratite nam se bez ustručavanja ako imate dodatna pitanja o načinu na koji američke obavještajne službe namjeravaju provesti Izvršni nalog br. 14086.

([1]) U razdoblju od 2001. do 2020. FBI-ju je na temelju glave V. FISA-e bilo dopušteno tražiti odobrenje od FISC-a da pribavi „fizičke predmete" relevantne za određene odobrene istrage. Vidjeti članak 215. zakona USA PATRIOT, Javni zakon br. 107-56, Zakonik br. 115, str. 272. (2001.). Ta je odredba stavljena izvan snage, ali zbog navedenog je izraza vlada u određenom razdoblju imala ovlasti za skupno prikupljanje metapodataka o telefonskim pozivima. Međutim, čak i prije nego što je odredba stavljena izvan snage, izmijenjena je zakonom USA FREEDOM na način da je uvedena obveza da molbe koje vlada upućuje FISC-u budu utemeljene na „posebnom čimbeniku za odabir". Vidjeti članak 103. zakona USA FREEDOM iz 2015., Javni zakon br. 114-23, Zakonik br. 129, str. 268. (2015.).

([2]) U skladu s člancima 703. i 704., kojima se obavještajnim službama dopušta prikupljanje podataka o američkim državljanima koji se nalaze izvan SAD-a, potreban je sudski nalog (osim u hitnim slučajevima) i uvijek mora postojati osnovana sumnja da je ciljana osoba strana sila, agent strane sile ili službenik ili zaposlenik strane sile. Vidjeti glavu 50. članke 1881.b i 1881.c Zakonika SAD-a.

Sincerely,

Christopher C. FONZONE
Glavni pravni savjetnik

PRILOG VIII.

Popis pokrata

U ovoj se Odluci pojavljuju sljedeće pokrate:

AAA	Američko udruženje za arbitražu
Uredba glavnog državnog odvjetnika	Uredba glavnog državnog odvjetnika o Žalbenom sudu za zaštitu podataka
AGG-DOM	Smjernice glavnog državnog odvjetnika za domaće operacije FBI-ja
APA	Zakon o upravnom postupku
CIA	Središnja obavještajna agencija
CNSS	Odbor za sustave nacionalne sigurnosti
Sud	Sud Europske unije
Odluka	Provedbena odluka Komisije u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenoj razini zaštite osobnih podataka u skladu s okvirom EU-a i SAD-a za privatnost podataka
DHS	Ministarstvo domovinske sigurnosti
DNI	Direktor Nacionalne obavještajne službe
DoC	Ministarstvo trgovine SAD-a
DoJ	Ministarstvo pravosuđa SAD-a
DoT	Ministarstvo prometa SAD-a
DPA	Tijelo za zaštitu podataka
Popis DPF-a	Popis organizacija uključenih u okvir za privatnost podataka
DPRC	Žalbeni sud za zaštitu podataka
ECOA	Zakon o jednakim mogućnostima za dobivanje kredita
ECPA	Zakon o zaštiti privatnosti elektroničke komunikacije
EEA	Europski gospodarski prostor
Izvršni nalog br. 12333	Izvršni nalog br. 12333 „Obavještajne aktivnosti Sjedinjenih Država”
Izvršni nalog br. 14086, izvršni nalog	Izvršni nalog br. 14086. „Poboljšanje zaštitnih mjera u američkim aktivnostima elektroničkog izviđanja”
DPF EU-a i SAD-a ili DPF	Okvir EU-a i SAD-a za privatnost podataka
Panel DPF-a EU-a i SAD-a	Panel okvira EU-a i SAD-a za privatnost podataka
FBI	Savezni istražni ured
FCRA	Zakon o poštenom izvješćivanju o kreditnoj sposobnosti
FISA	Zakon o nadzoru stranih obavještajnih aktivnosti
FISC	Sud za nadzor stranih obavještajnih aktivnosti
FISCR	Žalbeni sud za nadzor stranih obavještajnih aktivnosti
FOIA	Zakon o pravu na pristup informacijama
FRA	Zakon o saveznim evidencijama

FTC	Savezna trgovinska komisija SAD-a
HIPAA	Zakon o prenosivosti i odgovornosti u zdravstvenom osiguranju
ICDR	Međunarodni centar za rješavanje sporova
IOB	Odbor za nadzor obavještajnih aktivnosti
NIST	Nacionalni institut za standardizaciju i tehnologiju
NSA	Nacionalna sigurnosna agencija
NSL	Dopis(i) o nacionalnoj sigurnosti
ODNI	Ured direktora Nacionalne obavještajne službe
ODNI CLPO, CLPO	Službenik za zaštitu građanskih sloboda ureda direktora Nacionalne obavještajne službe
OMB	Ured za upravljanje i proračun
OPCL	Ured za privatnost i građanske slobode Ministarstva pravosuđa
PCLOB	Nadzorni odbor za zaštitu privatnosti i građanskih sloboda
PIAB	Predsjednički savjetodavni odbor za obavještajne aktivnosti
PPD br. 28	Predsjednički ukaz br. 28
Uredba (EU) 2016/679	Uredba (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
SAOP	Viši službenik Agencije za zaštitu privatnosti
Načela	Načela okvira EU-a i SAD-a za privatnost podataka
SAD	Sjedinjene Američke Države
Unija	Europska unija