Uradni list Evropske unije

L 207

Slovenska izdaja

Zakonodaja

Zvezek 59

1. avgust 2016

Vsebina

II *Nezakonodajni akti*

SKLEPI

★ **Izvedbeni sklep Komisije (EU) 2016/1250 z dne 12. julija 2016 na podlagi Direktive Evropskega parlamenta in Sveta 95/46/ES o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA** *(notificirano pod dokumentarno številko C(2016) 4176)* [1] 1

★ **Izvedbeni sklep Komisije (EU) 2016/1251 z dne 12. julija 2016 o sprejetju večletnega programa Unije za zbiranje, upravljanje in uporabo podatkov v sektorjih ribištva in akvakulture za obdobje 2017–2019** *(notificirano pod dokumentarno številko C(2016) 4329)* 113

[1] Besedilo velja za EGP

SL

Akti z rahlo natisnjenimi naslovi so tisti, ki se nanašajo na dnevno upravljanje kmetijskih zadev in so splošno veljavni za omejeno obdobje.

Naslovi vseh drugih aktov so v mastnem tisku in pred njimi stoji zvezdica.

II

(Nezakonodajni akti)

SKLEPI

IZVEDBENI SKLEP KOMISIJE (EU) 2016/1250

z dne 12. julija 2016

na podlagi Direktive Evropskega parlamenta in Sveta 95/46/ES o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA

(notificirano pod dokumentarno številko C(2016) 4176)

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]) in zlasti člena 25(6) Direktive,

po posvetovanju z Evropskim nadzornikom za varstvo podatkov ([2]),

1. UVOD

(1) Direktiva 95/46/ES določa pravila za prenos osebnih podatkov iz držav članic v tretje države, kolikor taki prenosi spadajo na področje njene uporabe.

(2) Namen člena 1 Direktive 95/46/ES ter uvodnih izjav 2 in 10 v njeni preambuli je zagotoviti ne le učinkovito in popolno varstvo temeljnih pravic in svoboščin posameznikov, zlasti temeljne pravice do spoštovanja zasebnega življenja v zvezi z obdelavo osebnih podatkov, temveč tudi visoko raven varstva teh temeljnih pravic in svoboščin ([3]).

(3) Sodišče je v svoji sodni praksi poudarilo pomembnost temeljne pravice do spoštovanja zasebnega življenja, zagotovljene s členom 7 Listine Evropske unije o temeljnih pravicah, in temeljne pravice do varstva osebnih podatkov, zagotovljene s členom 8 Listine ([4]).

(4) V skladu s členom 25(1) Direktive 95/46/ES morajo države članice določiti, da se prenos osebnih podatkov v tretjo državo lahko izvede le, če zadevna tretja država zagotavlja ustrezno raven varstva in če se pred prenosom upoštevajo zakoni države članice o izvajanju drugih določb Direktive. Komisija lahko ugotovi, da tretja država zagotavlja tako ustrezno raven varstva zaradi svoje domače zakonodaje ali mednarodnih obveznosti, ki jih je prevzela za zaščito pravic posameznikov. V tem primeru in brez poseganja v skladnost z nacionalnimi določbami, sprejetimi na podlagi drugih določb Direktive, se lahko osebni podatki iz držav članic prenesejo, ne da bi bila potrebna dodatna jamstva.

([1]) UL L 281, 23.11.1995, str. 31.
([2]) Glej Mnenje 4/2016 o osnutku sklepa o ustreznosti zasebnostnega ščita EU-ZDA, objavljeno 30. maja 2016.
([3]) Zadeva C-362/14, Maximillian Schrems proti Data Protection Commissioner (v nadaljnjem besedilu: Schrems), EU:C:2015:650, točka 39.
([4]) Zadeva C-553/07, Rijkeboer, EU:C:2009:293, točka 47; združeni zadevi C-293/12 in C-594/12, Digital Rights Ireland in drugi, EU:C:2014:238, točka 53; zadeva C-131/12, Google Spain in Google, EU:C:2014:317, točke 53, 66 in 74.

(5) V skladu s členom 25(2) Direktive 95/46/ES bi bilo treba raven varstva podatkov, ki jo nudi tretja država, oceniti ob upoštevanju vseh okoliščin v zvezi s postopkom prenosa podatkov ali nizom postopkov prenosa podatkov, vključno s splošnimi in sektorskimi pravnimi normami, ki veljajo v zadevni tretji državi.

(6) V Odločbi Komisije 2000/520/ES ([5]) se za namene člena 25(2) Direktive 95/46/ES šteje, da „načela zasebnosti varnega pristana", ki so uveljavljena v skladu s smernicami iz tako imenovanih „najpogosteje zastavljenih vprašanj", ki jih je izdalo Ministrstvo za trgovino ZDA, zagotavljajo ustrezno raven varstva osebnih podatkov, ki se prenašajo iz Unije v organizacije s sedežem v ZDA.

(7) Komisija je v sporočilih COM(2013) 846 final ([6]) in COM(2013) 847 final z dne 27. novembra 2013 ([7]) menila, da je treba temeljno podlago sheme varnega pristana proučiti in okrepiti v kontekstu nekaterih dejavnikov, vključno z eksponentnim povečanjem prenosa podatkov in njegovim odločilnim pomenom za čezatlantsko gospodarstvo, hitrim povečanjem števila družb v ZDA, ki so se zavezale k shemi varnega pristana, ter novimi informacijami o obsegu in področju uporabe nekaterih obveščevalnih programov ZDA, kar je sprožilo vprašanja glede ravni varstva, ki jo lahko ta shema zagotavlja. Poleg tega je Komisija odkrila številne slabosti in pomanjkljivosti sheme varnega pristana.

(8) Komisija je na podlagi zbranih dokazov, vključno z informacijami o delu kontaktne skupine EU-ZDA za varstvo zasebnosti ([8]) in informacijami o obveščevalnih programih ZDA, ki jih je prejela priložnostna delovna skupina EU-ZDA ([9]), oblikovala 13 priporočil za pregled sheme varnega pristana. Ta priporočila se osredotočajo na krepitev vsebinskih načel zasebnosti, povečanje preglednosti politik varstva zasebnosti samocertificiranih družb v ZDA, boljše nadziranje, spremljanje in uveljavljanje skladnosti s temi načeli s strani organov ZDA, dostopnost stroškovno ugodnih mehanizmov reševanja sporov ter potrebo po zagotovitvi, da se izjema v interesu nacionalne varnosti iz Odločbe 2000/520/ES uporablja le v obsegu, ki je nujno potreben ali sorazmeren..

(9) Sodišče je v sodbi z dne 6. oktobra 2015 v zadevi C-362/14, Maximillian Schrems proti Data Protection Commissioner ([10]) Odločbo 2000/520/ES razglasilo za neveljavno. Ne da bi proučilo vsebino načel zasebnosti varnega pristana, je Sodišče ugotovilo, da Komisija v zadevni odločbi ni ugotovila, da so ZDA dejansko „zagotavljale" ustrezno raven varstva zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti ([11]).

(10) V zvezi s tem je Sodišče pojasnilo, da čeprav izraz „ustrezna raven varstva" iz člena 25(6) Direktive 95/46/ES ne pomeni ravni varstva, ki je enaka ravni varstva, zagotovljeni v pravnem redu EU, ga je treba razumeti tako, da se z njim zahteva, da tretja država zagotavlja raven varstva temeljnih pravic in svoboščin, ki je „v bistvenem enaka" ravni, zagotovljeni v Uniji na podlagi Direktive 95/46/ES, kot se razlaga ob upoštevanju Listine o temeljnih pravicah. Četudi so sredstva, ki jih zadevna tretja država uporabi za zagotovitev take ravni varstva, lahko drugačna od sredstev, uporabljenih znotraj Unije, se morajo ta sredstva v praksi vseeno izkazati za učinkovita ([12]).

(11) Sodišče je kritiziralo odsotnost ugotovitev v Odločbi 2000/520/ES glede obstoja državnih predpisov v ZDA, katerih namen bi bil omejiti morebitne posege v temeljne pravice posameznikov, katerih podatki se prenašajo iz Unije v ZDA, posege, ki naj bi jih državni subjekti v tej državi lahko izvajali, kadar poskušajo doseči legitimne cilje, kot je nacionalna varnost, in glede obstoja učinkovitega sodnega varstva v primeru takih posegov ([13]).

([5]) Odločba Komisije 2000/520/ES z dne 26. julija 2000 po Direktivi Evropskega parlamenta in Sveta 95/46/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana, in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA (UL L 215, 28.8.2000, str. 7).

([6]) Sporočilo Komisije Evropskemu parlamentu in Svetu Obnovitev zaupanja v pretok podatkov med EU in ZDA, COM(2013) 846 final z dne 27. novembra 2013.

([7]) Sporočilo Komisije Evropskemu parlamentu in Svetu o delovanju varnega pristana z vidika državljanov EU in družb, ustanovljenih v EU, COM(2013) 847 final z dne 27. novembra 2013.

([8]) Glej na primer Svet Evropske unije, končno poročilo kontaktne skupine EU-ZDA na visoki ravni o izmenjavi informacij ter zasebnosti in varstvu osebnih podatkov (Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection), Dopis 9831/08, 28. maj 2008, na voljo na spletu na: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Poročilo o ugotovitvah predstavnikov EU, ki so sopredsedovali priložnostni delovni skupini EU-ZDA za varstvo podatkov, 27. november 2013, na voljo na spletu na: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Glej opombo 3.

([11]) Zadeva Schrems, točka 97.

([12]) Zadeva Schrems, točki 73 in 74.

([13]) Zadeva Schrems, točki 88 in 89.

(12) Komisija je leta 2014 začela pogovore z organi ZDA, da bi razpravljali o okrepitvi sheme varnega pristana v skladu s 13 priporočili iz Sporočila COM(2013) 847 final. Po sodbi Sodišča v zadevi Schrems so se ti pogovori okrepili, da bi se sprejel morebiten nov sklep o ustreznosti varstva, ki bi izpolnjeval zahteve iz člena 25 Direktive 95/46/ES, kakor jih razlaga Sodišče. Dokumenti, ki so priloženi temu sklepu in ki bodo tudi objavljeni v Zveznem registru ZDA, so rezultat teh razprav. Načela zasebnosti (Priloga II) skupaj z uradnimi zagotovili in zavezami različnih organov ZDA, vsebovanimi v dokumentih iz prilog I in III–VII, tvorijo „zasebnostni ščit EU-ZDA“.

(13) Komisija je podrobno proučila zakonodajo in prakso ZDA, vključno s temi uradnimi zagotovili in zavezami. Na podlagi ugotovitev, oblikovanih v uvodnih izjavah 136 do 140, je Komisija sklenila, da ZDA zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije samocertificiranim organizacijam v ZDA.

2. „ZASEBNOSTNI ŠČIT EU-ZDA“

(14) Zasebnostni ščit EU-ZDA temelji na sistemu samocertificiranja, s katerim se organizacije v ZDA zavežejo sklopu načel zasebnosti, tj. načelom okvira zasebnostnega ščita EU-ZDA, vključno z dopolnilnimi načeli (v nadaljnjem besedilu skupaj: načela), ki jih je izdalo Ministrstvo za trgovino ZDA in so navedena v Prilogi II k temu sklepu. Uporablja se za upravljavce in obdelovalce (posrednike), pri čemer je posebnost to, da morajo biti obdelovalci pogodbeno zavezani, da delujejo samo po navodilih upravljavca EU, kateremu pomagajo pri odgovorih posameznikom, ki uveljavljajo svoje pravice po načelih ([14]).

(15) Ta sklep brez poseganja v skladnost z nacionalnimi določbami, sprejetimi v skladu z Direktivo 95/46/ES, dovoljuje prenose z upravljavca ali obdelovalca v Uniji na organizacije v ZDA, ki so samocertificirale zavezanost k načelom pri Ministrstvu za trgovino in se zavezale, da jih bodo spoštovale. Načela se uporabljajo samo za obdelavo osebnih podatkov s strani organizacij ZDA, v kolikor obdelava s strani takih organizacij ne spada na področje uporabe zakonodaje Unije ([15]). Zasebnostni ščit ne vpliva na uporabo zakonodaje Unije, ki ureja obdelavo osebnih podatkov v državah članicah ([16]).

([14]) Glej Prilogo II, člen III.10.a. V skladu z opredelitvijo iz člena I.8.c upravljavec iz EU določi namen in načine obdelave osebnih podatkov. Poleg tega mora biti v pogodbi s posrednikom jasno določeno, ali so dovoljeni prenosi tretjemu (glej člen III.10a.ii.2).

([15]) To velja tudi v primeru prenašanja podatkov o človeških virih iz Unije v okviru zaposlitvenega razmerja. Čeprav načela poudarjajo „primarno odgovornost“ delodajalca iz EU (glej člen III.9.d. Priloge II), hkrati jasno navajajo, da bo njegovo ravnanje zajeto v pravilih, ki veljajo v Uniji in/ali zadevni državi članici, ne pa v načelih. Glej Prilogo II, člen III.9.a.i, b.ii, c.i in d.i.

([16]) To velja tudi za obdelavo, ki se izvaja z uporabo opreme, ki se nahaja v Uniji, ki pa jo uporablja organizacija s sedežem zunaj Unije (glej člen 4(1)(c) Direktive 95/46/ES). Od 25. maja 2018 se bo Splošna uredba o varstvu podatkov (GDPR) uporabljala za obdelavo osebnih podatkov (i) v okviru dejavnosti ustanovitve upravljavca ali obdelovalca v Uniji (tudi če obdelava poteka v ZDA) ali (ii) posameznikov v Uniji, na katere se nanašajo osebni podatki, s strani upravljavca ali obdelovalca, ki nima sedeža v Uniji, pri čemer so dejavnosti obdelave povezane s (a) ponujanjem blaga ali storitev, ne glede na to, ali posameznik, na katerega se nanašajo podatki, zahteva plačilo, takim posameznikom v Uniji, na katere se nanašajo osebni podatki, ali (b) spremljanjem njihovega vedenja v Uniji. Glej člen 3(1), (2) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

(16) Varstvo osebnih podatkov, ki ga zagotavlja zasebnostni ščit, velja za katerega koli posameznika v EU, na katerega se nanašajo osebni podatki ([17]), ki so bili preneseni iz Unije organizacijam v ZDA, ki so samocertificirale zavezanost k načelom pri Ministrstvu za trgovino.

(17) Načela zasebnosti začnejo veljati takoj po certifikaciji. Ena izjema se nanaša na načelo odgovornosti za prenos tretjemu v primeru, ko organizacija, ki se je samocertificirala po zasebnostnem ščitu že ima predhodno obstoječa trgovinska razmerja s tretjimi strankami. Glede na to, da lahko traja nekaj časa, da se ta trgovinska razmerja uskladijo s pravili v okviru načela odgovornosti za prenos tretjemu, mora organizacija to storiti čim prej in v vsakem primeru najpozneje devet mesecev po samocertifikaciji (če se to zgodi v prvih dveh mesecih po datumu začetka veljavnosti zasebnostnega ščita). V tem vmesnem obdobju mora organizacija uporabljati načeli obvestila in možnosti izbire (s čimer posameznikom iz EU, na katere se nanašajo podatki, omogoča zavrnitev) ter mora, če se podatki prenašajo tretji stranki, ki nastopa v vlogi posrednika, zagotoviti, da slednja zagotavlja vsaj enako raven varstva, kot jo zahtevajo načela ([18]). To prehodno obdobje zagotavlja razumno in ustrezno ravnovesje med spoštovanjem temeljne pravice do varstva podatkov in zakonitimi potrebami podjetij, da imajo na voljo dovolj časa za prilagoditev novemu okviru, pri čemer je to odvisno tudi od trgovinskih razmerij s tretjimi strankami.

(18) Ta sistem bo upravljalo in nadzorovalo Ministrstvo za trgovino na podlagi svojih zavez, navedenih v zagotovilih Ministra za trgovino ZDA (Priloga I k temu sklepu). Kar zadeva uveljavljanje načel, sta Zvezna komisija za trgovino (Federal Trade Commission, v nadaljnjem besedilu: FTC) in Ministrstvo za promet podala zagotovila, navedena v prilogah IV in V k temu sklepu.

2.1 *Načela zasebnosti*

(19) Organizacije se morajo v okviru samocertificiranja na podlagi zasebnostnega ščita EU-ZDA zavezati, da bodo spoštovale načela ([19]).

(20) V skladu z *načelom obvestila* morajo organizacije posameznikom, na katere se nanašajo osebni podatki, zagotoviti informacije o številu ključnih elementov, ki se nanašajo na obdelavo njihovih osebnih podatkov (npr. vrsta zbranih podatkov, namen obdelave, pravica do dostopa in izbire, pogoji za prenose tretjemu in odgovornost). Uporabljajo se dodatni zaščitni ukrepi, zlasti zahteva, da organizacije objavijo svoje politike varstva zasebnosti (ki izražajo načela) in navedejo povezave do spletišča Ministrstva za trgovino (s podrobnejšimi informacijami o samocertificiranju, pravicah posameznikov, na katere se nanašajo osebni podatki, in razpoložljivih pritožbenih mehanizmih), seznam zasebnostnega ščita (iz uvodne izjave 30) in spletišče ustreznega organa za alternativno reševanje sporov.

(21) V skladu z *načelom celovitosti podatkov in omejitve namena* morajo biti osebni podatki omejeni na tisto, kar je pomembno za obdelavo, zanesljivi za predvideno uporabo, točni, popolni in aktualni. Organizacija ne sme obdelovati osebnih podatkov na način, ki je nezdružljiv z namenom, za katerega so bili podatki prvotno zbrani ali ki ga je posameznik, na katerega se nanašajo osebni podatki, naknadno odobril. Organizacije morajo zagotoviti, da so osebni podatki zanesljivi za predvideno uporabo, točni, popolni in aktualni.

([17]) Ta sklep velja za EGP. Sporazum o Evropskem gospodarskem prostoru (v nadaljnjem besedilu: Sporazum EGP) predvideva razširitev notranjega trga Evropske unije na tri države EGP, tj. Islandijo, Lihtenštajn in Norveško. Zakonodaja Unije na področju varstva podatkov, vključno z Direktivo 95/46/ES, je zajeta v Sporazumu EGP in je bila vključena v Prilogo XI Sporazuma. Skupni odbor EGP mora sprejeti odločitev glede vključitve tega sklepa v Sporazum EGP. Ko bo ta sklep začel veljati na Islandiji, v Lihtenštajnu in na Norveškem, bo zasebnostni ščit EU–ZDA vključeval tudi te tri države, sklicevanja v svežnju zasebnostnega ščita na EU in njene države članice pa se razumejo tako, da vključujejo Islandijo, Lihtenštajn in Norveško.

([18]) Glej Prilogo II, člen III.6.e.

([19]) Za podatke o človeških virih, zbrane v okviru zaposlitve, se uporabljajo posebna pravila, ki zagotavljajo dodatne zaščitne ukrepe, kot je določeno v dodatnem načelu o „podatkih o človeških virih“ k načelom zasebnosti (glej Prilogo II, člen III.9). Na primer, delodajalci bi morali ustreči prednostnim pravicam zaposlenih po zasebnosti z omejitvijo dostopa do osebnih podatkov, anonimizacijo nekaterih podatkov ali dodelitvijo kod ali psevdonimov. Najpomembneje je, da se od organizacij zahteva, da sodelujejo z organi za varstvo podatkov Unije in upoštevajo njihove nasvete v zvezi s takimi podatki.

(22) Če je nov (spremenjen) namen bistveno drugačen, vendar še vedno združljiv s prvotnim namenom, *načelo izbire* posameznikom, na katere se nanašajo osebni podatki, daje pravico do ugovora (zavrnitve). *Načelo izbire* ne nadomešča izrecne prepovedi nezdružljive obdelave ([20]). Posebna pravila običajno omogočajo, da se uporaba osebnih podatkov za neposredno trženje „kadar koli“ zavrne ([21]). V primeru občutljivih podatkov morajo organizacije običajno pridobiti izrecno pritrdilno soglasje (privolitev) posameznika, na katerega se nanašajo osebni podatki.

(23) Poleg tega se lahko osebni podatki v skladu z *načelom celovitosti podatkov in omejitve namena* hranijo v obliki, ki omogoča identifikacijo posameznika (in s tem v obliki osebnih podatkov), le dokler služijo namenom, za katere so bili prvotno zbrani ali ki so bili naknadno odobreni. Ta obveznost organizacijam v zasebnostnem ščitu ne preprečuje nadaljnje obdelave osebnih podatkov za daljša obdobja, ampak le za obdobje in v obsegu, v katerih se taka obdelava razumno uporablja za enega od naslednjih posebnih namenov: arhiviranje v javnem interesu, novinarstvo, literaturo in umetnost, znanstvene in zgodovinske raziskave ter statistično analizo. Daljše hranjenje osebnih podatkov za enega od teh namenov bo predmet zaščitnih ukrepov v skladu z načeli.

(24) V skladu z *načelom varnosti* morajo organizacije, ki ustvarjajo, vzdržujejo, uporabljajo ali razširjajo osebne podatke, izvesti „razumne in ustrezne“ varnostne ukrepe, ob upoštevanju tveganj, povezanih z obdelavo in naravo podatkov. V primeru podobdelave morajo organizacije skleniti pogodbo s podobdelovalcem, ki zagotavlja enako raven varstva, kot jo zagotavljajo načela, in sprejeti ukrepe za zagotovitev njenega pravilnega izvajanja.

(25) V skladu z *načelom dostopa* ([22]) imajo posamezniki, na katere se nanašajo osebni podatki, pravico, da brez utemeljitve in samo za nepretirano plačilo od organizacije pridobijo potrditev, da taka organizacija obdeluje osebne podatke, povezane z njimi, in da jim podatke sporoči v razumnem času. To pravico je mogoče omejiti le v izjemnih okoliščinah; vsako zanikanje ali omejitev pravice do dostopa je treba nujno in ustrezno utemeljiti, pri čemer mora organizacija dokazati, da so te zahteve izpolnjene. Posamezniki, na katere se nanašajo osebni podatki, morajo imeti možnost, da popravijo, spremenijo ali izbrišejo osebne podatke, če niso točni ali če so bila pri njihovi obdelavi kršena načela. Na področjih, kjer podjetja najverjetneje uporabljajo samodejno obdelavo osebnih podatkov za sprejemanje odločitev, ki vplivajo na posameznika (npr. dajanje posojil, nudenje hipotek, zaposlovanje), zakonodaja ZDA zagotavlja posebno varstvo pred zavrnilnimi odločitvami ([23]). Ti akti posameznikom običajno zagotavljajo pravico do obveščenosti o posebnih razlogih, na katerih temelji odločitev (npr. zavrnitev odobritve posojila), do oporekanja nepopolnim ali netočnim informacijam (pa tudi uporabi nezakonitih elementov) in uveljavljanja pravnega varstva. Ta pravila zagotavljajo varstvo v verjetno precej omejenem številu primerov, kjer samodejne odločitve sprejema sama organizacija v zasebnostnem ščitu ([24]). Vendar je glede na vse večjo uporabo samodejne obdelave podatkov (vključno z oblikovanjem profilov) kot podlage za sprejemanje odločitev, ki vplivajo na posameznike v sodobnem gospodarstvu, to področje, ki ga je treba pozorno spremljati. Za olajšanje tega spremljanja je bilo z organi ZDA dogovorjeno, da bo dialog o samodejnem sprejemanju odločitev, vključno z izmenjavo informacij o podobnostih in razlikah pristopa EU in ZDA v zvezi s tem, del prvega letnega pregleda, pa tudi naslednjih pregledov, če bo to primerno.

([20]) To velja za vse prenose podatkov v okviru zasebnostnega ščita, tudi če se ti nanašajo na podatke, zbrane v zaposlitvenem razmerju. Čeprav lahko samocertificirana organizacija v ZDA načeloma uporablja podatke o človeških virih za različne namene, ki niso povezani z zaposlitvijo (npr. nekatere tržne komunikacije), mora spoštovati prepoved nezdružljive obdelave, poleg tega pa lahko to počne samo v skladu z *načeloma obvestila in možnosti izbire*. Prepoved, da organizacija v ZDA sprejme kakršen koli kazenski ukrep zoper zaposlenega zaradi uveljavljanja take možnosti izbire, vključno s kakršnim koli omejevanjem zaposlitvenih možnosti, zagotavlja, da se nad zaposlenim, kljub podrejenemu razmerju in s tem povezano odvisnostjo, ne izvaja pritisk in da lahko tako dejansko uveljavlja možnost svobodne izbire.

([21]) Glej Prilogo II, člen III.12.

([22]) Glej tudi dopolnilno načelo o „dostopu“ (Priloga II, člen III.8).

([23]) Glej na primer zakon o enakih možnostih pridobitve posojila (Equal Credit Opportunity Act, v nadaljnjem besedilu: ECOA) (člen 1691 in naslednji naslova 15 zakonodajne zbirke ZDA), zakon o pravičnem poročanju o kreditni sposobnosti (Fair Credit Reporting Act, v nadaljnjem besedilu: FRCA) (člen 1681 in naslednji naslova 15 zakonodajne zbirke ZDA) ali zakon proti diskriminaciji v zvezi s prodajo in najemom stanovanj in hiš (Fair Housing Act, v nadaljnjem besedilu: FHA) (člen 3601 in naslednji naslova 42 zakonodajne zbirke ZDA).

([24]) V okviru prenosa osebnih podatkov, ki so bili zbrani v EU, v večini primerov obstaja pogodbeno razmerje med posameznikom (stranko) in upravljavcem iz EU, ki mora spoštovati predpise EU o varstvu podatkov in običajno sprejme kakršno koli odločitev, ki temelji na samodejni obdelavi. To vključuje scenarije, v katerih podatke obdeluje organizacija v zasebnostnem ščitu, ki nastopa v vlogi posrednika in deluje v imenu upravljavca iz EU.

(26) V skladu z *načelom pritožbenega mehanizma, izvrševanja in odgovornosti* ([25]) morajo sodelujoče organizacije zagotoviti zanesljive mehanizme za zagotavljanje skladnosti z drugimi načeli in pritožbeni mehanizem za posameznike iz EU, katerih podatki so bili neskladno obdelani, vključno z učinkovitimi pravnimi sredstvi. Ko se organizacija prostovoljno odloči za samocertificiranje ([26]) v okviru zasebnostnega ščita EU-ZDA, je njeno dejansko upoštevanje načel obvezno. Da bi še naprej lahko uporabljala zasebnostni ščit za prejemanje podatkov iz Unije, mora taka organizacija vsako leto znova potrditi svojo udeležbo v okviru. Organizacije morajo sprejeti tudi ukrepe za preverjanje ([27]), ali so njihove objavljene politike varstva zasebnosti skladne z načeli in ali se dejansko upoštevajo. To se lahko izvede s sistemom samoocenjevanja, ki mora vključevati notranje postopke, ki zagotavljajo, da so zaposleni deležni usposabljanja o izvajanju politik organizacije glede varstva zasebnosti in da se skladnost redno objektivno preverja, ali, pri zunanjih pregledih skladnosti, z metodami, ki lahko vključujejo revizijo in naključne preglede. Poleg tega mora organizacija vzpostaviti učinkovit mehanizem pravnega varstva za obravnavanje morebitnih pritožb (v zvezi s tem glej tudi uvodno izjavo 43), zanjo pa morajo veljati preiskovalna in izvršilna pooblastila FTC, Ministrstva za promet ali drugega ameriškega zakonsko določenega organa, ki učinkovito zagotavlja skladnost z načeli.

(27) Posebna pravila se uporabljajo za tako imenovane „prenose tretjemu“, tj. prenose osebnih podatkov z organizacije na tretjega upravljavca ali obdelovalca, ne glede na to, ali je ta v ZDA ali tretji državi zunaj ZDA (in Unije). Namen teh pravil je zagotoviti, da varstvo osebnih podatkov posameznikov iz EU ni ogroženo in da se mu ni mogoče izogniti z njegovim prenosom na tretje stranke. To je zlasti pomembno v bolj zapletenih verigah obdelave, ki so značilne za sodobno digitalno gospodarstvo.

(28) V skladu z *načelom odgovornosti za prenos tretjemu* ([28]) se lahko kakršen koli prenos tretjemu izvaja samo (i) za omejene in določene namene, (ii) na podlagi pogodbe (ali primerljivega dogovora v skupini podjetij ([29])) in (iii) samo, če taka pogodba zagotavlja enako raven varstva, kot ga zagotavljajo načela, kar vključuje zahtevo, da je uporaba načel lahko omejena le toliko, kolikor je potrebno za izpolnitev namenov nacionalne varnosti, kazenskega pregona in drugih javnih interesov ([30]). To bi bilo treba razlagati v povezavi z načelom *obvestila* in, v primeru prenosa tretjemu upravljavcu ([31]), z *načelom izbire*, v skladu s katerima morajo biti posamezniki, na katere se nanašajo osebni podatki, obveščeni (med drugim) o vrsti/identiteti katerega koli tretjega prejemnika, namenu prenosa tretjemu, pa tudi o možnostih izbire ter lahko nasprotujejo prenosom tretjemu (oziroma jih zavrnejo) ali morajo, v primeru občutljivih podatkov, dati „izrecno pritrdilno soglasje“ (privolitev) za prenose. Ob upoštevanju *načela celovitosti podatkov in omejitve namena* obveznost zagotavljanja enake ravni varstva, kot jo zagotavljajo načela, predvideva, da lahko tretja stranka obdeluje samo osebne podatke, ki so preneseni nanjo za namene, ki so skladni z nameni, za katere so bili prvotno zbrani ali ki jih je posameznik naknadno odobril.

(29) Obveznost zagotavljanja enake ravni varstva, kot jo zahtevajo načela, velja za katero koli in vse tretje stranke, vključene v obdelavo podatkov, ki se prenašajo na tak način, ne glede na njihovo lokacijo (v ZDA ali drugi tretji državi), pa tudi, kadar sam prvotni tretji prejemnik prenaša zadevne podatke drugemu tretjemu prejemniku, na primer za namene podobdelave. V vseh primerih mora biti v pogodbi s tretjim prejemnikom določeno, da bo ta obvestil organizacijo v zasebnostnem ščitu, če bo ugotovil, da ne more več izpolnjevati te obveznosti. V primeru

([25]) Glej tudi dopolnilno načelo o reševanju sporov in izvrševanju (Priloga II, člen III.11).
([26]) Glej tudi dopolnilno načelo o samocertificiranju (Priloga II, člen III.6).
([27]) Glej tudi dopolnilno načelo o preverjanju (Priloga II, člen III.7).
([28]) Glej tudi dopolnilno načelo o obveznih pogodbah za prenos tretjemu (Priloga II, člen III.10).
([29]) Glej tudi dopolnilno načelo o obveznih pogodbah za prenos tretjemu (Priloga II, člen III.10.b). Čeprav to načelo omogoča prenose tudi na podlagi nepogodbenih instrumentov (npr. programi skladnosti in nadzora znotraj skupine), besedilo jasno navaja, da morajo ti instrumenti vedno „zagotavljati neprekinjeno varstvo osebnih podatkov v skladu z načeli“. Poleg tega bo to načelo glede na to, da bodo samocertificirane organizacije v ZDA še vedno odgovorne za skladnost z načeli, zagotavljalo močno spodbudo za uporabo instrumentov, ki so dejansko učinkoviti v praksi.
([30]) Glej Prilogo II, člen I.5.
([31]) Posamezniki ne bodo imeli pravice zavrnitve, če se osebni podatki prenašajo tretji stranki, ki v vlogi posrednika izvaja naloge v imenu in po navodilih organizacije v ZDA. Vendar to zahteva pogodbo s posrednikom in organizacija v ZDA bo odgovorna za zagotavljanje varstva v skladu z načeli z izvajanje pooblastil za dajanje navodil.

take ugotovitve se obdelava s strani tretje stranke preneha, ali pa je treba sprejeti druge razumne in ustrezne ukrepe za izboljšanje stanja ([32]). Kadar se v verigi (pod)obdelave pojavijo težave glede skladnosti, mora organizacija v zasebnostnem ščitu, ki deluje kot upravljavec osebnih podatkov, dokazati, da ni odgovorna za dogodek, ki povzroča škodo, ali kako drugače prevzeti odgovornost, kot je navedeno v *načelu pritožbenega mehanizma, izvrševanja in odgovornosti*. Dodatno varstvo se uporablja v primeru prenosa tretjemu posredniku ([33]).

2.2 *Preglednost, upravljanje in nadzor zasebnostnega ščita EU-ZDA*

(30) Zasebnostni ščit EU-ZDA zagotavlja mehanizme nadzora in izvrševanja za preverjanje in zagotavljanje, da samocertificirana podjetja v ZDA spoštujejo načela in da se obravnava vsako nespoštovanje načel. Ti mehanizmi so določeni v načelih (Priloga II) ter zavezah Ministrstva za trgovino (Priloga I), FTC (Priloga IV) in Ministrstva za promet (Priloga V).

(31) Za zagotovitev pravilne uporabe zasebnostnega ščita EU-ZDA morajo biti zainteresirane strani, kot so posamezniki, na katere se nanašajo osebni podatki, izvozniki podatkov in nacionalni organi za varstvo podatkov, sposobne opredeliti organizacije, ki spoštujejo načela. V ta namen se mora Ministrstvo za trgovino zavezati, da bo vodilo seznam organizacij, ki so samocertificirale zavezanost k načelom in spadajo v pristojnost vsaj enega od organov pregona, navedenih v prilogah I in II k temu sklepu (v nadaljnjem besedilu: seznam zasebnostnega ščita) ([34]), ter javnosti omogočilo dostop do takega seznama. Ministrstvo za trgovino bo posodabljalo seznam na podlagi letnih izjav organizacij o ponovnem certificiranju ali kadar se organizacija umakne ali je umaknjena s seznama zasebnostnega ščita EU-ZDA. Vodilo bo tudi veljavno evidenco organizacij, ki so bile umaknjene s seznama, in javnosti omogočalo dostop do nje, pri čemer bo v vsakem primeru navedlo razloge za tako izključitev. Navedlo bo tudi povezavo do seznama zadev FTC v zvezi z izvrševanjem, povezanih z zasebnostnim ščitom, ki se hranijo na spletišču FTC.

(32) Ministrstvo za trgovino bo seznam zasebnostnega ščita in izjave o ponovnem certificiranju objavilo na posebnem spletišču, samocertificirane organizacije pa morajo navesti spletni naslov Ministrstva za seznam zasebnostnega ščita Poleg tega mora politika organizacije glede varstva zasebnosti, če je objavljena na spletu, vključevati hiperpovezavo do spletišča zasebnostnega ščita in hiperpovezavo do spletišča ali obrazca za vložitev pritožbe v okviru neodvisnega pritožbenega mehanizma, ki je na voljo za proučitev nerešenih pritožb. Ministrstvo za trgovino bo v okviru certificiranja in ponovnega certificiranja organizacije za okvir zasebnostnega ščita sistematično preverjalo, ali so njene politike varstva zasebnosti skladne z načeli.

(33) Organizacije, ki vztrajno ne spoštujejo načel, bodo umaknjene s seznama zasebnostnega ščita ter morajo vrniti ali izbrisati osebne podatke, prejete v okviru zasebnostnega ščita EU-ZDA. V drugih primerih umika, kot je prostovoljna prekinitev sodelovanja ali neizvedba ponovnega certificiranja, lahko organizacija zadrži take podatke, če Ministrstvu za trgovino vsako leto potrdi svojo zavezanost k nadaljnji uporabi načel ali zagotovi ustrezno varstvo osebnih podatkov z drugimi dovoljenimi sredstvi (npr. z uporabo pogodbe, ki v celoti izraža zahteve ustreznih standardnih pogodbenih klavzul, ki jih je odobrila Komisija). V tem primeru mora organizacija določiti kontaktno točko v organizaciji za vsa vprašanja, povezana z zasebnostnim ščitom.

(34) Ministrstvo za trgovino bo spremljalo organizacije, ki niso več članice zasebnostnega ščita EU-ZDA, bodisi zato, ker so se prostovoljno umaknile ali ker je njihovo potrdilo poteklo, da bi preverilo, ali bodo vrnile, izbrisale ali zadržale ([35]) osebne podatke, ki so jih predhodno prejele v okviru zasebnostnega ščita. Če organizacije zadržijo te

([32]) Stanje je različno, odvisno od tega, ali je tretja stranka upravljavec ali obdelovalec (posrednik). V prvem scenariju mora biti v pogodbi s tretjo stranko določeno, da tretja stranka preneha z obdelavo ali sprejme druge razumne in ustrezne ukrepe za izboljšanje stanja. V drugem scenariju mora te ukrepe sprejeti organizacija v zasebnostnem ščitu, ki nadzoruje obdelavo in po katere navodilih deluje posrednik.

([33]) V takem primeru mora tudi organizacija v ZDA sprejeti razumne in ustrezne ukrepe (i) za zagotovitev, da posrednik učinkovito obdeluje osebne podatke, ki se prenašajo v skladu z obveznostmi organizacije po načelih ter (ii) za ustavitev in prenehanje nedovoljene obdelave na podlagi obvestila.

([34]) Informacije o vodenju seznama zasebnostnega ščita so v Prilogi I in Prilogi II (člen I.3, člen I.4, člen III.6.d in člen III.11.g).

([35]) Glej npr. Prilogo II, člen I.3, člen III.6.f in člen III.11.g.i.

podatke, morajo še naprej uporabljati načela. Če Ministrstvo za trgovino izloči organizacije iz okvira zasebnostnega ščita zaradi vztrajnega nespoštovanja načel, zagotovi, da te organizacije vrnejo ali izbrišejo osebne podatke, ki so jih prejele v okviru zasebnostnega ščita.

(35) Če organizacija iz katerega koli razloga zapusti zasebnostni ščit EU-ZDA, mora umakniti vse javne izjave, ki kažejo na to, da še naprej sodeluje v zasebnostnem ščitu EU-ZDA ali da je upravičena do njegovih koristi, zlasti kakršna koli sklicevanja na zasebnostni varnostni ščit EU-ZDA v njeni objavljeni politiki varstva zasebnosti. Ministrstvo za trgovino bo iskalo in obravnavalo lažne navedbe o sodelovanju v okviru, tudi z nekdanjimi člani ([36]). Za vsako zavajanje širše javnosti v zvezi z zavezanostjo k načelom v obliki zavajajočih izjav ali praks lahko FTC, Ministrstvo za promet ali drugi ustrezni izvršni organi ZDA ukrepajo proti kršitvi; zavajanje Ministrstva za trgovino se lahko preganja po zakonu o lažnih navedbah (False Statements Act) (člen 1001 naslova 18 zakonodajne zbirke ZDA) ([37]).

(36) Ministrstvo za trgovino bo po uradni dolžnosti spremljalo kakršne koli lažne navedbe o sodelovanju v zasebnostnem ščitu ali nepravilno uporabo potrditvene oznake zasebnostnega ščita, organi za varstvo podatkov pa lahko napotijo organizacije na pregled na posebno kontaktno točko v okviru Ministrstva. Če se je organizacija umaknila iz zasebnostnega ščita EU-ZDA, se ni ponovno certificirala ali je umaknjena s seznama zasebnostnega ščita, bo Ministrstvo za trgovino redno preverjalo, ali je iz objavljene politike varstva zasebnosti izbrisala kakršna koli sklicevanja na zasebnostni ščit, ki kažejo na njeno nadaljnje sodelovanje, in, če še naprej podaja lažne navedbe, predalo zadevo FTC, Ministrstvu za promet ali drugemu pristojnemu organu, da izvedejo morebitne izvršilne ukrepe. Poslalo bo tudi vprašalnike organizacijam, ki se niso samocertificirale ali ki so se prostovoljno umaknile iz zasebnostnega ščita EU-ZDA, da bi preverilo, ali bo organizacija vrnila, izbrisala ali še naprej uporabljala načela zasebnosti za osebne podatke, ki jih je prejela med sodelovanjem v zasebnostnem ščitu EU-ZDA, in, če namerava osebne podatke zadržati, da bi preverilo, kdo v organizaciji bo stalna kontaktna točka za vprašanja, povezana z zasebnostnim ščitom.

(37) Ministrstvo za trgovino bo redno izvajalo preglede skladnosti samocertificiranih organizacij po uradni dolžnosti ([38]), tudi s pošiljanjem podrobnih vprašalnikov. Prav tako bo sistematično izvajalo preglede, kadar koli bo prejelo določeno (neutemeljeno) pritožbo, če organizacija ne zagotovi zadovoljivega odgovora na njegove poizvedbe ali če obstajajo verodostojni dokazi, da organizacija morda ne spoštuje načel. Po potrebi se bo o takih pregledih skladnosti posvetovalo tudi z organi za varstvo podatkov.

2.3 *Mehanizmi pravnega varstva, reševanje pritožb in izvrševanje*

(38) Zasebnostni ščit EU-ZDA v skladu z *načelom pritožbenega mehanizma, izvrševanja in odgovornosti* zahteva, da organizacije zagotovijo pritožbeni mehanizem za posameznike, na katere vpliva nespoštovanje načel, ter s tem možnost, da posamezniki iz EU, na katere se nanašajo osebni podatki, vložijo pritožbe v zvezi z nespoštovanjem načel s strani samocerticifiranih podjetij v ZDA in da se te pritožbe rešijo, če to zahteva odločitev, ki zagotavlja učinkovita pravna sredstva.

(39) Organizacije morajo v okviru samocertificiranja izpolnjevati zahteve načela pritožbenega mehanizma, izvrševanja in odgovornosti z zagotavljanjem učinkovitih in zlahka dostopnih neodvisnih pritožbenih mehanizmov, s katerimi se lahko pritožbe in spori vsakega posameznika raziščejo in hitro razrešijo brez stroškov za posameznika.

(40) Organizacije lahko izberejo neodvisne pritožbene mehanizme v Uniji ali ZDA. To vključuje možnost prostovoljne zaveza za sodelovanje z organi za varstvo podatkov EU. Vendar taka možnost ne obstaja, če organizacije

([36]) Glej člen o iskanju in obravnavi lažnih navedb o sodelovanju v Prilogi I.
([37]) Glej Prilogo II, člen III.6.h in člen III.11.f.
([38]) Glej Prilogo I.

obdelujejo podatke o človeških virih, saj je v takem primeru sodelovanje z organi za varstvo podatkov obvezno. Druge možnosti vključujejo neodvisno alternativno reševanje sporov ali v zasebnem sektorju razvite *programe za varstvo zasebnosti*, ki v svoja pravila vključujejo načela zasebnosti. Slednji morajo vključevati učinkovite mehanizme izvrševanja v skladu z zahtevami načela pritožbenega mehanizma, izvrševanja in odgovornosti. Organizacije morajo odpraviti vse težave, povezane z nespoštovanjem načel. Navesti morajo tudi, da zanje veljajo preiskovalna in izvršilna pooblastila FTC, Ministrstva za promet ali katerega koli drugega ameriškega zakonsko določenega organa.

(41) Tako okvir zasebnostnega ščita posameznikom, na katere se nanašajo osebni podatki, zagotavlja številne možnosti, da uveljavljajo svoje pravice, vložijo pritožbe v zvezi z nespoštovanjem načel s strani samocertificiranih podjetij v ZDA in da se te pritožbe rešijo, če to zahteva odločitev, ki zagotavlja učinkovita pravna sredstva. Posamezniki lahko vložijo pritožbo neposredno pri organizaciji, neodvisnem organu za reševanje sporov, ki ga imenuje organizacija, pri nacionalnih organih za varstvo podatkov ali FTC.

(42) Če se njihove pritožbe ne rešijo z nobenim od teh pritožbenih mehanizmov ali mehanizmov izvrševanja, lahko uveljavljajo zavezujočo arbitražo senata zasebnostnega ščita (Priloga 1 Priloge II tega sklepa). Razen za arbitražni senat, za katerega je treba pred uveljavitvijo izčrpati nekatera pravna sredstva, lahko posamezniki uporabijo kateri koli ali vse mehanizme pravnega varstva po lastni izbiri in jim ni treba izbrati določenega mehanizma ali slediti določenemu zaporedju. Vendar obstaja določeno logično zaporedje, ki mu je priporočljivo slediti, kot je opisano v nadaljevanju.

(43) Prvič, posamezniki iz EU, na katere se nanašajo osebni podatki, lahko spremljajo primere nespoštovanja načel z neposrednimi stiki s *samocertificiranim podjetjem v ZDA*. Za lažje reševanje pritožb mora organizacija vzpostaviti učinkovit mehanizem pravnega varstva za obravnavanje takih pritožb. Zato mora politika organizacije glede varstva zasebnosti jasno obveščati posameznike o kontaktni točki, bodisi v organizaciji ali zunaj nje, ki bo obravnavala pritožbe (vključno s katero koli ustrezno organizacijo v Uniji, ki lahko odgovarja na poizvedbe ali pritožbe), in o neodvisnih mehanizmih za obravnavo pritožb.

(44) Organizacija mora po prejemu pritožbe, neposredno od posameznika ali prek Ministrstva za trgovino na podlagi napotitve organa za varstvo podatkov, posamezniku v EU, na katerega se nanašajo osebni podatki, odgovoriti v 45 dneh. Ta odgovor mora vključevati oceno utemeljenosti pritožbe in, v primeru utemeljenosti pritožbe, informacije o tem, kako bo organizacija rešila težavo. Podobno morajo organizacije nemudoma odgovoriti na poizvedbe in druge zahteve za informacije s strani Ministrstva za trgovino ali organa za varstvo ([39]) (če se je organizacija zavezala, da bo sodelovala z organom za varstvo podatkov), ki se nanašajo na njihovo spoštovanje načel. Organizacije morajo voditi tudi evidenco o izvajanju politike varstva zasebnosti in jo na zahtevo v okviru preiskave ali pritožbe zaradi nespoštovanja načel dati na voljo neodvisnemu pritožbenemu mehanizmu ali FTC (ali drugemu organu ZDA s pristojnostjo za preiskovanje nepoštenih ali goljufivih dejanj).

(45) Drugič, posamezniki lahko vložijo pritožbo tudi neposredno pri *neodvisnem organu za reševanje sporov* (v ZDA ali Uniji), ki ga imenuje organizacija za preiskovanje in reševanje posameznih pritožb (razen če so očitno neutemeljene ali neresne) ter zagotovitev ustreznih pravnih sredstev, ki so za posameznika brezplačna. Sankcije in pravna sredstva, ki jih naloži tak organ, morajo biti dovolj stroga, da zagotavljajo spoštovanje načel s strani organizacij, in bi morala določati, da morajo organizacije odpraviti ali popraviti učinke neskladnosti ter, odvisno od okoliščin, prenehati obdelovati zadevne osebne podatke in/ali jih izbrisati ter objaviti ugotovitev o neskladnosti. Neodvisni organi za reševanje sporov, ki jih imenuje organizacija, bodo morali na svoja javna spletišča vključiti ustrezne informacije v zvezi z zasebnostnim ščitom EU-ZDA in storitvami, ki jih zagotavljajo v njegovem okviru. Vsako leto morajo objaviti letno poročilo s skupnimi statističnimi podatki v zvezi s temi storitvami ([40]).

([39]) To je organ za obravnavanje pritožb, ki ga imenuje senat organov za varstvo podatkov, določen v dopolnilnem načelu o vlogi organov za varstvo podatkov (Priloga II, člen III.5).

([40]) Letno poročilo mora vsebovati: (1) skupno število pritožb, povezanih z zasebnostnim ščitom, prejetih v letu poročanja; (2) vrste prejetih pritožb; (3) merila kakovosti reševanja sporov, kot je čas, porabljen za obdelavo pritožb in (4) izide prejetih pritožb, zlasti število in vrste pravnih sredstev ali uvedenih sankcij.

(46) Ministrstvo za trgovino bo v okviru postopkov pregleda skladnosti preverilo, ali so se samocerticifirana podjetja v ZDA dejansko registrirala v neodvisnih pritožbenih mehanizmih, v katerih naj bi bila po njihovih trditvah registrirana. Organizacije in odgovorni neodvisni pritožbeni mehanizmi morajo nemudoma odgovoriti na poizvedbe in zahteve Ministrstva za trgovino za informacije v zvezi z zasebnostnim ščitom.

(47) Če organizacija ne upošteva odločitve v zvezi z rešitvijo spora ali samoregulativnega organa, mora slednji o taki neskladnosti obvestiti Ministrstvo za trgovino in FTC (ali drug organ ZDA s pristojnostjo za preiskovanje nepoštenih ali goljufivih praks) ter pristojno sodišče ([41]). Če organizacija noče ravnati v skladu s končno ugotovitvijo organa s samourejevalnim sistemom za varstvo zasebnosti, neodvisnega organa za reševanje sporov ali vladnega organa ali kadar tak organ ugotovi, da organizacija pogosto ravna proti načelom, se to šteje za vztrajno nespoštovanje načel, zaradi česar Ministrstvo za trgovino po izteku 30-dnevnega roka, v katerem ima organizacija, ki ni ravnala v skladu z načeli, možnost odziva, črta organizacijo s seznama ([42]). Če se organizacija po umiku s seznama še naprej sklicuje na certifikacijo v okviru zasebnostnega ščita, Ministrstvo preda zadevo FTC ali drugemu organu pregona ([43]).

(48) Tretjič, posamezniki lahko vložijo pritožbo tudi pri nacionalnem *organu za varstvo podatkov*. Organizacije morajo sodelovati pri preiskavi in reševanju pritožbe organa za varstvo podatkov, če se nanaša na obdelavo podatkov o človeških virih, zbranih v okviru zaposlitvenega razmerja, ali če so se prostovoljno sprejele nadzor organov za varstvo podatkov. Predvsem morajo odgovarjati na poizvedbe, upoštevati nasvete organa za varstvo podatkov, vključno glede reševanja pritožb in izplačila odškodnin, ter predložiti organu za varstvo podatkov pisno potrdilo, da so bili taki ukrepi sprejeti.

(49) Nasvete organov za varstvo podatkov bo posredoval neuradni senat organov za varstvo podatkov, ustanovljen na ravni Unije ([44]), ki bo pomagal zagotoviti usklajen in skladen pristop k posamezni pritožbi. Nasvet bo izdan, ko bosta oba udeleženca v sporu imela ustrezno priložnost za predložitev pripomb in kakršnih koli dokazov. Senat bo dal nasvet kakor, hitro to dopušča zahteva po dolžnem pravnem postopanju, praviloma v 60 dneh po prejemu pritožbe. Če organizacija tudi po 25 dneh po prejemu nasveta ne ravna v skladu z njim in če za zamudo ne poda zadovoljive obrazložitve, senat sporoči svojo namero, da bo bodisi predložil zadevo FTC (ali drugemu izvršnemu organu ZDA) bodisi sklenil, da gre za resno kršitev zaveze o sodelovanju. Pri prvi možnosti lahko to vodi do pregona na podlagi člena 5 zakona o FTC (ali podobnega zakona). Pri drugi možnosti bo senat obvestil Ministrstvo za trgovino, ki bo neupoštevanje nasveta senata organov za varstvo podatkov obravnavalo kot vztrajno neizpolnjevanje načel, zaradi česar bo organizacija črtana s seznama zasebnostnega ščita.

(50) Če organ za varstvo podatkov, na katerega je bila naslovljena pritožba, ni ukrepal ali ni sprejel zadostnih ukrepov za obravnavo pritožbe, lahko posamezni pritožnik izpodbija tako (ne)ukrepanje pri nacionalnih sodiščih zadevne države članice.

(51) Posamezniki lahko pritožbo pri organih za varstvo podatkov vložijo tudi, če senat organov za varstvo podatkov ni bil imenovan kot organ za reševanje sporov organizacije. V takih primerih lahko organ za varstvo podatkov posreduje take pritožbe Ministrstvu za trgovino ali FTC. Ministrstvo za trgovino bo za olajšanje in povečanje sodelovanja na področju zadev, povezanih s posameznimi pritožbami in nespoštovanjem načel s strani organizacij v zasebnostnem ščitu, vzpostavilo posebno kontaktno točko, ki bo delovala kot povezovalna točka in bo pomagala organu za varstvo podatkov pri poizvedbah v zvezi s spoštovanjem načel s strani organizacije ([45]). FTC se je tudi zavezala, da bo vzpostavila posebno kontaktno točko ([46]) in organu za varstvo podatkov nudila pomoč pri preiskavah v skladu z zakonom ZDA o spletni varnosti (U.S. SAFE WEB Act) ([47]).

([41]) Glej Prilogo II, člen III.11.e.
([42]) Glej Prilogo II, člen III.11.g, zlasti točki (ii) in (iii).
([43]) Glej člen o iskanju in obravnavi lažnih navedb o sodelovanju v Prilogi I.
([44]) Organi za varstvo podatkov bi morali pripraviti poslovnik neuradnega senata organov za varstvo podatkov na podlagi svoje pristojnosti za organizacijo dela in medsebojno sodelovanje.
([45]) Glej člen o okrepitvi sodelovanja z organi za varstvo podatkov in člen o olajšanju reševanja pritožb zaradi nespoštovanja načel v Prilogi I ter Prilogo II, člen II.7.e.
([46]) Glej str. 6 Priloge IV.
([47]) Glej prejšnjo opombo.

(52) Četrtič, *Ministrstvo za trgovino* se je zavezalo, da bo sprejemalo, pregledalo in si po najboljših močeh prizadevalo rešiti pritožbe o nespoštovanju načel s strani organizacije. V ta namen Ministrstvo za trgovino zagotavlja posebne postopke, s katerimi organi za varstvo podatkov posredujejo pritožbe posebni kontaktni točki, jih spremljajo in skupaj s podjetji določijo nadaljnje ukrepe za olajšanje reševanja. Da bi pospešila obdelavo posameznih pritožb, se bo kontaktna točka neposredno povezala z ustreznim organom za varstvo podatkov glede težav v zvezi s skladnostjo in ga najpozneje v 90 dneh od predložitve pritožbe zlasti obvestila o statusu pritožbe. To posameznikom, na katere se nanašajo osebni podatki, omogoča, da pritožbe zaradi neskladnosti samocertificiranih podjetij v ZDA predložijo neposredno svojim nacionalnim organom za varstvo podatkov in jih posredujejo Ministrstvu za trgovino kot organu ZDA, ki upravlja zasebnostni ščit EU-ZDA. Ministrstvo za trgovino se je tudi zavezalo, da bo v okviru letnega pregleda delovanja zasebnostnega ščita EU-ZDA predložilo poročilo, v katerem bodo v obliki povzetka analizirane pritožbe, ki jih prejme vsako leto ([48]).

(53) Če Ministrstvo za trgovino na podlagi preverjanj po uradni dolžnosti, pritožb ali kakršnih koli drugih informacij sklene, da organizacija vztrajno ne spoštuje načel zasebnosti, umakne tako organizacijo s seznama zasebnostnega ščita. Če kateri koli samoregulativni organ za varstvo zasebnosti, neodvisni organ za reševanje sporov ali vladni organ, vključno z organom za varstvo podatkov, noče ravnati v skladu s končno odločitvijo, se to šteje za vztrajno neizpolnjevanje načel.

(54) Petič, za organizacijo v zasebnostnem ščitu morajo veljati preiskovalna in izvršilna pooblastila organov ZDA, zlasti *Zvezne komisije za trgovino* ([49]), ki bo učinkovito zagotavljala skladnost z načeli. FTC bo prednostno obravnavala sporočene zadeve glede nespoštovanja načel zasebnosti, ki jih je prejela od neodvisnih organov za reševanje sporov ali samoregulativnih organov, Ministrstva za trgovino in organov za varstvo podatkov (ki delujejo na lastno pobudo ali na podlagi pritožb), da bi ugotovila, ali je bil kršen člen 5 zakona o FTC ([50]). FTC se je zavezala, da bo oblikovala standardiziran postopek za pošiljanje zadev, imenovala kontaktno točko organa za zadeve, ki jih sporoči organ za varstvo podatkov, in izmenjevala informacije o sporočenih zadevah. Poleg tega bo sprejemala pritožbe neposredno od posameznikov in na lastno pobudo izvajala preiskave zasebnostnega ščita, zlasti v okviru obsežnejših preiskav zadev v zvezi z zasebnostjo.

(55) FTC lahko zagotavlja skladnost z upravnimi odločbami (v nadaljnjem besedilu: odločba o soglasju) in bo sistematično spremljala spoštovanje takih odločb. Če organizacije ne spoštujejo takih odločb, lahko FTC predloži zadevo pristojnemu sodišču za uveljavitev denarnih kazni in drugih pravnih sredstev, tudi za škodo, povzročeno s protipravnim ravnanjem. FTC lahko pri zveznem sodišču tudi neposredno zaprosi za predhodno ali trajno prepoved ali druga pravna sredstva. Vsaka odločba o soglasju, ki jo izda organizacija v zasebnostnem ščitu, bo vsebovala določbe o samoporočanju ([51]), organizacije pa bodo morale objaviti vse ustrezne dele katerega koli poročila o skladnosti ali ocenjevalnega poročila, predloženega FTC, ki se nanašajo na zasebnostni ščit. FTC bo vodila tudi spletni seznam podjetij, za katera veljajo odločbe FTC ali sodne odločbe v zadevah, povezanih z zasebnostnim ščitom.

(56) Šestič, če se pritožba posameznika ne reši z uporabo katere od navedenih možnosti pravnega varstva, lahko posameznik iz EU, na katerega se nanašajo osebni podatki, v skrajnem primeru zaprosi za zavezujočo arbitražo *„senata zasebnostnega ščita“*. Organizacije morajo obvestiti posameznike o njihovi možnosti, da pod določenimi pogoji uveljavijo zavezujočo arbitražo, in se po uveljavitvi te možnosti s strani posameznika odzvati tako, da pošljejo obvestilo zadevni organizaciji ([52]).

([48]) Glej člen o olajšanju reševanja pritožb zaradi nespoštovanja načel v Prilogi I.

([49]) Organizacija v zasebnostnem ščitu se mora javno zavezati k spoštovanju načel, javno razkriti svoje politike varstva zasebnosti v skladu s temi načeli in jih v celoti izvajati. Nespoštovanje načel se preganja na podlagi člena 5 zakona o FTC, ki prepoveduje nepoštena in goljufiva dejanja v trgovini ali v zvezi z njo.

([50]) FTC glede na informacije, ki jih je podala, nima pooblastil za izvajanje pregledov na kraju samem na področju varstva zasebnosti. Vendar ima pooblastila, da od organizacij zahteva, da predložijo dokumente in izjave prič (glej člen 20 zakona o FTC), ter lahko v primeru neizpolnitve uporabi sodni sistem za izvršitev takih odločb.

([51]) Odločbe FTC ali sodne odločbe lahko vsebujejo zahtevo, da podjetja izvajajo programe zasebnosti in redno pripravljajo poročila o skladnosti ali ocene neodvisnih tretjih strani za zadevne programe, ki so na voljo FTC.

([52]) Glej Prilogo II, člena II.1.xi in III.7.c.

(57) Ta arbitražni senat bo sestavljala skupina najmanj 20 arbitrov, ki jih imenujeta Ministrstvo za trgovino in Komisija na podlagi njihove neodvisnosti, integritete, pa tudi izkušenj na področju zakonodaje ZDA o varstvu zasebnosti in zakonodaje Unije o varstvu podatkov. Strani za vsak posamezni spor iz te skupine izbereta senat z enim ali tremi ([53]) arbitri. Postopke urejajo standardna pravila arbitraže, o katerih se dogovorita Ministrstvo za trgovino in Komisija. Ta pravila bodo dopolnjevala že dogovorjeni okvir, ki vsebuje več elementov, ki povečujejo dostopnost tega mehanizma za posameznike iz EU, na katere se nanašajo osebni podatki: (i) posameznikom, na katere se nanašajo osebni podatki, lahko pri pripravi zahtevka pred senatom pomagajo njihovi nacionalni organi za varstvo podatkov; (ii) arbitraža sicer poteka v ZDA, vendar se lahko posamezniki iz EU, na katere se nanašajo osebni podatki, odločijo, da bodo sodelovali prek video ali telefonske konference, ki je za posameznika brezplačna; (iii) čeprav je jezik, ki se uporablja pri arbitraži, praviloma angleščina, se tolmačenje na arbitražnem zaslišanju in prevod na utemeljeno zahtevo posameznika, na katerega se nanašajo osebni podatki, običajno ([54]) zagotovita brezplačno; (iv) nenazadnje, čeprav mora vsaka stran v primeru, da jo pred senatom zastopa odvetnik, kriti svoje odvetniške stroške, bo Ministrstvo za trgovino ustanovilo sklad, v katerem se bodo zbirali letni prispevki organizacij v zasebnostnem ščitu in ki bo kril upravičene stroške arbitražnega postopka do najvišjih določenih zneskov, ki jih določijo organi ZDA v posvetovanju s Komisijo.

(58) Senat zasebnostnega ščita lahko zahteva „nedenarno pravično nadomestilo za posameznika“ ([55]), ki je potrebno za odpravo nespoštovanja načel. Čeprav senat upošteva druga pravna sredstva, ki so bila že pridobljena z drugimi mehanizmi zasebnostnega ščita med njegovim odločanjem, lahko posamezniki še vedno uporabijo arbitražo, če menijo, da so ta druga pravna sredstva nezadostna. To posameznikom iz EU, na katere se nanašajo osebni podatki, omogoča, da uporabijo arbitražo v vseh primerih, kjer se z ukrepanjem ali neukrepanjem pristojnih organov ZDA (na primer FTC) njihove pritožbe niso zadovoljivo rešile. Arbitraže ni dovoljeno začeti, če ima organ za varstvo podatkov pravno pooblastilo za rešitev zadevnega zahtevka v zvezi s samocertificiranim podjetjem iz ZDA, in sicer v primerih, ko je organizacija bodisi dolžna sodelovati in upoštevati nasvet organov za varstvo podatkov, kar zadeva obdelavo podatkov o človeških virih, zbranih v okviru zaposlovanja, ali se je k temu prostovoljno zavezala. Posamezniki lahko izvršijo arbitražno odločbo pred sodišči ZDA na podlagi zveznega zakona o arbitraži (Federal Arbitration Act), s čimer zagotovijo pravno sredstvo v primeru, da podjetje ne izpolni obveznosti.

(59) Sedmič če organizacija ne izpolnjuje zavez v zvezi z načeli in objavljeno politiko varstva zasebnosti, so po zakonodaji držav ZDA morda na voljo dodatne možnosti sodnega varstva, ki zagotavljajo pravna sredstva po odškodninskem pravu in v primeru goljufivih lažnih navedb, nepoštenih ali goljufivih dejanj ali kršitve pogodbe.

(60) Nenazadnje, če organ za varstvo podatkov po prejemu zahtevka posameznika iz EU, na katerega se nanašajo osebni podatki, meni, da za osebne podatke posameznika, prenesene na organizacijo v ZDA, ni zagotovljena ustrezna raven varstva, lahko uveljavlja tudi svoja pooblastila v zvezi z izvoznikom podatkov in po potrebi ustavi prenos podatkov.

(61) Komisija ob upoštevanju informacij v tem členu meni, da načela, ki jih je izdalo Ministrstvo za trgovino ZDA, kot taka zagotavljajo raven varstva osebnih podatkov, ki je v bistvenem enaka ravni, ki jo zagotavljajo osnovna vsebinska načela, določena v Direktivi 95/46/ES.

(62) Poleg tega je učinkovita uporaba načel zagotovljena z obveznostmi glede preglednosti ter upravljanjem in pregledom skladnosti zasebnostnega ščita s strani Ministrstva za trgovino.

(63) Komisija tudi meni, da nadzorni in pritožbeni mehanizmi ter mehanizmi izvrševanja, ki jih zagotavlja zasebnostni ščit, kot celota omogočajo ugotavljanje kršitev načel s strani organizacij v zasebnostnem ščitu in njihovo kaznovanje v praksi ter posamezniku, na katerega se nanašajo osebni podatki, ponujajo pravna sredstva za pridobitev dostopa do osebnih podatkov, povezanih z njim, in, na koncu, popravek ali izbris takih podatkov.

([53]) Strani se morata dogovoriti o številu arbitrov v senatu.
([54]) Vendar lahko senat ugotovi, da bo kritje v okoliščinah posebne arbitraže povzročilo neupravičene ali nesorazmerne stroške.
([55]) Posamezniki lahko v arbitraži zahtevajo odškodnino, vendar uporaba arbitraže ne izključuje možnosti za vložitev zahtevka za odškodnino na rednih sodiščih v ZDA.

3. DOSTOP DO OSEBNIH PODATKOV, KI JIH JAVNI ORGANI PRENAŠAJO V OKVIRU ZASEBNOSTNEGA ŠČITA EU-ZDA, IN NJIHOVA UPORABA

(64) Kot izhaja iz člena I.5 Priloge II, je spoštovanje načel omejeno na tisto, kar je potrebno za izpolnitev zahtev glede nacionalne varnosti, javnega interesa ali kazenskega pregona.

(65) Komisija je ocenila omejitve in zaščitne ukrepe, ki so na voljo v zakonodaji ZDA, kar zadeva dostop in uporabo osebnih podatkov, ki jih javni organi v ZDA prenašajo v okviru zasebnostnega ščita EU-ZDA za namene nacionalne varnosti, kazenskega pregona in drugih javnih interesov. Poleg tega je vlada ZDA prek urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence, v nadaljnjem besedilu: ODNI) ([56]) Komisiji predložila podrobna zagotovila in zaveze, vsebovane v Prilogi VI k temu sklepu. Z dopisom, ki ga je podpisal državni sekretar in ki je priložen kot Priloga III k temu sklepu, se je vlada ZDA tudi zavezala, da bo ustvarila nov nadzorni mehanizem za posege na področju nacionalne varnosti, varuha človekovih pravic na področju zasebnostnega ščita, ki bo neodvisen od obveščevalne skupnosti. Zagotovilo Ministrstva za obrambo ZDA, vsebovano v Prilogi VII k temu sklepu, opisuje omejitve in zaščitne ukrepe, ki se uporabljajo za dostop do podatkov in njihovo uporabo s strani javnih organov pregona in za druge namene javnega interesa. Za povečanje preglednosti in izražanje pravne narave teh zavez bo vsak od dokumentov, navedenih v in priloženih temu sklepu, objavljen v zveznem registru ZDA.

(66) Ugotovitve Komisije glede omejitev dostopa in uporabe osebnih podatkov, ki jih javni organi ZDA prenašajo iz Evropske unije v ZDA, in obstoja učinkovitega pravnega varstva so podrobneje pojasnjene v nadaljevanju.

3.1 *Dostop in uporaba s strani javnih organov ZDA za namene nacionalne varnosti*

(67) Analiza Komisije kaže, da zakonodaja ZDA vsebuje številne omejitve glede dostopa do osebnih podatkov in njihove uporabe, ki se prenašajo v okviru zasebnostnega ščita EU-ZDA za namene socialne varnosti, pa tudi nadzornih in pritožbenih mehanizmov, ki zagotavljajo dovolj zaščitnih ukrepov, da so zadevni podatki učinkovito zaščiteni proti nezakonitim posegom in nevarnosti zlorabe ([57]). Od leta 2013, ko je Komisija izdala dve sporočili (glej uvodno izjavo 7), se je ta pravni okvir znatno okrepil, kakor je opisano v nadaljevanju.

3.1.1 Omejitve

(68) Po zakonodaji ZDA je zagotavljanje nacionalne varnosti v pristojnosti predsednika kot glavnega poveljnika, glavnega upravitelja in, kar zadeva tuje obveščevalne službe, kot pristojnega za zunanje zadeva ZDA ([58]). Ker ima kongres pristojnosti za uvedbo omejitev in je to storil v različnih primerih, lahko v okviru teh omejitev usmerja dejavnosti obveščevalne skupnosti ZDA, zlasti z odredbami ali predsedniškimi direktivami. To seveda velja tudi za področja, za katera ni nobenih kongresnih smernic. Trenutno sta glavna pravna instrumenta v zvezi s tem Odredba št. 12333 ([59]) in Predsedniška politična direktiva št. 28 (Presidential Policy Directive 28, v nadaljnjem besedilu: PPD-28).

([56]) Direktor nacionalne obveščevalne službe (DNI) vodi obveščevalno skupnost ter deluje kot glavni svetovalec predsednika in Sveta za nacionalno varnost. Glej zakon o reformi obveščevalne službe in preprečevanju terorizma (Intelligence Reform and Terrorism Prevention Act) iz leta 2004, Zbirka aktov Kongresa s področja javnega prava, št. 108–458 z dne 17. 12. 2004. ODNI med drugim določi zahteve za zbiranje, analizo, pripravo in razširjanje nacionalnih obveščevalnih podatkov s strani obveščevalne skupnosti ter upravlja in vodi dodeljevanje nalog, vključno s pripravo smernic o načinu dostopa do informacij ali obveščevalnih podatkov, njihovi uporabi in izmenjavi. Glej člen 1.3(a) in (b) Odredbe 12333.

([57]) Glej zadevo Schrems, točka 91.

([58]) Ustava ZDA, člen II. Glej tudi uvod k Predsedniški politični direktivi št. 28.

([59]) Odredba št. 12333: Obveščevalne dejavnosti ZDA (United States Intelligence Activities), Zvezni register, zvezek 40, št. 235 (8. december 1981). V obsegu, v katerem je odredba javno dostopna, opredeljuje cilje, usmeritve, naloge in odgovornosti v zvezi z obveščevalnimi dejavnostmi ZDA (vključno z vlogo različnih organov obveščevalne skupnosti) ter določa splošne parametre za izvajanje obveščevalnih dejavnosti (zlasti potrebo po razglasitvi posebnih postopkovnih pravil). V skladu s členom 3.2 Odredbe št. 12333 predsednik, ki ga podpira Svet za nacionalno varnost, in direktor nacionalne obveščevalne službe izdata take ustrezne direktive, postopke in smernice, kot so potrebni za izvajanje odredbe.

(69) Predsedniška politična direktiva št. 28 (v nadaljnjem besedilu: PPD-28), objavljena 17. januarja 2014, uvaja številne omejitve za „obveščevalne operacije SIGINT“ ([60]). Ta predsedniška direktiva je zavezujoča za obveščevalne organe ZDA ([61]) in ostane veljavna po spremembi v administraciji ZDA ([62]). PPD-28 je zlasti pomembna za nedržavljane ZDA, vključno s posamezniki iz EU, na katere se nanašajo osebni podatki. Med drugim določa da:

(a) mora zbiranje obveščevalnih podatkov SIGINT temeljiti na statutu ali predsedniškem pooblastilu ter se mora izvajati v skladu z ustavo ZDA (zlasti četrtim amandmajem) in zakonodajo ZDA;

(b) bi se morale vse osebe obravnavati z dostojanstvom in spoštovanjem, ne glede na njihovo državljanstvo ali prebivališče;

(c) imajo vse osebe legitimne interese za varstvo zasebnosti pri obdelavi njihovih osebnih podatkov;

(d) so zasebnost in državljanske svoboščine sestavni del premislekov pri načrtovanju obveščevalnih dejavnosti SIGINT v ZDA;

(e) morajo obveščevalne dejavnosti SIGINT v ZDA zato vključevati ustrezne zaščitne ukrepe za osebne podatke vseh posameznikov, ne glede na njihovo državljanstvo ali prebivališče.

(70) PPD-28 določa, da se lahko obveščevalni podatki SIGINT zbirajo izključno za namen tujih obveščevalnih služb in protiobveščevalnih služb za podporo nacionalnim in ministrskim misijam, ne pa za kateri koli drug namen (npr. za zagotavljanje konkurenčne prednosti podjetjem iz ZDA). V zvezi s tem ODNI pojasnjuje, da bi morali organi obveščevalne skupnosti „zahtevati, da se zbiranje podatkov, kadar je to izvedljivo, osredotoča na posebne cilje ali teme zbiranja tujih obveščevalnih podatkov z uporabo diskriminant (npr. posebni pripomočki, izbirni izrazi, identifikatorji)“ ([63]). Poleg tega iz zagotovil izhaja, da odločitve glede zbiranja obveščevalnih podatkov niso prepuščene presoji posameznih obveščevalnih agentov, ampak so predmet politik in postopkov, ki jih morajo vzpostaviti različni organi (agencije) obveščevalne skupnosti ZDA za izvajanje PPD-28 ([64]). V skladu s tem v skupnem „okviru prednostnih nalog nacionalnih obveščevalnih služb (National Intelligence Priorities Framework, v nadaljnjem besedilu: NIPF)“ potekajo tudi raziskave in določanje ustreznih izbirnikov, kar zagotavlja, da prednostne naloge obveščevalnih služb določijo oblikovalci politik na visoki ravni in da se te prednostne naloge redno pregledujejo, da se še naprej odzivajo na dejanske grožnje nacionalni varnosti in da se upoštevajo morebitna tveganja, vključno s tveganji za zasebnost ([65]). Na podlagi tega osebje agencije prouči in določi posebne izbirne izraze, s pomočjo katerih naj bi se zbirali tuji obveščevalni podatki, prilagojeni prednostnim nalogam ([66]). Izbirne izraze oziroma „izbirnike“ je treba redno pregledovati, da se preveri, ali še vedno zagotavljajo dragocene obveščevalne podatke v skladu s prednostnimi nalogami ([67]).

([60]) V skladu z Odredbo št. 12333 je direktor Agencije za nacionalno varnost (National Security Agency, v nadaljnjem besedilu: NSA) funkcionalni vodja zbiranja obveščevalnih podatkov SIGINT in vodi enotno organizacijo za obveščevalne dejavnosti SIGINT.

([61]) Za opredelitev pojma „obveščevalna skupnost“ glej člen 3.5(h) Odredbe št. 12333 z opombo 1 PPD-28.

([62]) Glej memorandum Urada pravnega svetovalca, Ministrstva za pravosodje, predsedniku Clintonu, 29. januar 2000. V skladu s tem pravnim mnenjem imajo predsedniške direktive „enak vsebinski pravni učinek kot odredba“.

([63]) Zagotovila ODNI (Priloga VI), str. 3.

([64]) Glej člen 4(b) in (c) PPD-28. Glede na javne podatke je bilo v pregledu za leto 2015 potrjenih šest obstoječih namenov. Glej poročilo ODNI o napredku pri reformi zbiranja obveščevalnih podatkov SIGINT za leto 2016 (Signals Intelligence Reform, 2016 Progress Report).

([65]) Zagotovila ODNI (Priloga VI), str. 6 (s sklicevanjem na direktivo o obveščevalni skupnosti št. 204 (Intelligence Community Directive 204). Glej tudi člen 3 PPD-28.

([66]) Zagotovila ODNI (Priloga VI), str. 6. Glej na primer poročilo Urada NSA za državljanske svoboščine in zasebnost (NSA Civil Liberties and Privacy Office, v nadaljnjem besedilu: NSA CLPO) NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 (Varstvo državljanskih svoboščin in zasebnosti s strani NSA za ciljne obveščevalne dejavnosti SIGINT na podlagi Odredbe št. 12333), 7. oktober 2014. Glej tudi poročilo ODNI o stanju za leto 2014. Poizvedbe v zvezi z zahtevami za dostop v skladu s členom 702 zakona o nadzoru tujih obveščevalnih podatkov urejajo postopki zmanjševanja količine podatkov, ki jih odobri sodišče za nadzor tujih obveščevalnih podatkov. Glej poročilo NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act (Izvajanje člena 702 zakona o nadzoru tujih obveščevalnih podatkov s strani NSA), 16. april 2014.

([67]) Glej jubilejno poročilo za leto 2015 Signal Intelligence Reform (Reforma zbiranja obveščevalnih podatkov SIGINT). Glej tudi zagotovila ODNI (Priloga VI), str. 6, 8–9, 11.

(71) Poleg tega zahtevi, določeni v PPD-28, da mora biti zbiranje vedno ([68])„prilagojeno in izvedljivo“ in da mora obveščevalna skupnost dajati prednost razpoložljivosti drugih informacij ter ustreznim in izvedljivim alternativam ([69]), izražata splošno pravilo dajanja prednosti ciljnemu zbiranju podatkov pred množičnim zbiranjem podatkov. V skladu z zagotovili ODNI zagotavljata zlasti, da množično zbiranje ni niti „masovno“ niti „neselektivno“ in da izjema ne razveljavi pravila ([70]).

(72) Čeprav PPD-28 pojasnjuje, da morajo organi obveščevalne skupnosti včasih v določenih okoliščinah zbirati množične obveščevalne podatke SIGINT, na primer za ugotavljanje in oceno novih ali nastajajočih groženj, določa, da morajo ti organi dajati prednost alternativam, ki omogočajo izvajanje ciljnega zbiranja obveščevalnih podatkov SIGINT ([71]). Iz tega sledi, da se množično zbiranje podatkov izvaja le, če ciljno zbiranje podatkov z uporabo diskriminant, tj. identifikatorja, povezanega z določeno ciljno osebo (kot je e-poštni naslov ali telefonska številka ciljne osebe), ni mogoče „zaradi tehničnih ali operativnih razlogov“ ([72]). To se nanaša na način zbiranja obveščevalnih podatkov SIGINT in na dejansko zbrane podatke ([72]).

(73) V skladu z zagotovili ODNI obveščevalna skupnost tudi v primeru, če ne more uporabiti posebnih identifikatorjev za ciljno zbiranje podatkov, poskuša „čim bolj“ omejiti zbiranje. Za zagotovitev tega „uporablja filtre in druga tehnična orodja za osredotočanje zbiranja na tiste elemente, ki verjetno vsebujejo komunikacije, ki so pomembne za tuje obveščevalne službe“ (in bodo tako ustrezali zahtevam, ki so jih izrazili oblikovalci politike ZDA v skladu s postopkom, opisanim v uvodni izjavi 70). Zato bo množično zbiranje ciljno usmerjeno na vsaj dva načina. Prvič, vedno bo povezano z določenimi cilji tuje obveščevalne službe (npr. pridobivanje obveščevalnih podatkov SIGINT o dejavnostih teroristične skupine, ki deluje v določeni regiji) in osredotočalo se bo na komunikacije, ki so povezane s takimi cilji. Glede na zagotovilo ODNI se to izraža v dejstvu, da „obveščevalne dejavnosti SIGINT ZDA dosežejo le del komunikacij, ki potekajo prek interneta“ ([73]). Drugič, v zagotovilih ODNI je pojasnjeno, da bodo filtri in druga tehnična orodja, ki se uporabljajo, zasnovana tako, da se bodo osredotočala na „čim bolj natančno“ zbiranje za zagotovitev, da bo zbranih čim manj „neustreznih informacij“.

(74) Tudi kadar ZDA menijo, da je treba obveščevalne podatke zbirati množično, v skladu s pogoji, določenimi v uvodnih izjavah 70 do 73, Predsedniška politična direktiva št. 28 omejuje uporabo takih podatkov na določen seznam šestih namenov nacionalne varnosti za varstvo zasebnosti in državljanskih pravic vseh oseb, ne glede na njihovo državljanstvo in prebivališče ([74]). Ti dovoljeni nameni vključujejo ukrepe za odkrivanje in preprečevanje groženj oboroženim silam ali vojaškemu osebju, ki izhajajo iz vohunstva, terorizma, orožja za množično

([68]) Glej zagotovila ODNI (Priloga VI), str. 3.

([69]) Opozoriti je treba tudi, da v skladu s členom 2.4 Odredbe 12333 organi obveščevalne skupnosti „uporabljajo najmanj vsiljive tehnike zbiranja podatkov, ki so izvedljive v ZDA“. Glede omejitev nadomestitve množičnega zbiranja podatkov s ciljnim zbiranjem glej rezultate ocene nacionalnega raziskovalnega sveta, kot jih je sporočila Agencija Evropske unije za temeljne pravice (Fundamental Rights Agency), Surveillance by Intelligence Services: fundamental rights, safeguards and remedies in the EU (2015) (Nadzor s strani obveščevalnih služb: zaščitni ukrepi in pravna sredstva za temeljne pravice v EU (2015)), str. 18.

([70]) Zagotovila ODNI (Priloga VI), str. 4.

([71]) Glej tudi člen 5(d) PPD-28, ki določa, da mora direktor nacionalne obveščevalne službe v sodelovanju z vodji ustreznih organov obveščevalne skupnosti ter Uradom za politiko znanosti in tehnologije predsedniku predložiti „poročilo o oceni izvedljivosti oblikovanja programske opreme, ki bi obveščevalni skupnosti omogočala, da lažje pridobi ciljne podatke, namesto da bi jih množično zbirala.“ Glede na javne podatke je bilo na podlagi tega poročila ugotovljeno, da „ne obstaja alternativa, ki bi temeljila na programski opremi in zagotavljala popoln nadomestek za množično zbiranje podatkov pri odkrivanju nekaterih groženj nacionalni varnosti“. Glej jubilejno poročilo za leto 2015 Signal Intelligence Reform (Reforma zbiranja obveščevalnih podatkov SIGINT).

([72]) Glej opombo 68.

([73]) Zagotovila ODNI (Priloga VI). To se posebej nanaša na pomisleke, ki so jih izrazili nacionalni organi za varstvo podatkov v svojem mnenju glede osnutka sklepa o ustreznosti. Glej mnenje Delovne skupine za varstvo podatkov iz člena 29 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (Mnenje 01/2016 o osnutku sklepa o ustreznosti zasebnostnega ščita EU–ZDA) (sprejeto 13. aprila 2016), str. 38 v povezavi z opombo 47.

([74]) Glej člen 2 PPD-28.

uničevanje ali groženj kibernetski varnosti, pa tudi nadnacionalnih kriminalnih groženj, povezanih z drugimi petimi nameni, pregledovali pa se bodo vsaj enkrat letno. Glede na zagotovila vlade ZDA so organi obveščevalne skupnosti okrepili svoje analitične prakse in standarde za iskanje neocenjenih obveščevalnih podatkov SIGINT, da bi izpolnili te zahteve; uporaba ciljnih poizvedb „zagotavlja, da se analitikom v proučitev vedno predložijo samo tisti obveščevalni podatki, za katere se šteje, da bi bili lahko koristni za obveščevalne namene“ ([75]).

(75) Te omejitve so zlasti pomembne za osebne podatke, ki se prenašajo v okviru zasebnostnega ščita EU-ZDA, zlasti, če se do osebnih podatkov dostopa zunaj ZDA, tudi med njihovim prenašanjem po čezatlantskih kablih iz Unije v ZDA. Kot so potrdili organi ZDA v zagotovilih ODNI, se za tako zbiranje uporabljajo omejitve in zaščitni ukrepi, navedeni v zadevnih zagotovilih, vključno s tistimi iz PPD-28 ([76]).

(76) Čeprav ta načela niso navedena v zadevnih pravnih izrazih, zajemajo bistvo načel nujnosti in sorazmernosti. Ciljno zbiranje podatkov ima očitno prednost, medtem ko je množično zbiranje podatkov omejeno na (izredne) primere, ko ciljno zbiranje podatkov ni mogoče zaradi tehničnih ali operativnih razlogov. Tudi če se *množičnemu zbiranju podatkov* ni mogoče izogniti, je nadaljnja „uporaba“ takih podatkov z dostopom *strogo omejena* na posebne, legitimne namene nacionalne varnosti ([77]).

(77) Tako kot direktiva, ki jo izda predsednik kot glavni upravitelj, so te zahteve zavezujoče za celotno obveščevalno skupnost in se še naprej izvajajo prek pravil in postopkov agencije, ki prenašajo splošna načela v posebna navodila za vsakodnevne dejavnosti. Poleg tega je kongres, čeprav ga ne zavezuje PPD-28, sprejel tudi ukrepe za zagotovitev, da sta zbiranje in dostop do osebnih podatkov v ZDA ciljno usmerjena in se ne izvajata „na splošni podlagi“.

(78) Razpoložljive informacije, vključno z zagotovili vlade ZDA, kažejo, da lahko obveščevalne agencije v ZDA po prenosu podatkov do organizacij v ZDA, ki so samocertificirane v okviru zasebnostnega ščita EU-ZDA, zahtevajo osebne podatke le ([78]), če je njihova zahteva skladna z zakonom o nadzoru tujih obveščevalnih podatkov (Foreign Intelligence Surveillance Act, v nadaljnjem besedilu: FISA) ali jo vloži Zvezni preiskovalni urad (Federal Bureau of Investigation, v nadaljnjem besedilu: FBI) na podlagi tako imenovanega dopisa o nacionalni varnosti (National Security Letter, v nadaljnjem besedilu: NSL) ([79]). V skladu s FISA obstaja več pravnih podlag, ki se lahko uporabljajo za zbiranje (in poznejšo obdelavo) osebnih podatkov posameznikov iz EU, na katere se nanašajo

([75]) Zagotovila ODNI (Priloga VI), str. 4. Glej tudi direktivo o obveščevalni skupnosti št. 203.
([76]) Zagotovila ODNI (Priloga VI), str. 2. Prav tako se uporabljajo omejitve iz Odredbe št. 12333 (npr. potreba po tem, da zbrani podatki ustrezajo prednostnim nalogam obveščevalnih služb, ki jih določi predsednik).
([77]) Glej zadevo Schrems, točka 93.
([78]) Poleg tega lahko zbiranje podatkov s strani FBI temelji tudi na pooblastilih za kazenski pregon (glej člen 3.2 tega sklepa).
([79]) Za dodatna pojasnila glede uporabe NSL glej zagotovila ODNI (Priloga VI), str. 13–14 z opombo 38. Kot je navedeno v teh zagotovilih, lahko FBI uporablja NSL samo za zahtevanje nevsebinskih informacij, ki so pomembne za odobreno preiskavo nacionalne varnosti za zaščito pred mednarodnim terorizmom ali tajnimi obveščevalnimi dejavnostmi. Kar zadeva prenose podatkov v okviru zasebnostnega ščita EU–ZDA, se zdi, da je najpomembnejše zakonsko pooblastilo zakon o zasebnosti elektronskih komunikacij (Electronic Communications Privacy Act) (člen 2709 naslova 18 zakonodajne zbirke ZDA), ki zahteva, da se pri vsaki zahtevi za informacije o naročnikih ali evidenco transakcij uporabi „izraz, ki izrecno opredeljuje osebo, subjekt, telefonsko številko ali račun“.

osebni podatki, ki se prenašajo v okviru zasebnostnega ščita EU-ZDA. Poleg člena 104 FISA ([80]), ki ureja tradicionalni individualizirani elektronski nadzor, in člena 402 FISA ([81]) o namestitvi snemalnikov klicev (*pen registers*) ali sledilnih naprav (*trap and trace devices*) sta osrednja instrumenta člen 501 FISA (prejšnji člen 215 zakona o domovinski varnosti ZDA (U.S. PATRIOT ACT) in člen 702 FISA ([82]).

(79) V zvezi s tem zakon ZDA o svobodi (USA FREEDOM Act), ki je bil sprejet 2. junija 2015, prepoveduje množično zbiranje evidenc na podlagi člena 402 FISA (pooblastilo za snemanje klicev sledenje) in člena 501 FISA (prejšnji člen 215 zakona o domovinski varnosti ZDA) ([83]) ter z uporabo NSL in namesto tega zahteva uporabo posebnih „izbirnih izrazov“ ([84]).

(80) Čeprav FISA vsebuje dodatna pravna pooblastila za izvajanje nacionalnih obveščevalnih dejavnosti, vključno z obveščevalno dejavnostjo SIGINT, je ocena Komisije pokazala, da kar zadeva osebne podatke, ki se prenašajo v okviru zasebnostnega ščita EU-ZDA, ta pooblastila enako omejujejo javne posege javnih organov v ciljno zbiranje podatkov in dostop do podatkov.

(81) To je jasno pri tradicionalnem individualiziranem elektronskem nadzoru na podlagi člena 104 FISA ([85]). Kot je navedeno v členu 702 FISA, ki določa podlago za dva pomembna obveščevalna programa, ki ju izvajajo obveščevalne agencije ZDA (PRISM in UPSTREAM), se preiskave izvajajo ciljno z uporabo posameznih izbirnikov, ki opredeljujejo posebna komunikacijska sredstva, kot je e-poštni naslov ali telefonska številka ciljne osebe, ne pa ključnih besed ali imen ciljnih oseb ([86]). Zato, kot je navedel Nadzorni odbor za zasebnost in državljanske

([80]) Člen 1804 naslova 50 zakonodajne zbirke ZDA. Čeprav to pravno pooblastilo zahteva „izjavo o dejstvih in okoliščinah, na katere se opira prosilec, da bi utemeljil svoje prepričanje, da (A) je cilj elektronskega nadzora tuja sila ali agent tuje sile“, lahko slednji vključuje osebe, ki niso državljani ZDA in ki sodelujejo v mednarodnem terorizmu ali mednarodnem širjenju orožja za množično uničevanje (vključno s pripravljalnimi dejanji) (člen 1801 (b)(1) naslova 50 zakonodajne zbirke ZDA). Vendar kljub temu obstaja zgolj teoretična povezava do osebnih podatkov, ki se prenašajo v okviru zasebnostnega ščita EU–ZDA, glede na to, da mora biti v izjavi o dejstvih utemeljeno tudi prepričanje, da „vsakega od objektov ali prostorov, v katerih se upravlja elektronski nadzor, uporablja ali ga bo uporabljala tuja sila ali agent tuje sile“. V vsakem primeru uporaba tega pooblastila zahteva predložitev zahtevka FISC, ki med drugim oceni, ali na podlagi predstavljenih dejstev obstaja verjeten razlog, da to dejansko drži.

([81]) Člen 1842 v povezavi s členom 1841(2) naslova 50 zakonodajne zbirke ZDA in člen 3127 naslova 18 zakonodajne zbirke ZDA. To pooblastilo se ne nanaša na vsebino komunikacij, ampak na podatke o stranki ali naročniku, ki uporablja storitev (kot so ime, naslov, številka naročnika, trajanje/vrsta opravljene storitve, vir/mehanizem plačila). Zahteva uporabo odločbe FISC (ali sodnika nižjega sodišča) in posebnega izbirnega izraza v smislu člena 1841(4), tj. izraza, ki izrecno opredeljuje osebo, račun itd. in se v čim večji razumni meri uporablja za omejitev obsega iskanih informacij.

([82]) Medtem ko člen 501 FISA (prejšnji člen 215 zakona o domovinski varnosti ZDA) pooblašča FBI, da zahteva sodni nalog za predložitev „oprijemljivih predmetov“ (zlasti telefonskih metapodatkov, vendar tudi poslovnih evidenc) za namene tujih obveščevalnih služb, člen 702 FISA omogoča organom obveščevalne skupnosti ZDA, da zahtevajo dostop do podatkov, vključno z vsebino internetnih komunikacij, ki izvirajo iz ZDA, vendar so namenjeni določenim nedržavljanom ZDA zunaj ZDA.

([83]) Na podlagi tega sklepa lahko FBI zahteva „oprijemljive predmete“ (npr. evidence, spise, dokumente) na podlagi dokazil, predloženih Sodišču za nadzor nad tujo obveščevalno dejavnostjo (Foreign Intelligence Surveillance Court, v nadaljnjem besedilu: FISC), da se upravičeno domneva, da so pomembne za določeno preiskavo FBI. FBI mora pri preiskavi uporabiti izbirne izraze, ki jih odobri FISC in za katere obstaja „razumen in utemeljen sum“, da so povezani z eno ali več tujimi silami ali njihovim agenti, ki sodelujejo v mednarodnem terorizmu ali dejavnostih priprave terorističnih dejavnosti. Glej Poročilo Nadzornega odbora za zasebnost in državljanske svoboščine o členu 215, str. 59; Poročilo NSA CLPO o preglednosti: The USA Freedom Act Business Records FISA Implementation (Poročilo o preglednosti: izvajanje FISA v zvezi s poslovnimi evidencami na podlagi zakona ZDA o svobodi), 15. januar 2016, str. 4–6.

([84]) Zagotovila ODNI (Priloga VI), str. 13 (opomba 38).

([85]) Glej opombo 81.

([86]) Poročilo PCLOB o členu 702, str. 32 in 33 z nadaljnjimi sklici. Po navedbah svojega urada za varstvo zasebnosti mora NSA preveriti, ali obstaja povezava med ciljem in izbirnikom, dokumentirati tuje obveščevalne podatke, ki naj bi bili pridobljeni, te podatke morata pregledati in odobriti dva višja analitika NSA, celoten postopek pa se spremlja za naknadne preglede skladnosti, ki jih izvedeta ODNI in Ministrstvo za pravosodje. Glej poročilo NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act (Izvajanje člena 702 zakona o nadzoru tujih obveščevalnih podatkov s strani NSA), 16. april 2014.

svoboščine (Privacy and Civil Liberties Oversight Board, v nadaljnjem besedilu: PCLOB), nadzor iz člena 702 „zajema izključno ciljno usmerjanje na določene osebe (ki niso državljani ZDA), za katere so bile oblikovane individualizirane ugotovitve“ ([87]). Zaradi klavzule o časovni omejitvi veljavnosti bo treba člen 702 FISA pregledati leta 2017, ko bo morala Komisija znova oceniti zaščitne ukrepe, ki so na voljo posameznikom iz EU, na katere se nanašajo osebni podatki.

(82) Poleg tega je vlada ZDA v svojih zagotovilih navedla, da je Evropska komisija izrecno zagotovila, da obveščevalna skupnost ZDA „ne sodeluje pri neselektivnem nadzoru vseh, vključno z običajnimi evropskimi državljani“ ([88]). Kar zadeva osebne podatke, ki se zbirajo v ZDA, je ta izjava podprta z empiričnimi dokazi, ki kažejo, da se *zahteve za dostop* z NSL in na podlagi FISA, posamično ali skupaj, nanašajo le na razmeroma majhno število ciljnih subjektov v primerjavi s skupnim pretokom podatkov na internetu ([89]).

(83) Kar zadeva *dostop* do zbranih podatkov in *varstvo podatkov*, PPD-28 zahteva, da se dostop „omeji na pooblaščeno osebje, ki mora biti seznanjeno z informacijami za opravljanje svojih nalog“, ter da se osebni podatki „obdelujejo in hranijo pod pogoji, ki zagotavljajo ustrezno varstvo in preprečujejo dostop nepooblaščenim osebam, v skladu z veljavnimi zaščitnimi ukrepi za občutljive podatke“. Obveščevalno osebje je deležno ustreznega in zadostnega usposabljanja v zvezi z načeli iz PPD-28 ([90]).

(84) Kar zadeva *hrambo* in nadaljnje *razširjanje* osebnih podatkov posameznikov iz EU, na katere se nanašajo osebni podatki, ki jih zbirajo obveščevalni organi ZDA, je v PPD-28 navedeno, da bi se morale vse osebe (vključno z nedržavljani ZDA) obravnavati z dostojanstvom in spoštovanjem, da imajo vse osebe legitimni interes za varstvo zasebnosti pri obdelavi njihovih osebnih podatkov in da morajo organi obveščevalne skupnosti zato vzpostaviti politike, ki zagotavljajo ustrezne zaščitne ukrepe za take podatke, „ki so razumno zasnovani za zmanjšanje [njihovega] razširjanja in hrambe“ ([91]).

([87]) Poročilo PCLOB o členu 702, str. 111. Glej tudi zagotovila ODNI (Priloga VI), str. 9 („Zbiranje podatkov v skladu s členom 702 [FISA] ni ‘množično in neselektivno’, ampak ozko osredotočeno na zbiranje tujih obveščevalnih podatkov od individualno opredeljenih legitimnih ciljnih subjektov“) in str. 13, opomba 36 (s sklicem na mnenje FISC iz leta 2014); NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act (Izvajanje člena 702 zakona o nadzoru tujih obveščevalnih podatkov s strani NSA), 16. april 2014. Tudi v primeru programa UPSTREAM lahko NSA zahteva samo prestrezanje elektronskih komunikacij do določenih izbirnikov od njih ali o njih.

([88]) Zagotovila ODNI (Priloga VI), str. 18. Glej tudi stran 6, kjer je navedeno, da veljavni postopki „kažejo jasno zavezo za preprečevanje samovoljnega in neselektivnega zbiranja obveščevalnih podatkov SIGINT ter izvajanje načela razumnosti vse do najvišjih ravni naše vlade“.

([89]) Glej Statistical Transparency Report Regarding Use of National Security Authorities (Statistično poročilo o preglednosti v zvezi z uporabo pooblastil na področju nacionalne varnosti), 22. april 2015. Za skupni pretok podatkov na internetu glej na primer poročilo Agencije za temeljne pravice (Fundamental Rights Agency) Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015) (Nadzor s strani obveščevalnih služb: zaščitni ukrepi in pravna sredstva za temeljne pravice v EU (2015)), str. 15 in16. Kar zadeva program UPSTREAM, je glede na mnenje FISC s preklicano zaupnostjo iz leta 2011 več kot 90 % elektronskih komunikacij, pridobljenih v skladu s členom 702 FISA, izhajalo iz programa PRISM in manj kot 10 % iz programa UPSTREAM. Glej predhodno mnenje FISC št. 2011 WL 10945618 (FISA Ct., 3.10.2011), opomba 21 (na voljo na: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Glej člen 4(a)(ii) PPD-28. Glej tudi poročilo ODNI Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (Varstvo osebnih informacij vseh: Poročilo o stanju na področju razvoja in izvajanja postopkov na podlagi Predsedniške politične direktive št. 28) iz julija 2014, str. 5, v skladu s katerim „bi morali organi obveščevalne skupnosti okrepiti obstoječe analitične prakse in standarde, pri čemer si morajo analitiki prizadevati za strukturiranje poizvedb ali drugih izbirnih izrazov in tehnik za opredelitev obveščevalnih podatkov, ki so pomembni za upravičeno obveščevalno nalogo ali nalogo kazenskega pregona, osredotočenje poizvedb o osebah na kategorije obveščevalnih podatkov, ki ustrezajo zahtevi v zvezi z obveščevalnimi podatki ali kazenskim pregonom, in zmanjšanje pregledovanja osebnih podatkov, ki niso pomembni za zahteve v zvezi z obveščevalnimi podatki ali kazenskim pregonom“. Glej na primer CIA, Signals Intelligence Activities (Obveščevalne dejavnosti SIGINT), str. 5; FBI, Presidential Policy Directive 28 Policies and Procedures (Politike in postopki na podlagi Predsedniške politične direktive št. 28), str. 3. Glede na poročilo o napredku reforme zbiranja obveščevalnih podatkov SIGINT iz leta 2016 so organi obveščevalne skupnosti (vključno z FBI, CIA in NSA) sprejeli ukrepe za seznanjanje svojega osebja z zahtevami PPD-28 z oblikovanjem novih ali spreminjanjem obstoječih politik usposabljanja.

([91]) Glede na zagotovila ODNI se te omejitve uporabljajo ne glede na to, ali so se informacije zbirale množično ali ciljno, in ne glede na državljanstvo posameznika.

(85) Vlada ZDA je pojasnila, da ta zahteva po razumnosti pomeni, da organom obveščevalne skupnosti ne bo treba sprejeti „kakršnih koli teoretično mogočih ukrepov“, ampak bodo morale „uravnotežiti svoja prizadevanja za zaščito legitimnih interesov glede zasebnosti in državljanskih svoboščin s praktičnimi potrebami obveščevalnih dejavnosti SIGINT“ ([92]). V zvezi s tem bodo nedržavljani ZDA obravnavani enako kot državljani ZDA, na podlagi postopkov, ki jih odobri generalni državni tožilec ([93]).

(86) V skladu s temi pravili je hramba običajno omejena na največ pet let, razen če zakonodaja vsebuje posebno določbo ali če direktor nacionalne obveščevalne službe po natančni oceni vprašanj v zvezi z zasebnostjo, pri čemer upošteva mnenja uradnika za varstvo državljanskih svoboščin ODNI, pa tudi uradnih oseb agencije za varstvo zasebnosti in državljanske pravice agencije, določi, da je stalna hramba v interesu nacionalne varnosti ([94]). Razširjanje je omejeno na primere, ko so podatki pomembni za osnovni namen zbiranja podatkov in tako ustrezajo zahtevi pooblaščenih tujih obveščevalnih organov ali organov kazenskega pregona ([95]).

(87) Glede na zagotovila vlade ZDA se osebni podatki ne smejo razširjati zgolj zato, ker zadevni posameznik ni državljan ZDA in se „obveščevalni podatki SIGINT o običajnih dejavnostih tuje osebe ne bi šteli za tuje obveščevalne podatke, ki bi se lahko stalno razširjali ali hranili zgolj zaradi tega dejstva, razen če sicer ustrezajo zahtevi pooblaščenih tujih obveščevalnih organov“ ([96]).

(88) Na podlagi zgoraj navedenega je Komisija zato sklenila, da so v ZDA vzpostavljena pravila, namenjena omejitvi morebitnih posegov za namene nacionalne varnosti v temeljne pravice oseb, katerih osebni podatki se prenašajo iz Unije v ZDA v okviru zasebnostnega ščita EU-ZDA, na tisto, kar je nujno potrebno za doseganje zadevnega legitimnega cilja.

(89) Kot je prikazano v zgornji analizi, pravo ZDA zagotavlja, da se bodo nadzorni ukrepi uporabili le za pridobivanje tujih obveščevalnih podatkov, kar je legitimni cilj politike ([97]), in da bodo čim bolj prilagojeni. Zlasti množično

([92]) Glej zagotovila ODNI (Priloga VI).

([93]) Glej člen 4(a)(i) PPD-28 v povezavi s členom 2.3 Odredbe 12333.

([94]) Člen 4(a)(i) PPD-28; Zagotovila ODNI (Priloga VI), str. 7. Na primer, za osebne podatke, ki se zbirajo na podlagi člena 702 FISA, postopki NSA za zmanjševanje količine podatkov, ki jih odobri FISC, praviloma določajo, da se metapodatki in neovrednotena vsebina za program PRISM hranijo največ pet let, podatki za program UPSTREAM pa največ dve leti. NSA upošteva omejitve hrambe z uporabo avtomatiziranega postopka, ki na koncu ustreznega obdobja hrambe izbriše zbrane podatke. Glej postopke NSA za zmanjševanje količine podatkov po členu 702 FISA, člen 7 v povezavi s členom 6(a)(1); poročilo NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act (Izvajanje člena 702 zakona o nadzoru tujih obveščevalnih podatkov s strani NSA), z dne 16. 4. 2014. Enako je tudi hramba iz člena 501 FISA (prejšnji člen 215 zakona o domovinski varnosti ZDA) omejena na pet let, razen če so osebni podatki del ustrezno odobrenega razširjanja tujih obveščevalnih podatkov ali če Ministrstvo za pravosodje pisno obvesti NSA, da za evidence velja obveznost hrambe podatkov v nerešenih ali pričakovanih sodnih sporih. Glej NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation (Poročilo o preglednosti: izvajanje FISA v zvezi s poslovnimi evidencami na podlagi zakona ZDA o svobodi), 15. januar 2016.

([95]) Natančneje, v primeru člena 501 (prejšnji člen 215 zakona o domovinski varnosti ZDA) se razširjanje osebnih podatkov lahko izvaja samo za namene boja proti terorizmu ali kot dokaz kaznivega dejanja, v primeru iz člena 702 FISA pa samo za utemeljen namen zbiranja tujih obveščevalnih podatkov ali kazenskega pregona. Glej NSA, CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 (Izvajanje člena 702 zakona o nadzoru tujih obveščevalnih podatkov s strani NSA), 16. april 2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation (Poročilo o preglednosti: izvajanje FISA v zvezi s poslovnimi evidencami na podlagi zakona ZDA o svobodi), 15. januar 2016. Glej tudi NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 (Varstvo državljanskih svoboščin in zasebnosti s strani NSA za ciljne obveščevalne dejavnosti SIGINT na podlagi Odredbe št. 12333), 7. oktober 2014.

([96]) Zagotovila ODNI (Priloga VI), str. 7 (s sklicem na direktivo o obveščevalni skupnosti št. 203 (Intelligence Community Directive – ICD) 203).

([97]) Sodišče je pojasnilo, da je nacionalna varnost legitimni cilj politike. Glej zadevo Schrems, točka 88. Glej tudi zadevo Digital Rights Ireland in drugi, točke 42 do 44 in 51, v katerih je Sodišče menilo, da je boj proti hudim kaznivim dejanjem, zlasti organiziranemu kriminalu in terorizmu, lahko v veliki meri odvisen od uporabe sodobnih preiskovalnih tehnik. V nasprotju s kazenskimi preiskavami, ki se običajno nanašajo na retrospektivno ugotavljanje odgovornosti in krivde za ravnanje v preteklosti, se obveščevalne dejavnosti pogosto osredotočajo na preprečevanje groženj nacionalni varnosti, preden je povzročena škoda. Zato lahko take preiskave pogosto zajemajo več potencialnih akterjev (ciljev) in širše geografsko območje. Glej ESČP, Weber in Saravia proti Nemčiji, odločba z dne 29. junija 2006, tožba št. 54934/00, točke 105 do 118 (o t. i. strateškem spremljanju).

zbiranje podatkov bo izjemoma dovoljeno le, če ciljno zbiranje podatkov ne bo mogoče, spremljali pa ga bodo dodatni zaščitni ukrepi, da se bosta zmanjšala količina zbranih podatkov in nadaljnji dostop (ki bo moral biti ciljno usmerjen in dovoljen le za posebne namene).

(90) Po oceni Komisije je to skladno s standardom Sodišča iz sodbe v zadevi Schrems, v skladu s katerim mora predpis, ki pomeni poseg v temeljne pravice, zagotovljene v členih 7 in 8 Listine, določati „minimalne zahteve“ ([98]) in „ni zgolj na nujno potrebno omejena ureditev, ki splošno dovoljuje hrambo vseh osebnih podatkov vseh posameznikov, katerih podatki so bili preneseni iz Unije v Združene države, ne da bi se uporabljalo kakršno koli razlikovanje, omejitev ali izjema glede na cilj, ki se ga poskuša doseči, in ne da bi bilo predvideno objektivno merilo, ki bi omogočalo dostop javnih organov do podatkov in poznejšo uporabo teh podatkov samo v namene, ki so natančno določeni, strogo omejeni in bi lahko utemeljevali poseg, ki ga pomenita dostop in uporaba teh podatkov“ ([99]). Prav tako ne bo neomejenega zbiranja in hrambe podatkov vseh oseb brez kakršnih koli omejitev ali neomejenega dostopa. Poleg tega zagotovila, predložena Komisiji, vključno z zagotovilom, da se ameriške obveščevalne dejavnosti SIGNIT nanašajo le na del komunikacij na internetu, izključujejo „splošni“ dostop do vsebine elektronskih komunikacij ([100]).

3.1.2 Učinkovito pravno varstvo

(91) Komisija je ocenila nadzorne mehanizme, ki obstajajo v ZDA, glede morebitnih posegov obveščevalnih organov ZDA v osebne podatke, ki se prenašajo v ZDA, in možnosti individualne pritožbe, ki so na voljo posameznikov iz EU, na katere se nanašajo osebni podatki.

Nadzor

(92) Za ameriško obveščevalno skupnost se uporabljajo različni mehanizmi pregleda in nadzorni mehanizmi, za katere so pristojne tri veje države. Ti vključujejo notranje in zunanje organe izvršilne veje oblasti, številne kongresne odbore ter sodni nadzor, zlasti dejavnosti zakona o nadzoru tujih obveščevalnih podatkov.

(93) Obveščevalne dejavnosti organov ZDA obsežno nadzoruje izvršilna veja oblasti.

(94) V skladu s členom 4(a)(iv) PPD-28 politike in postopki organov obveščevalne skupnosti „vključujejo ustrezne ukrepe za olajšanje nadzora nad izvajanjem zaščitnih ukrepov za varstvo osebnih podatkov“, ti ukrepi pa bi morali vključevati redno izvajanje revizij ([101]).

([98]) Zadeva Schrems, točka 91 z nadaljnjimi sklici.
([99]) Zadeva Schrems, točka 93.
([100]) Glej zadevo Schrems, točka 94.
([101]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (Varstvo osebnih informacij vseh: Poročilo o stanju na področju razvoja in izvajanja postopkov na podlagi Predsedniške politične direktive št. 28), str. 7. Glej npr. CIA, Signals Intelligence Activities (Obveščevalne dejavnosti SIGINT), str. 6 (skladnost); FBI, Politike in postopki na podlagi Predsedniške politične direktive št. 28, člena III (A)(4) in III (B)(4) ter NSA, postopki na podlagi člena 4 PPD-28 z dne 12. januarja 2015, člena 8.1 in 8.6(c).

(95) V zvezi s tem je bilo vzpostavljenih več ravni nadzora, vključno na ravni uradnikov za državljanske pravice in varstvo zasebnosti, generalnega inšpektorja, Urada ODNI za državljanske svoboščine in varstvo zasebnosti, PCLOB in predsedniškega obveščevalnega nadzornega odbora (President's Intelligence Oversight Board). Te nadzorne funkcije pomaga izvajati osebje za skladnost v vseh agencijah ([102]).

(96) Kot je pojasnila vlada ZDA ([103]), obstajajo na različnih ministrstvih, pristojnih za obveščevalne dejavnosti, in v obveščevalnih agencijah *uradniki za državljanske pravice ali varstvo zasebnosti*, ki so pristojni za nadzor ([104]). Čeprav se posebne pristojnosti teh uradnikov lahko nekoliko razlikujejo glede na zakonsko podlago, s katero so jim pooblastila podeljena, običajno zajemajo nadzor nad postopki za zagotovitev, da zadevno ministrstvo/agencija ustrezno upošteva pomisleke, povezane z zasebnostjo ali državljanskimi pravicami, in da ima vzpostavljene ustrezne postopke za obravnavo pritožb posameznikov, ki menijo, da je kršena njihova zasebnost ali državljanske svoboščine (in v nekaterih primerih, kot je ODNI, so lahko sami pooblaščeni za obravnavanje pritožb ([105])). Vodja ministrstva/agencije mora zagotoviti, da uradniki prejmejo vse podatke, in zagotovi se mu dostop do vsega gradiva, potrebnega za opravljanje njegovih nalog. Uradniki za državljanske pravice in varstvo zasebnosti redno poročajo kongresu in PCLOB, vključno s poročanjem o številu in naravi pritožb, ki jih prejme ministrstvo/agencija, povzetkom obravnave takih pritožb, opravljenimi pregledi in preiskavami ter vplivom dejavnosti, ki jih je izvedel uradnik ([106]). Glede na oceno nacionalnih organov za varstvo podatkov se lahko notranji nadzor, ki ga izvajajo uradniki za državljanske pravice ali varstvo zasebnosti, obravnava kot „razmeroma zanesljiv", čeprav po njihovem mnenju ne dosega zahtevane stopnje neodvisnosti ([107]).

(97) Poleg tega ima vsak organ obveščevalne skupnosti svojega *generalnega inšpektorja*, ki je med drugim pristojen za nadzor nad tujimi obveščevalnimi dejavnostmi ([108]). To v okviru ODNI vključuje Urad generalnega inšpektorja (Office of the Inspector General) s celovito pristojnostjo nad celotno obveščevalno skupnostjo in pooblastili za proučitev pritožb ali informacij v zvezi z obtožbami o protipravnem ravnanju ali zlorabi položaja v povezavi s programi ali dejavnostmi ODNI in/ali obveščevalne skupnosti ([109]). Generalni inšpektorji so zakonsko neodvisne ([110]) enote, pristojne za izvajanje revizij in preiskav v zvezi s programi in postopki, ki jih izvaja ustrezna agencija za nacionalne obveščevalne namene, vključno s primeri zlorab ali kršitev zakona ([111]). Pooblaščeni so za dostop do vseh evidenc, poročil, revizij, pregledov, dokumentov, spisov, priporočil ali drugega

([102]) NSA na primer v Direktoratu za skladnost (Directorate for Compliance) zaposluje več kot 300 oseb, ki skrbijo za skladnost. Glej zagotovila ODNI (Priloga VI), str. 7.

([103]) Glej mehanizem varuha človekovih pravic (Priloga III), člen 6(b) (i) do (iii).

([104]) Glej člen 2000ee-1 naslova 42 zakonodajne zbirke ZDA. To vključuje na primer Ministrstvo za zunanje zadeve, Ministrstvo za pravosodje (vključno z FBI), Ministrstvo za domovinsko varnost, Ministrstvo za obrambo, NSA, CIA in ODNI.

([105]) Po navedbah vlade ZDA se bo Urad za državljanske svoboščine in zasebnost ODNI, če bo prejel pritožbo, usklajeval tudi z drugimi organi obveščevalne skupnosti glede nadaljnje obravnave zadevne pritožbe v okviru obveščevalne skupnosti. Glej mehanizem varuha človekovih pravic (Priloga III), člen 6(b)(ii).

([106]) Glej člen 2000ee-1 (f)(1) in (2) naslova 42 zakonodajne zbirke ZDA.

([107]) Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (Mnenje 01/2016 o sklepu o ustreznosti osnutka zasebnostnega ščita EU-ZDA), Delovna skupina za varstvo podatkov iz člena 29 (sprejeto 13. aprila 2016), str. 41.

([108]) Zagotovila ODNI (Priloga VI), str. 7. Glej na primer NSA, postopki na podlagi člena 4 PPD-28, z dne 12. januarja 2015, člen 8.1 ter CIA, Signals Intelligence Activities (Obveščevalne dejavnosti SIGINT), str. 7 (odgovornosti).

([109]) Tega generalnega inšpektorja (ki je bil vzpostavljen oktobra 2010) imenuje predsednik s potrditvijo senata ter ga lahko odstavi samo predsednik in ne direktor nacionalne obveščevalne službe.

([110]) Ti generalni inšpektorji imajo zagotovljen mandat in jih lahko odstavi samo predsednik, ki mora pisno sporočiti kongresu razloge za tako odstavitev. To ne pomeni nujno, da jim ni treba upoštevati nobenih navodil. V nekaterih primerih lahko vodja ministrstva prepove generalnemu inšpektorju, da začne, izvede ali dokonča revizijo ali preiskavo, če se to šteje za nujno za ohranitev pomembnih nacionalnih (varnostnih) interesov. Vendar mora biti kongres obveščen o izvajanju te pristojnosti in na tej podlagi naloži odgovornost ustreznemu direktorju. Glej zakon o generalnih inšpektorjih iz leta 1978, člen 8 (generalni inšpektor Ministrstva za obrambo); člen 8E (generalni inšpektor Ministrstva za pravosodje), člen 8G (d)(2)(A) in (B) (generalni inšpektor NSA); člen 403q (b) naslova 50 zakonodajne zbirke ZDA (generalni inšpektor CIA); zakon o pooblastilih za obveščevalno dejavnost za davčno leto 2010 (Intelligence Authorization Act For Fiscal Year 2010), člen 405(f) (generalni inšpektor obveščevalne skupnosti). Glede na oceno nacionalnih organov za varstvo podatkov generalni inšpektorji „večinoma izpolnjujejo merilo glede organizacijske neodvisnosti, kot ga opredeljujeta Sodišče Evropske unije in Evropsko sodišče za človekove pravice (ESČP), vsaj od trenutka, ko se za vse uporablja nov postopek imenovanja". Glej Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (Mnenje 01/2016 o sklepu o ustreznosti osnutka zasebnostnega ščita EU–ZDA), Delovna skupina za varstvo podatkov iz člena 29 (sprejeto 13. aprila 2016), str. 40.

([111]) Glej zagotovila ODNI (Priloga VI), str. 7. Glej tudi zakon o generalnih inšpektorjih iz leta 1978 s spremembami, Zbirka aktov Kongresa s področja javnega prava, št. 113–126 z dne 7. julija 2014.

ustreznega gradiva, po potrebi s sodnim pozivom, in lahko opravljajo zaslišanja ([112]). Čeprav lahko generalni inšpektorji izdajajo samo nezavezujoča priporočila za popravne ukrepe, se njihova poročila, vključno s poročili o nadaljnjih ukrepih (ali odsotnosti ukrepov), objavijo in pošljejo Kongresu, ki lahko na podlagi teh poročil opravlja svojo nadzorno funkcijo ([113]).

(98) Poleg tega so *Nadzornemu odboru za zasebnost in državljanske svoboščine*, neodvisni agenciji ([114]) izvršilne oblasti, sestavljeni iz dvostrankarskega petčlanskega odbora ([115]), ki ga imenuje predsednik z odobritvijo senata za šestletno obdobje, podeljena pooblastila na področju politik boja proti terorizmu in njihovem izvajanju z namenom varstva zasebnosti in državljanskih svoboščin. Pri pregledu ukrepov obveščevalne skupnosti lahko dostopa do vseh ustreznih evidenc, poročil, revizij, pregledov, dokumentov, spisov in priporočil agencije, vključno z zaupnimi informacijami, opravlja pogovore in prisostvuje zaslišanjem. Prejema poročila uradnikov za državljanske pravice in varstvo zasebnosti več zveznih ministrstev/agencij ([116]), jim lahko izdaja priporočila ter redno poroča kongresnim odborom in predsedniku ([117]). Odbor za nadzor zasebnosti in državljanskih svoboščin mora v okviru svojega mandata pripraviti tudi poročilo o oceni izvajanja PPD-28.

(99) Navedene nadzorne mehanizme dopolnjuje *obveščevalni nadzorni odbor (Intelligence Oversight Board)*, ustanovljen v okviru predsedniškega obveščevalnega svetovalnega odbora (President's Intelligence Advisory Board), ki nadzoruje skladnost obveščevalnih organov ZDA z ustavo in vsemi veljavnimi pravili.

(100) Za olajšanje nadzora se organe obveščevalne skupnosti spodbuja k oblikovanju informacijskih sistemov za omogočanje spremljanja, evidentiranja in pregledovanja poizvedb ali drugih iskanj osebnih podatkov ([118]). Organi za nadzor in skladnost redno preverjajo prakse organov obveščevalne skupnosti za varstvo osebnih podatkov, vsebovanih v obveščevalnih podatkih SIGINT, in njihovo skladnost s temi postopki ([119]).

(101) Te nadzorne funkcije so podprte tudi z obsežnimi zahtevami za poročanje glede neskladnosti. Postopki agencije morajo zlasti zagotavljati, da se v primeru velikih težav v zvezi s skladnostjo, ki vključuje osebne podatke katere koli osebe, ne glede na državljanstvo, zbrane s pomočjo obveščevalnih dejavnosti SIGINT, taka težava takoj sporoči vodji organa obveščevalne skupnosti, ki nato obvesti direktorja nacionalne obveščevalne službe, ki na podlagi PPD-28 določi, ali so potrebni kakršni koli popravni ukrepi ([120]). Poleg tega morajo vsi organi obveščevalne skupnosti na podlagi Odredbe št. 12333 poročati obveščevalnemu svetovalnemu odboru o primerih neskladnosti ([121]). Ti mehanizmi zagotavljajo, da se težava obravnava na najvišji ravni v obveščevalni

([112]) Glej zakon o generalnih inšpektorjih iz leta 1978, člen 6.

([113]) Glej zagotovila ODNI (Priloga VI), str. 7. Glej tudi zakon o generalnih inšpektorjih iz leta 1978, člena 4(5) in 5. V skladu s členom 405 (b)(3) in (4) zakona o pooblastilih za obveščevalno dejavnost za davčno leto 2010 (Zbirka aktov Kongresa s področja javnega prava, št. 111–259 z dne 7. oktobra 2010) bo generalni inšpektor obveščevalne skupnosti direktorja nacionalne obveščevalne službe in kongres obveščal o potrebi po popravnih ukrepih in njihovem napredku.

([114]) Glede na oceno nacionalnih organov za varstvo podatkov je Odbor za nadzor zasebnosti in državljanskih svoboščin v preteklosti dokazal, „da ima neodvisna pooblastila". Glej Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (Mnenje 01/2016 o sklepu o ustreznosti osnutka zasebnostnega ščita EU-ZDA), Delovna skupina za varstvo podatkov iz člena 29 (sprejeto 13. aprila 2016), str. 42.

([115]) Poleg tega Odbor za nadzor zasebnosti in državljanskih svoboščin zaposluje približno 20 oseb. Glej https://www.pclob.gov/about-us/staff.html.

([116]) Mednje sodijo Ministrstvo za pravosodje, Ministrstvo za obrambo, Ministrstvo za domovinsko varnost, direktor nacionalne in centralne obveščevalne agencije in vsa druga ministrstva, agencije ali organi izvršilne oblasti, ki jih imenuje Odbor za nadzor zasebnosti in državljanskih svoboščin in jih je primerno vključiti.

([117]) Glej člen 2000ee naslova 42 zakonodajne zbirke ZDA. Glej tudi mehanizem varuha človekovih pravic (Priloga III), člen 6(b) (iv). Med drugim mora Odbor za nadzor zasebnosti in državljanskih svoboščin sporočiti, ko agencija izvršilne veje oblasti ne upošteva njegovega nasveta.

([118]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (Varovanje osebnih podatkov vseh ljudi: poročilo o stanju na področju razvoja in izvajanja postopkov na podlagi Predsedniške politične direktive št. 28), str. 7–8.

([119]) Prav tam, str. 8. Glej tudi zagotovila ODNI (Priloga VI), str. 9.

([120]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (Varstvo osebnih informacij vseh: Poročilo o stanju na področju razvoja in izvajanja postopkov na podlagi Predsedniške politične direktive št. 28), str. 7. Glej na primer NSA, postopki na podlagi člena 4 PPD-28, z dne 12. januarja 2015, člena 7.3 ter 8.7(c) in (d); FBI, Politike in postopki na podlagi Predsedniške politične direktive št. 28, člena III (A)(4) in III (B)(4) ter CIA, Signals Intelligence Activities (Obveščevalne dejavnosti SIGINT), str. 6 (skladnost) in str. 8 (odgovornosti).

([121]) Glej člen 1.6(c) odredbe 12333.

skupnosti. Če je vpletena oseba, ki ni državljan ZDA, direktor nacionalne obveščevalne službe v posvetovanju z državnim sekretarjem in vodjo ministrstva ali agencije, ki pošlje sporočilo, določi, ali je treba sprejeti ukrepe za obveščanje ustrezne tuje vlade v skladu z zaščito virov in metod ter osebja ZDA ([122]).

(102) Poleg za te nadzorne mehanizme v okviru izvršilne oblasti je kongres ZDA, natančneje *stalni obveščevalni in pravosodni odbori ter obveščevalni in pravosodni odbori v okviru senata (House and Senate Intelligence and Judiciary Committees),* pristojen za nadzor nad vsemi tujimi obveščevalnimi dejavnostmi v ZDA, vključno z dejavnosti SIGINT v ZDA. V skladu z zakonom o nacionalni varnosti (National Security Act) „predsednik zagotovi, da se kongresni obveščevalni odbori v celoti in sproti obveščajo o obveščevalnih dejavnostih ZDA, vključno s katero koli pomembno predvideno obveščevalno dejavnostjo, kot se zahteva v skladu s tem podpoglavjem“ ([123]). Poleg tega „[p]redsednik zagotovi, da se kongresni obveščevalni odbori nemudoma obvestijo o kakršni koli nezakoniti obveščevalni dejavnosti, pa tudi o kakršnih koli popravnih ukrepih, ki so bili sprejeti ali so načrtovani v povezavi s tako nezakonito dejavnostjo“ ([124]). Člani teh odborov imajo dostop do zaupnih podatkov, pa tudi do obveščevalnih metod in programov ([125]).

(103) S poznejšimi zakoni so bile zahteve za poročanje razširjene in izpopolnjene, tako v zvezi z organi obveščevalne skupnosti kot tudi ustreznimi generalnimi inšpektorji in generalnim državnim tožilcem. Na primer, FISA zahteva, da generalni državni tožilec „v celoti obvešča“ obveščevalne in pravosodne odbore v okviru senata ter stalne obveščevalne in pravosodne odbore o dejavnostih vlade v skladu z nekaterimi členi FISA ([126]). Zahteva tudi, da vlada kongresnim odborom predloži kopije „vseh sklepov, odredb ali mnenj sodišča za nadzor tujih obveščevalnih podatkov ali prizivnega sodišča za nadzor tujih obveščevalnih podatkov, ki vključujejo pomembno sestavo ali razlago“ določb FISA. Zlasti kar zadeva nadzor v skladu s členom 702 FISA, se ta izvaja z zakonsko določenimi poročili za obveščevalne in pravosodne odbore, pa tudi s pogostim obveščanjem in zaslišanji. To vključuje polletno poročilo generalnega državnega tožilca, v katerem je opisana uporaba člena 702 FISA, s spremnimi dokumenti, vključno zlasti s poročili o skladnosti Ministrstva za pravosodje in ODNI, opisom morebitnih primerov neskladnosti ([127]) ter ločeno polletno oceno generalnega državnega tožilca in direktorja nacionalne obveščevalne službe, ki beleži skladnost s postopki izbire cilja in zmanjševanja količine podatkov, vključno s skladnostjo s postopki za zagotavljanje, da se zbiranje izvaja za upravičen namen zbiranja tujih obveščevalnih podatkov ([128]). Kongres prejema tudi poročila generalnih inšpektorjev, ki so pooblaščeni za ocenjevanje, ali agencije upoštevajo postopke za izbiro cilja in zmanjševanje količine podatkov ter smernice generalnega državnega tožilca.

(104) V skladu z zakonom ZDA o svobodi iz leta 2015 mora vlada ZDA med drugim Kongresu (in javnosti) vsako leto razkriti število zahtevanih in prejetih odredb in direktiv FISA, pa tudi oceno števila državljanov in nedržavljanov ZDA, nad katerimi se izvaja nadzor ([129]). Zakon zahteva tudi dodatno javno poročanje o številu izdanih NSL tako

([122]) PPD-28, člen 4(a)(iv).
([123]) Glej člen 501(a)(1) (člen 413(a)(1) naslova 50 zakonodajne zbirke ZDA). Ta določba vsebuje splošne zahteve v zvezi s kongresnim nadzorom na področju nacionalne varnosti.
([124]) Glej člen 501(b) (člen 413(b) naslova 50 zakonodajne zbirke ZDA).
([125]) Glej člen 501(d) (člen 413(d) naslova 50 zakonodajne zbirke ZDA).
([126]) Glej člene 1808, 1846, 1862, 1871 in 1881f naslova 50 zakonodajne zbirke ZDA.
([127]) Glej člen 1881f naslova 50 zakonodajne zbirke ZDA.
([128]) Glej člen 1881a(l)(1) naslova 50 zakonodajne zbirke ZDA.
([129]) Glej zakon ZDA o svobodi iz leta 2015, Zbirka aktov Kongresa s področja javnega prava, št. 114–23, člen 602(a). Poleg tega v skladu s členom 402 „direktor nacionalne obveščevalne službe v posvetovanju z generalnim državnim tožilcem izvede pregled v zvezi z odpravo zaupnosti vsakega sklepa, odredbe ali mnenja, ki ga izda sodišče za nadzor tujih obveščevalnih podatkov ali drugostopenjsko sodišče za nadzor tujih obveščevalnih podatkov (kot je opredeljeno v členu 601(e)) in ki vključuje pomembno sestavo ali razlago katere koli zakonske določbe, vključno s kakršno koli novo ali pomembno sestavo ali razlago izraza ‘posebni izbirni izraz’, ter skladno s tem pregledom v največji možni meri zagotovi javno dostopnost vsakega takega sklepa, odredbe ali mnenja“.

v zvezi z državljani kot tudi nedržavljani ZDA (ter hkrati omogoča prejemnikom odredb in potrdil FISA, pa tudi zahtevkov na podlagi NSL, da pod določenimi pogoji izdajo poročila o preglednosti) ([130]).

(105) Tretjič, obveščevalne dejavnosti javnih organov ZDA, ki temeljijo na FISA, omogočajo pregled in v nekaterih primerih predhodno odobritev ukrepov s strani *sodišča FISA* (v nadaljnjem besedilu: FISC) ([131]), neodvisnega sodišča ([132]), katerega odločbe se lahko izpodbijajo na drugostopenjskem sodišču za nadzor tujih obveščevalnih podatkov (Foreign Intelligence Court of Review, v nadaljnjem besedilu: FISCR) ([133]) in na koncu vrhovnem sodišču ZDA ([134]). V primeru predhodne odobritve morajo organi, ki zaprosijo za ukrepe (FBI, NSA CIA itd.), osnutek zahtevka predložiti pravnikom na Oddelku za nacionalno varnosti Ministrstva za pravosodje, ki ga pregledajo in po potrebi zahtevajo dodatne informacije ([135]). Ko je zahtevek dokončan, ga mora odobriti generalni državni tožilec, namestnik generalnega državnega tožilca ali pomočnik generalnega državnega tožilca za nacionalno varnost ([136]). Ministrstvo za pravosodje nato predloži zahtevek FISC, ki ga oceni in sprejme predhodno odločitev o nadaljnjih ukrepih ([137]). Kadar poteka obravnava, lahko FISC opravi zaslišanje, kar lahko vključuje strokovno svetovanje ([138]).

(106) Sodišču FISC (in FISCR) pomaga stalni senat petih posameznikov, ki imajo strokovno znanje in izkušnje na področju nacionalne varnosti in državljanskih svoboščin ([139]). Iz te skupine sodišče imenuje posameznika, ki deluje kot *amicus curiae*, za pomoč pri obravnavi kakršnega koli zahtevka za odredbo ali pregled, ki po mnenju sodišča predstavlja novo ali pomembno razlago zakona, razen če sodišče ugotovi, da tako imenovanje ni primerno ([140]). To bi moralo zlasti zagotoviti, da so pomisleki glede zasebnosti ustrezno izraženi v oceni sodišča. Sodišče lahko posameznika ali organizacijo imenuje za opravljanje naloge *amicus curiae*, vključno z zagotavljanjem tehničnega strokovnega znanja, kadar se mu to zdi primerno, ali na predlog dovoli posamezniku ali organizaciji, da predloži stališče *amicus curiae* ([141]).

([130]) Ameriški zakon o svobodi (USA FREEDOM Act), člena 602(a) in 603(a).

([131]) Za nekatere vrste nadzora ima lahko sodnik nižjega sodišča ZDA, ki ga javno imenuje vrhovni sodnik ZDA, pooblastila za obravnavanje zahtevkov in odobritev odredb.

([132]) FISC sestavlja enajst sodnikov, ki jih imenuje vrhovni sodnik ZDA izmed sodnikov okrožnih sodišč ZDA, ki jih je pred tem imenoval predsednik in potrdil senat. Sodniki imajo trajni mandat, ki lahko preneha samo zaradi upravičenega razloga, in so zaposleni na sodišču FISC za obdobja, razporejena čez sedem let. FISA zahteva, da se sodniki izberejo iz najmanj sedmih različnih sodnih okrožij ZDA. Glej člen 103 FISA (člen 1803 (a) naslova 50 zakonodajne zbirke ZDA) in poročilo PCLOB o členu 215, str. 174 do 187. Sodnikom pomagajo izkušeni sodni uradniki, ki sestavljajo pravno osebje sodišča in pripravljajo pravne analize zahtev za zbiranje podatkov. Glej poročilo PCLOB o členu 215, str. 178, in dopis predsedujočega sodnika drugostopenjskega sodišča za nadzor tujih obveščevalnih podatkov, spoštovanega Reggieja B. Waltona, predsedniku odbora za pravosodje senata ZDA, spoštovanemu Patricku J. Leahyju (z dne 29. julija 2013) (v nadaljevanju: Waltonov dopis), str. 2 do 3.

([133]) FISCR sestavljajo trije sodniki, ki jih imenuje vrhovni sodnik ZDA in so izbrani izmed okrožnih ali prizivnih sodišč ZDA ter zaposleni za obdobja, razporejena čez sedem let. Glej člen 103 FISA (člen 1803 (b) naslova 50 zakonodajne zbirke ZDA).

([134]) Glej člene 1803 (b), 1861 a (f), 1881 a (h) in 1881 a (i)(4) naslova 50 zakonodajne zbirke ZDA.

([135]) Na primer, podrobnosti o cilju nadzora, tehnične informacije o metodologiji nadzora ali zagotovila glede tega, kako se bodo pridobljeni podatki uporabljali in razširjali. Glej poročilo PCLOB o členu 215, str. 177.

([136]) Člena 1804 (a) in 1801 (g) naslova 50 zakonodajne zbirke ZDA.

([137]) FISC lahko odobri zahtevek, zahteva dodatne informacije, odloči, da je potrebno zaslišanje, ali navede možnost zavrnitev zahtevka. Vlada na podlagi te predhodne ugotovitve pripravi končni zahtevek. Ta lahko vključuje bistvene spremembe prvotnega zahtevka na podlagi uvodnih opomb sodnika. Čeprav FISC odobri velik delež končnih zahtevkov, jih veliko vsebuje bistvene spremembe prvotnega zahtevka, npr. 24 % zahtevkov, odobrenih za obdobje od julija do septembra 2013. Glej poročilo PCLOB o členu 215, str. 179; Waltonov dopis, str. 3.

([138]) Poročilo PCLOB o členu 215, str. 179, opomba 619.

([139]) Člen 1803 (i)(1) in (3)(A) naslova 50 zakonodajne zbirke ZDA. S to novo zakonodajo so se izvedla priporočila PCLOB za vzpostavitev skupine strokovnjakov za varstvo zasebnosti in državljanske pravice, ki lahko deluje kot *amicus curiae*, da se sodišču zagotovijo pravni argumenti za okrepitev varstva zasebnosti in državljanskih pravic. Glej poročilo PCLOB o členu 215, str. 183 do 187.

([140]) Člen 1803 (i)(2)(A) naslova 50 zakonodajne zbirke ZDA. Po podatkih ODNI je že prišlo do takih imenovanj. Glej poročilo o napredku 2016 Signals Intelligence Reform (Reforma zbiranja obveščevalnih podatkov SIGINT).

([141]) Člen 1803 (i)(2)(B) naslova 50 zakonodajne zbirke ZDA.

(107) Kar zadeva pravni pooblastili za nadzor v okviru FISA, ki sta najpomembnejši za prenose podatkov v okviru zasebnostnega ščita EU-ZDA, se nadzor s strani FISC razlikuje.

(108) V skladu s členom 501 FISA ([142]), ki dovoljuje zbiranje „kakršnih koli oprijemljivih predmetov (vključno s knjigami, evidencami, spisi, dokumenti in drugimi listinami)“, mora zahtevek, ki se predloži FISC, vsebovati izjavo o dejstvih, ki kažejo, da obstajajo utemeljeni razlogi za sklepanje, da so zahtevani oprijemljivi predmeti pomembni za odobreno preiskavo (ki ni ocena nevarnosti), izvedeno za pridobitev tujih obveščevalnih podatkov, ki se ne nanašajo na državljana ZDA, ali za zaščito pred mednarodnim terorizmom ali tajnimi obveščevalnimi dejavnostmi. Zahtevek mora vsebovati tudi seznam postopkov za zmanjševanje količine podatkov, ki jih je generalni državni tožilec sprejel za hrambo in razširjanje zbranih obveščevalnih podatkov ([143]).

(109) V nasprotju s tem pa FISC v skladu s členom 702 FISA ([144]) ne dovoljuje posameznih nadzornih ukrepov, temveč dovoljuje nadzorne programe (kot sta programa PRISM in UPSTREAM) na podlagi letnih potrdil, ki jih pripravita generalni državni tožilec in direktor nacionalne obveščevalne službe. Člen 702 FISA dovoljuje ciljno osredotočanje na osebe, za katere se utemeljeno sklepa, da se nahajajo zunaj ZDA, za pridobitev tujih obveščevalnih podatkov ([145]). NSA tako izbiro cilja izvede v dveh korakih: prvič, analitiki NSA identificirajo nedržavljane ZDA v tujini, katerih nadzor bo na podlagi ocene analitikov zagotovil ustrezne tuje obveščevalne podatke, navedene v potrdilu; drugič, po identifikaciji teh posameznikov in odobritvi ciljnega osredotočanja nanje z mehanizmom obseženih pregledov v okviru NSA ([146]) se izbirnikom, ki opredelijo komunikacijska sredstva (kot so e-poštni naslovi), ki jih uporabljajo ciljne osebe, „dodelijo naloge“ (tj. ti izbirniki se razvijejo in uporabljajo) ([147]). Kot je navedeno, potrdila, ki ji odobri FISC, ne vsebujejo nobenih informacij o ciljnih posameznikih, temveč so v njih opredeljene kategorije tujih obveščevalnih podatkov ([148]). Čeprav FISC ne presoja – na podlagi verjetnega vzroka ali katerega koli drugega standarda – ustreznosti ciljnega osredotočanja na posameznike za pridobivanje tujih obveščevalnih podatkov ([149]), njegov nadzor zajema tudi nadzor nad izpolnjevanjem pogoja, da „je pomemben namen pridobivanja zbrati tuje obveščevalne podatke“ ([150]). NSA lahko namreč v skladu s členom 702 FISA zbira sporočila nedržavljanov ZDA zunaj ZDA samo, če je mogoče utemeljeno sklepati, da se zadevno komunikacijsko sredstvo uporablja za sporočanje tujih obveščevalnih podatkov (npr. povezanih z mednarodnim terorizmom, širjenjem jedrskega orožja ali sovražne kibernetske dejavnosti). Ugotovitve v zvezi s tem so predmet sodne presoje ([151]). V potrdilih morajo biti določeni tudi postopki izbire cilja in zmanjševanja količine podatkov ([152]).

([142]) Člen 1861 naslova 50 zakonodajne zbirke ZDA.
([143]) Člen 1861 (b) naslova 50 zakonodajne zbirke ZDA.
([144]) Člen 1881 naslova 50 zakonodajne zbirke ZDA.
([145]) Člen 1881a (a) naslova 50 zakonodajne zbirke ZDA.
([146]) Poročilo PCLOB o členu 702, str. 46.
([147]) Člen 1881a (h) naslova 50 zakonodajne zbirke ZDA.
([148]) Člen 1881a (g) naslova 50 zakonodajne zbirke ZDA. Po navedbah PCLOB so se te kategorije doslej večinoma nanašale na mednarodni terorizem in teme, kot je pridobivanje orožja za množično uničevanje. Glej poročilo PCLOB o členu 702, str. 25.
([149]) Poročilo PCLOB o členu 702, str. 27.
([150]) Člen 1881a naslova 50 zakonodajne zbirke ZDA.
([151]) „Liberty and Security in a Changing World“ („Svoboda in varnost v spreminjajočem se svetu“), poročilo in priporočila predsedniške skupine za presojo obveščevalnih in komunikacijskih tehnologij, 12. december 2013, str. 152.
([152]) Člen 1881a (i) naslova 50 zakonodajne zbirke ZDA.

Generalni državni tožilec in direktor nacionalne obveščevalne službe preverjata skladnost, agencije pa morajo kakršen koli primer neskladnosti sporočiti FISC ([153]) (pa tudi kongresu in predsedniškemu obveščevalnemu nadzornemu odboru), ki lahko na tej podlagi spremeni pooblastilo ([154]).

(110) Poleg tega je administracija ZDA privolila, da bo za povečanje učinkovitosti nadzora s strani FISC izvedla priporočilo PCLOB za predložitev dokumentacije odločb FISC o izbiri cilja iz člena 702, vključno z naključnim vzorcem seznamov nalog, da se FISC omogoči, da oceni, kako se zahteva glede namena zbiranja tujih obveščevalnih podatkov upošteva v praksi ([155]). Hkrati je administracija ZDA sprejela in izvedla ukrepe za revidiranje postopkov izbire cilja NSA za boljše dokumentiranje razlogov za zbiranje tujih obveščevalnih podatkov za odločitve o izbiri cilja ([156]).

Individualna pravna sredstva

(111) Na podlagi zakonodaje ZDA so posameznikom iz EU, na katere se nanašajo osebni podatki, na voljo številne možnosti, če jih skrbi, ali njihove osebne podatke obdelujejo (zbirajo, ocenjujejo itd.) člani obveščevalne skupnosti in, če jih, ali se upoštevajo veljavne omejitve v skladu z zakonodajo ZDA. Te možnosti se nanašajo zlasti na tri področja, in sicer: posege na podlagi FISA; nezakonit in namerni dostop vladnih uslužbencev do osebnih podatkov ter dostop do informacij na podlagi zakona o dostopu do informacij javnega značaja (Freedom of Information Act, v nadaljnjem besedilu: FOIA) ([157]).

(112) Prvič, zakon o nadzoru tujih obveščevalnih podatkov določa več pravnih sredstev za izpodbijanje nezakonitega elektronskega nadzora, ki so na voljo tudi nedržavljanom ZDA ([158]). To vključuje možnost, da posamezniki vložijo civilni zahtevek za denarno odškodnino proti ZDA, če so bile informacije o njih nezakonito in namerno uporabljene ali razkrite ([159]), da osebno tožijo uslužbence vlade ZDA (ki so ravnali „pod pretvezo zakona“) za denarno odškodnino ([160]) in da izpodbijajo zakonitost nadzora (ter zahtevajo omejitev informacij), če namerava vlada ZDA uporabiti ali razkriti kakršne koli informacije, ki so pridobljene ali izhajajo iz elektronskega nadzora, proti posamezniku v sodnem ali upravnem postopku v ZDA ([161]).

(113) Drugič, vlada ZDA je opozorila Komisijo na številne dodatne možnosti, ki bi jih posamezniki iz EU, na katere se nanašajo osebni podatki, lahko uporabili za pritožbo proti vladnim uslužbencem zaradi nezakonitega vladnega

([153]) Pravilo 13(b) poslovnika FISC določa, da mora vlada Sodišču predložiti pisno obvestilo takoj po odkritju, da se pooblastilo ali dovoljenje, ki ga je dodelilo Sodišče, izvaja na način, ki ni skladen s pooblastilom ali dovoljenjem Sodišča ali veljavno zakonodajo. Določa tudi, da mora vlada pisno obvestiti Sodišče o dejstvih in okoliščinah, povezanih s tako neskladnostjo. Vlada običajno predloži končno obvestilo iz pravila 13(a) potem, ko so znana vsa pomembna dejstva in so bile vse morebitne nedovoljene zbirke uničene. Glej Waltonov dopis, str. 10.

([154]) Člen 1881 (l) naslova 50 zakonodajne zbirke ZDA. Glej poročilo PCLOB o členu 702, str. 66 do 76 in poročilo NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act (Izvajanje člena 702 zakona o nadzoru tujih obveščevalnih podatkov s strani NSA), z dne 16. 4. 2014. Zbiranje osebnih podatkov za obveščevalne namene v skladu s členom 702 FISA je predmet notranjega in zunanjega nadzora v okviru izvršilne oblasti. Notranji nadzor med drugim vključuje notranje programe skladnosti za ocenjevanje in nadzor skladnosti s postopki izbire cilja in zmanjševanja količine podatkov, notranje in zunanje poročanje ODNI, Ministrstvu za pravosodje, kongresu in FISC o primerih neskladnosti ter letne preglede, ki se pošljejo istim organom. Zunanji nadzor vključuje predvsem preglede postopkov izbire cilja in zmanjševanja količine podatkov, ki jih izvajajo ODNI, Ministrstvo za pravosodje in generalni inšpektorji, ki nato poročajo kongresu in FISC, med drugim tudi o primerih neskladnosti. O pomembnih primerih neskladnosti je treba FISC poročati nemudoma, o drugih pa v četrtletnem poročilu. Glej poročilo PCLOB o členu 702, str. 66 do 77.

([155]) PCLOB, Recommendations Assessment Report (Poročilo o oceni izvajanja priporočil), 29. januar 2015, str. 20.

([156]) PCLOB, Recommendations Assessment Report (Poročilo o oceni izvajanja priporočil), 29. januar 2015, str. 16.

([157]) Poleg tega člen 10 zakona o postopkih za izmenjavo zaupnih podatkov (Classified Information Procedures Act) določa, da ZDA pri vsakem sodnem pregonu, pri katerem morajo dokazati, da gradivo predstavlja zaupne podatke (npr. ker zahteva varstvo pred nepooblaščenim razkritjem podatkov zaradi državne varnosti), obvestijo toženo stranko o tistih delih gradiva, za katere utemeljeno pričakujejo, da jih bodo uporabile za dokazovanje elementa kršitve zaupnosti podatkov.

([158]) Glej za naslednja zagotovila ODNI (Priloga VI), str. 16.

([159]) Člen 2712 naslova 18 zakonodajne zbirke ZDA.

([160]) Člen 1810 naslova 50 zakonodajne zbirke ZDA.

([161]) Člen 1806 naslova 50 zakonodajne zbirke ZDA.

dostopa do osebnih podatkov ali njihove uporabe, tudi za domnevne namene nacionalne varnosti (to so zakon o računalniških goljufijah in zlorabah (Computer Fraud Abuse Act) ([162]), zakon o zasebnosti elektronskih komunikacij (Electronic Communications Privacy Act) ([163]) in zakon o pravici do finančne zasebnosti (Right to Financial Privacy Act) ([164])). Vsa ta pravna sredstva se nanašajo na posebne podatke, ciljne posameznike in/ali vrste dostopa (npr. oddaljeni dostop računalnika prek interneta) in so na voljo pod določenimi pogoji (npr. naklepno/namerno ravnanje, ravnanje zunaj uradnih pooblastil, utrpela škoda) ([165]). Splošnejšo možnost pravnega varstva nudi zakon o upravnem postopku (Administrative Procedure Act, člen 702 naslova 5 Zakonodajne zbirke ZDA), v skladu s katerim ima „vsaka oseba, ki ji je bila storjena pravna krivica zaradi ukrepanja agencije ali na katero je to ukrepanje agencije negativno vplivalo ali jo oškodovalo," pravico, da zahteva sodno presojo. To vključuje možnost, da se od sodišča zahteva, naj „ugotovi, da so ukrepanje, ugotovitve in sklepi agencije, za katere je bilo ugotovljeno, da so […] samovoljni, kapriciozni, da predstavljajo zlorabo diskrecijske pravice ali so na drugačen način neskladni s pravom, nezakoniti in naj jih razveljavi" ([166]).

(114) Nenazadnje je vlada ZDA opozorila, da je zakon o dostopu do informacij javnega značaja sredstvo, s pomočjo katerega lahko nedržavljani ZDA zahtevajo dostop do obstoječih evidenc zvezne agencije, tudi če te evidence vsebujejo osebne podatke posameznika ([167]). Zakon o dostopu do informacij javnega značaja se ne osredotoča na določanje možnosti uporabe individualnih pravnih sredstev proti posegom v osebne podatke kot take, čeprav bi lahko posameznikom načeloma omogočal, da pridobijo dostop do ustreznih informacij, ki jih hranijo nacionalne obveščevalne agencije. Zdi se, da so tudi s tega vidika možnosti omejene, saj lahko agencije zadržijo informacije, ki spadajo med določene navedene izjeme, vključno z dostopom do zaupnih nacionalnih obveščevalnih podatkov in podatkov v zvezi s preiskavami kazenskega pregona ([168]). Vendar lahko posamezniki z zahtevo upravnega in sodnega pregleda izpodbijajo uporabo takih izjem s strani nacionalnih obveščevalnih agencij.

(115) Čeprav imajo zato posamezniki, vključno s posamezniki iz EU, na katere se nanašajo osebni podatki, na voljo različne možnosti pravnega varstva, če so predmet nezakonitega (elektronskega) nadzora za namene nacionalne varnosti, je prav tako jasno, da vsaj nekatere pravne podlage, ki jih lahko uporabijo obveščevalni organi ZDA (npr. Odredba št. 12333), niso zajete. Poleg tega so tudi kadar za nedržavljane ZDA načeloma obstajajo možnosti pravnega varstva, kot na primer pri nadzoru v skladu s FISA, razpoložljive možnosti za ukrepanje omejene ([169]) in zahtevki posameznikov (vključno z državljani ZDA) se razglasijo za nedopustne, če ne morejo dokazati pravnega interesa ([170]), kar omejuje dostop do rednih sodišč ([171]).

(116) Da bi zagotovila dodatne možnosti pravnega varstva, ki bi bile na voljo vsem posameznikom iz EU, na katere se nanašajo osebni podatki, se je vlada ZDA odločila, da bo ustvarila nov mehanizem varuha človekovih pravic, kot je določen v dopisu državnega sekretarja ZDA Komisiji, ki je priložen v Prilogi III k temu sklepu. Ta mehanizem temelji na imenovanju visokega koordinatorja (na ravni podsekretarja) na zunanjem ministrstvu v skladu s PPD-28 kot kontaktne točke za tuje vlade, na katero lahko naslovijo vprašanja v zvezi z obveščevalnimi dejavnostmi SIGINT ZDA, vendar bistveno presega prvotni koncept.

([162]) Člen 1030 naslova 18 zakonodajne zbirke ZDA.
([163]) Členi 2701 do 2712 naslova 18 zakonodajne zbirke ZDA.
([164]) Člen 3417 naslova 12 zakonodajne zbirke ZDA.
([165]) Zagotovila ODNI (Priloga VI), str. 17.
([166]) Člen 706(2)(A) naslova 5 zakonodajne zbirke ZDA.
([167]) Člen 552 naslova 5 zakonodajne zbirke ZDA. Podobni zakoni obstajajo na ravni države.
([168]) V tem primeru posameznik običajno prejme standardni odgovor, s katerim agencija odkloni potrditev ali zavrnitev obstoja kakršnih koli evidenc. Glej zadevo ACLU proti CIA, št. 710 F.3d 422 (Zvezno prizivno sodišče za okrožje D.C., 2014).
([169]) Glej zagotovila ODNI (Priloga VI), str. 16. Glede na predložena pojasnila razpoložljive možnosti za ukrepanje bodisi zahtevajo obstoj *škode* (člen 2712 naslova 18 zakonodajne zbirke ZDA in člen 1810 naslova 50 zakonodajne zbirke ZDA) ali dokaz, da *namerava vlada uporabiti ali razkriti podatke*, ki so pridobljeni ali izhajajo iz elektronskega nadzora zadevne osebe, proti tej osebi *v sodnem ali upravnem postopku* v ZDA (člen 1806 naslova 50 zakonodajne zbirke ZDA). Vendar, kot je Sodišče večkrat poudarilo, za ugotovitev posega v temeljne pravice do zasebnosti ni pomembno, ali je zadevna oseba zaradi zadevnega posega utrpela kakršne koli negativne posledice. Glej zadevo Schrems, točka 89 z nadaljnjimi sklici.
([170]) To merilo dopustnosti izhaja iz zahteve po „nasprotujočih si zahtevkih" („case or controversy") iz člena III ustave ZDA.
([171]) Glej zadevo Clapper proti Amnesty Int'l USA, Zbirka odločb državnega sodišča št. 133, str. 1138 in 1144 (2013). Kar zadeva uporabo dopisov o nacionalni varnosti, zakon ZDA o svobodi (USA FREEDOM Act, členi 502(f) do 503) določa, da je treba zahteve po nerazkritju redno pregledovati in da morajo biti *naslovniki* NSL obveščeni, kadar dejstva ne podpirajo več zahteve po nerazkritju (glej zagotovila ODNI (Priloga VI), str. 13). Vendar to ne zagotavlja, da bodo posamezniki iz EU, na katere se nanašajo osebni podatki, obveščeni, da so predmet preiskave.

(117) V skladu z obveznostmi vlade ZDA bo mehanizem varuha človekovih pravic zagotavljal, da se bodo posamezne pritožbe ustrezno proučile in obravnavale ter da bodo posamezniki prejeli neodvisno potrditev, da so bili zakoni ZDA upoštevani ali, v primeru kršitve takih zakonov, da je bila neskladnost odpravljena ([172]). Mehanizem vključuje „varuha človekovih pravic na področju zasebnostnega ščita“, tj. podsekretarja in dodatno osebje ter druge nadzorne organe, ki bo nadzoroval različne člane obveščevalne skupnosti, na sodelovanje katerih se bo varuh človekovih pravic na področju zasebnostnega ščita zanašal pri obravnavi pritožb. Zlasti če se bo posameznikova zahteva nanašala na združljivost nadzora s pravom ZDA, bi se lahko varuh človekovih pravic na področju zasebnostnega ščita obrnil na neodvisne nadzorne organe s pooblastili za preiskovanje (kot so generalni inšpektorji ali PCLOB). V vsakem primeru državni sekretar zagotovi, da ima varuh človekovih pravic sredstva za zagotavljanje, da njegov odgovor na posamezne zahtevke temelji na vseh potrebnih informacijah.

(118) Ta „sestavljena struktura“ mehanizmu varuha človekovih pravic zagotavlja neodvisen nadzor in individualna pravna sredstva. Poleg tega se s sodelovanjem z drugimi nadzornimi organi zagotovi, da ima dostop do potrebnega strokovnega znanja in izkušenj. Z uvedbo obveznosti varuha človekovih pravic na področju zasebnostnega ščita, da potrdi skladnost ali odpravo morebitne neskladnosti, mehanizem odraža zavezo vlade ZDA kot celote, da bo obravnavala in rešila pritožbe posameznikov iz EU.

(119) Prvič, za razliko od izključno medvladnega mehanizma bo varuh človekovih pravic na področju zasebnostnega ščita prejemal pritožbe posameznikov in odgovarjal nanje. Take pritožbe lahko javni organi naslovijo na nadzorne organe držav članic, ki so pristojni za nadzor nacionalnih varnostnih služb in/ali obdelavo osebnih podatkov, ki jih bodo predložili centraliziranemu organu EU, ta pa jih bo posredoval varuhu človekovih pravic na področju zasebnostnega ščita ([173]). To bo dejansko prineslo koristi za posameznike iz EU, ki se lahko obrnejo na nacionalni organ „blizu doma“ in v svojem jeziku. Naloga takega organa bo pomagati posamezniku pri vložitvi zahtevka pri varuhu človekovih pravic na področju zasebnostnega ščita, ki bo vseboval osnovne informacije in se bo zato lahko štel za „popolnega“. Posamezniku ni treba dokazati, da je vlada ZDA z obveščevalnimi dejavnostmi SIGINT dejansko dostopala do njegovih osebnih podatkov.

(120) Vlada ZDA se zavezuje, da bo zagotovila, da si bo varuh človekovih pravic na področju zasebnostnega ščita pri opravljanju svojih nalog lahko zagotovil sodelovanje drugih mehanizmov za nadzor in pregled skladnosti, ki jih določa pravo ZDA. To bo včasih vključevalo nacionalne obveščevalne organe, zlasti če se zahteva lahko razlaga kot zahteva za dostop do dokumentov v skladu z zakonom o dostopu do informacij javnega značaja (Freedom of Information Act). V drugih primerih, zlasti kadar so zahteve povezane z združljivostjo nadzora s pravom ZDA, bo tako sodelovanje vključevalo neodvisne nadzorne organe (npr. generalne inšpektorje), ki bodo imeli nalogo in pooblastila za izvedbo podrobne preiskave (zlasti na podlagi dostopa do vseh ustreznih dokumentov in pooblastila, da zahtevajo informacije in izjave) ter bodo obravnavali neskladnost ([174]). Varuh človekovih pravic na področju zasebnostnega ščita bo lahko tudi predložil zadeve PCLOB v proučitev ([175]). Če kateri koli od teh nadzornih organov odkrije neskladnost, bo moral zadevni organ obveščevalne skupnosti (npr. obveščevalna

([172]) Če pritožnik zahteva dostop do dokumentov, ki jih imajo javni organi ZDA, se uporabljajo pravila in postopki iz zakona o dostopu do informacij javnega značaja (Freedom of Information Act). To vključuje možnost, da zahteva pravno varstvo (namesto neodvisnega nadzora), če je zahteva zavrnjena, v skladu s pogoji iz zakona o dostopu do informacij javnega značaja (Freedom of Information Act).

([173]) V skladu z mehanizmom varuha človekovih pravic (Priloga III), člen 4(f), bo varuh človekovih pravic na področju zasebnostnega ščita organu za obravnavo pritožb posameznikov iz EU neposredno sporočil, kdo bo odgovoren za komuniciranje s posameznikom, ki je predložil zahtevo. Če je neposredna komunikacija del „osnovnih postopkov“, ki lahko zagotovijo zahtevano rešitev (npr. zahteva za dostop na podlagi zakona o dostopu do informacij javnega značaja (Freedom of Information Act), glej člen 5), bo taka komunikacija potekala v skladu z veljavnimi postopki.

([174]) Glej mehanizem varuha človekovih pravic (Priloga III), člen 2(a). Glej tudi uvodne izjave 0 do 0.

([175]) Glej mehanizem varuha človekovih pravic (Priloga III), člen 2(c). V skladu s pojasnili vlade ZDA PCLOB stalno pregleduje politike in postopke organov ZDA, ki so pristojni za boj proti terorizmu, pa tudi njihovo izvajanje, da bi ugotovila, ali njihovi ukrepi zagotavljajo „ustrezno varstvo zasebnosti in državljanskih svobočin ter so skladni z veljavnimi zakoni, predpisi in politikami v zvezi z zasebnostjo in državljanskimi svobočinami“. Poleg tega „prejema in pregleduje poročila in druge informacije uradnikov za varstvo zasebnosti in uradnikov za državljanske svobočine ter jim, kadar je to ustrezno, zagotovi priporočila v zvezi z njihovimi dejavnostmi“.

agencija) odpraviti neskladnosti, saj bo varuh človekovih pravic le tako lahko predložil „pozitiven“ odgovor posamezniku (tj. da je bila morebitna neskladnost odpravljena), h kateremu se je vlada ZDA zavezala. V okviru sodelovanja bo varuh človekovih pravic na področju zasebnostnega ščita tudi obveščen o rezultatu preiskave in mu bo omogočeno, da prejme vse informacije, ki jih potrebuje za pripravo odgovora.

(121) Varuh človekovih pravic na področju zasebnostnega ščita bo neodvisen od obveščevalne skupnosti ZDA in tako ne bo prejemal njenih navodil ([176]). To je zelo pomembno ob upoštevanju dejstva, da bo moral varuh človekovih pravic „potrditi“, da (i) je bila pritožba ustrezno proučena in da (ii) se je upoštevala ustrezna zakonodaja ZDA, vključno zlasti z omejitvami in zaščitnimi ukrepi iz Priloge VI, ali, v primeru neskladnosti, da je bila taka kršitev odpravljena. Da bo varuh človekovih pravic na področju zasebnostnega ščita lahko zagotovil navedeno neodvisno potrdilo, bo moral prejeti potrebne informacije o preiskavi, na podlagi katerih bo lahko ocenil točnost odgovora na pritožbo. Poleg tega se je državni sekretar zavezal, da bo podsekretar objektivno opravljal naloge varuha človekovih pravic na področju zasebnostnega ščita in da ne bo pod neustreznim vplivom, ki bi lahko vplival na predloženi odgovor.

(122) Na splošno ta mehanizem zagotavlja, da bodo posamezne pritožbe temeljito preiskane in rešene ter da bodo vsaj na področju nadzora pri tem vključeni neodvisni nadzorni organi s potrebnim strokovnim znanjem in izkušnjami ter pooblastili za preiskovanje in varuh človekovih pravic, ki bo lahko svoje naloge izvajal, ne da bi bil pod neustreznim, zlasti političnim, vplivom. Poleg tega bodo lahko posamezniki predložili pritožbe, ne da bi jim bilo treba dokazati, da so bili nadzorovani, ali za to navesti indice ([177]). Komisija je na podlagi navedenega zadovoljna, da obstajajo ustrezna in učinkovita zagotovila proti zlorabi.

(123) Na podlagi zgoraj navedenega je Komisija sklenila, da ZDA zagotavljajo učinkovito pravno varstvo pred posegi njenih obveščevalnih organov v temeljne pravice oseb, katerih podatki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije v ZDA.

(124) V zvezi s tem Komisija upošteva sodbo Sodišča v zadevi Schrems, v skladu s katero „ureditev, ki ne določa nobene možnosti, da bi posameznik lahko uporabil pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravo ali izbris takih podatkov, posega v bistvo temeljne pravice do učinkovitega sodnega varstva, določene v členu 47 Listine“ ([178]). Ocena Komisije je potrdila, da so v Združenih državah Amerike zagotovljena taka pravna sredstva, vključno prek uvedbe mehanizma varuha človekovih pravic. Mehanizem varuha človekovih pravic zagotavlja neodvisen nadzor s pooblastili za preiskovanje. V okviru stalnega spremljanja zasebnostnega ščita, ki ga izvaja Komisija in vključuje tudi letni skupni pregled, ki zajema tudi varuha človekovih pravic, se bo znova ocenila učinkovitost tega mehanizma.

3.2 *Dostop in uporaba s strani javnih organov ZDA za namene kazenskega pregona in javnega interesa*

(125) Kar zadeva posege v osebne podatke, ki se prenašajo v okviru zasebnostnega ščita EU-ZDA za namene kazenskega pregona, je vlada ZDA (prek Ministrstva za pravosodje) podala zagotovila glede veljavnih omejitev in zaščitnih ukrepov, ki po oceni Komisije izkazujejo ustrezno stopnjo varstva.

([176]) Glej sodbo v zadevi Roman Zakharov proti Rusiji z dne 4. decembra 2015 (Veliki senat), tožba št. 47143/06, točka 275 („čeprav je načeloma zaželeno, da je za nadzor odgovoren sodnik, je lahko nadzor organov, ki niso sodni organi, združljiv s Konvencijo, če je nadzorni organ neodvisen od organov, ki izvajajo nadzor, ter če ima zadostna in učinkovita nadzorna pooblastila“).

([177]) Glej sodbo v zadevi Kennedy proti Združenemu kraljestvi z dne 18. maja 2010, tožba št. 26839/05, točka 167.

([178]) Schrems, točka 95. Kot je razvidno iz točk 91 in 96 sodbe, se točka 95 nanaša na raven varstva, ki je zagotovljena v pravnem redu Unije, kateri mora biti raven varstva tretje države „v bistvenem enaka“. V skladu s točkama 73 in 74 sodbe to ne pomeni, da tretja država zagotavlja povsem enako raven varstva ali sredstev, ki jih uporabi za zagotovitev take ravni, vendar se morajo uporabljena sredstva v praksi vseeno izkazati kot učinkovita.

(126) V skladu s temi informacijami preiskave in zasegi organov pregona iz četrtega amandmaja ustave ZDA ([179]) načeloma ([180]) zahtevajo sodni nalog na podlagi dokazanega „utemeljenega razloga". V nekaterih posebej določenih in izjemnih primerih, ko se zahteva za nalog ne uporablja ([181]), je kazenski pregon predmet preskusa „razumnosti" ([182]). Ali sta preiskava ali zaseg razumna, „se določi z oceno, v kakšni meri preiskava ali zaseg posega v zasebnost posameznika na eni strani in v kakšni meri sta potrebna za spodbujanje zakonitih vladnih interesov na drugi strani" ([183]). Bolj splošno, četrti amandma zagotavlja zasebnost in dostojanstvo ter ščiti pred samovoljnimi in nasilnimi dejanji vladnih uslužbencev ([184]). Ti pojmi zajemajo zamisel o nujnosti in sorazmernosti v pravu Unije. Ko organom kazenskega pregona zaseženih sredstev ni treba več uporabljati kot dokaze, bi jih morali vrniti ([185]).

(127) Čeprav pravica iz četrtega amandmaja ne zajema oseb, ki niso državljani ZDA in ne prebivajo v Združenih državah Amerike, so te z njo vseeno posredno varovane, saj osebne podatke hranijo ameriška podjetja, kar pomeni, da morajo organi kazenskega pregona v vsakem primeru zaprositi za sodno odobritev (ali vsaj spoštovati zahtevo po razumnosti) ([186]). Dodatno varstvo zagotavljajo posebni zakonsko določeni organi, pa tudi smernice Ministrstva za pravosodje, ki omejujejo dostop organov pregona do podatkov na razloge nujnosti in sorazmernosti (npr. z zahtevanjem, da FBI uporablja najmanj vsiljive preiskovalne metode, ki so mogoče, ob upoštevanju vpliva na zasebnost in državljanske svoboščine) ([187]). Glede na zagotovila vlade ZDA se enako ali večje varstvo uporablja za preiskave organov pregona na ravni države (z upoštevanjem preiskav, ki se izvedejo v skladu z državnimi zakoni) ([188]).

(128) Čeprav predhodna sodna odobritev sodišča ali velike porote (preiskovalni organ sodišča, ki ga sodnik ali sodnik nižjega sodišča vključi v poroto) ni potrebna v vseh primerih ([189]), so upravni sodni pozivi omejeni na posebne primere in bodo predmet neodvisnega sodnega pregleda vsaj v primerih, ko vlada zahteva izvršilni postopek pred sodiščem ([190]).

([179]) V skladu s četrtim amandmajem Ustave ZDA „pravica ljudi, da so oni sami, njihove hiše, dokumenti in predmeti varni pred nerazumnimi preiskavami in zasegi, ne sme biti kršena in izdan ne sme biti noben nalog, razen na podlagi utemeljenega suma, podprtega z zaprisego ali izjavo, in ki zlasti opisuje kraj, ki ga je treba preiskati, ter osebe in predmete, ki jih je treba zaseči." Naloge za preiskavo lahko izdajo le sodniki (nižjih sodišč). Zvezne naloge za kopiranje elektronsko shranjenih informacij dodatno ureja pravilo 41 zveznih pravil o izvajanju kazenskega postopka.

([180]) Vrhovno sodišče je večkrat navedlo, da so preiskave brez nalogov „izjemne". Glej npr. zadevo Johnson proti Združenim državam, Zbirka odločb Vrhovnega sodišča št. 333, str. 10 in 14 (1948); zadevo McDonald proti Združenim državam, Zbirka odločb Vrhovnega sodišča št. 335, str. 451 in 453 (1948); zadevo Camara proti Municipal Court, Zbirka odločb Vrhovnega sodišča št. 387, str. 523, 528 in 529 (1967) ter zadevo G.M. Leasing Corp. v. United States, Zbirka odločb Vrhovnega sodišča št. 429, str. 338, 352, 353 in 355 (1977). Podobno vrhovno sodišče redno poudarja, da „je najosnovnejše ustavno pravilo na tem področju, da so preiskave, opravljene zunaj sodnega procesa brez predhodnega dovoljenja sodnika ali sodnika nižjega sodišča, kot take nerazumne v skladu s četrtim amandmajem – ter so dopustne le v nekaterih posebej določenih in natančno opisanih izjemnih primerih". Glej npr. zadevo Coolidge proti New Hampshire, Zbirka odločb Vrhovnega sodišča št. 403, str. 443, 454 in 455 (1971) in zadevo G.M. Leasing Corp. v. United States, Zbirka odločb Vrhovnega sodišča št. 429, str. 338, 352, 353 in 358 (1977).

([181]) Zadeva City of Ontario, Cal. proti Quon, Zbirka odločb Državnega sodišča št. 130, str. 2619 in 2630 (2010).

([182]) Poročilo PCLOB o členu 215, str. 107, ki se sklicuje na zadevo Maryland proti King, Zbirka odločb Državnega sodišča št. 133, str. 1958 in 1970 (2013).

([183]) Poročilo PCLOB o členu 215, str. 107, ki se sklicuje na zadevo Samson proti California, Zbirka odločb Vrhovnega sodišča št. 547, str. 843 in 848 (2006).

([184]) Zadeva City of Ontario, Cal. proti Quon, Zbirka odločb Državnega sodišča št. 130, str. 2619 in 2630 (2010), ter str. 2627.

([185]) Glej npr. zadevo *Združene države Amerike proti Wilson*, št. 540 F.2d 1100 (Zvezno prizivno sodišče za okrožje D.C., 1976).

([186]) Glej sodbo v zadevi Roman Zakharov proti Rusiji z dne 4. decembra 2015 (Veliki senat), tožba št. 47143/06, točka 269, v skladu s katero je „zahteva po predložitvi dovoljenja za prestrezanje komunikacij ponudniku komunikacijskih storitev pred pridobitvijo dostopa do komunikacij posameznika eden najpomembnejših zaščitnih ukrepov pred zlorabo organov kazenskega pregona, ki zagotavlja, da se v vseh primerih prestrezanja pridobi ustrezno dovoljenje".

([187]) Zagotovila Ministrstva za pravosodje (Priloga VII), str. 4 z nadaljnjimi sklici.

([188]) Zagotovila ODNI (Priloga VII), opomba 2.

([189]) Glede na informacije, ki jih je prejela Komisija, in ne glede na posebna področja, ki verjetno niso pomembna za prenose podatkov v okviru zasebnostnega ščita EU–ZDA (npr. preiskave goljufij na področju zdravstvenega varstva, zlorabe otrok ali primerov nadzorovanih snovi), se to večinoma nanaša na nekatere organe na podlagi zakona o zasebnosti elektronskih komunikacij (Electronic Communications Privacy Act), in sicer zahteve za osnovne podatke o naročnikih, sejah in obračunavanju (člen 2703(c)(1) in (2) naslova 18 zakonodajne zbirke ZDA, npr. naslov, vrsta/dolžina storitve) in za vsebino elektronskih sporočil, starih več kot 180 dni (člen 2703 (a) in (b) naslova 18 zakonodajne zbirke ZDA). Vendar mora biti zadevni posameznik v slednjem primeru obveščen in ima tako možnost izpodbijati zahtevo pred sodiščem. Glej tudi pregled Ministrstva za pravosodje, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Preiskovanje in zaseg računalnikov in pridobivanje elektronskih dokazov v kazenskih preiskavah), poglavje 3: Stored Communications Act (zakon o shranjenih komunikacijah), str. 115–138.

([190]) Glede na zagotovila vlade ZDA lahko prejemniki upravnih sodnih pozivov izpodbijajo te pozive pred sodiščem z utemeljitvijo, da so nerazumni, tj. skrajni, represivni ali obremenjujoči. Glej zagotovila Ministrstva za pravosodje (Priloga VII), str. 2.

(129) Enako velja za uporabo upravnih sodnih pozivov za namene javnega interesa. Poleg tega se glede na zagotovila vlade ZDA podobne vsebinske omejitve uporabljajo tudi v zvezi s tem, da lahko agencije zahtevajo dostop samo do tistih podatkov, ki so pomembni za zadeve, ki spadajo v njihovo pristojnost, in da morajo upoštevati standard razumnosti.

(130) Poleg tega pravo ZDA zagotavlja številne možnosti pravnega varstva za posameznike proti javnemu organu ali enemu od njegovih uslužbencev, če ti organi obdelujejo osebne podatke. Te možnosti, ki vključujejo zlasti zakon o upravnem postopku (Administrative Procedure Act – APA), zakon o dostopu do informacij javnega značaja (Freedom of Information Act – FOIA) in zakon o zasebnosti elektronskih komunikacij (Electronic Communications Privacy Act – ECPA), so na voljo vsem posameznikom, ne glede na njihovo državljanstvo, v skladu z morebitnimi veljavnimi pogoji.

(131) Običajno ima v skladu z določbami o sodni presoji zakona o upravnem postopku ([191]) (Administrative Procedure Act), „vsaka oseba, ki ji je bila storjena pravna krivica zaradi ukrepanja agencije ali na katero je to ukrepanje agencije negativno vplivalo ali jo oškodovalo," pravico, da zahteva sodno presojo ([192]). To vključuje možnost, da se od sodišča zahteva, naj „ugotovi, da so ukrepanje, ugotovitve in sklepi agencije, za katere je bilo ugotovljeno, da so […] samovoljni, kapriciozni, da predstavljajo zlorabo diskrecijske pravice ali so na drugačen način neskladni s pravom, nezakoniti in naj jih razveljavi" ([193]).

(132) Naslov II zakona o zasebnosti elektronskih komunikacij ([194]) (Electronic Communications Privacy Act) podrobneje določa sistem zakonskih pravic do zasebnosti in tako ureja dostop organov kazenskega pregona do vsebin telefonskih, ustnih ali elektronskih komunikacij, ki jih hranijo tretji ponudniki storitev ([195]). Kot kaznivo dejanje obravnava nezakonit dostop do takih komunikacij (tj. dostop, ki ga ne odobri sodišče ali ki drugače ni dopusten) in določa pravno varstvo za prizadetega posameznika, saj lahko vloži civilno tožbo na zveznem sodišču ZDA za dejansko in kaznovalno odškodnino ter za pravično nadomestilo ali ugotovitveno določbo proti vladnemu uslužbencu, ki je namerno storil taka nezakonita dajanja, ali Združenim državam Amerike.

(133) Prav tako ima v skladu z zakonom o dostopu do informacij javnega značaja (Freedom of Information Act, člen 552 naslova 5 zakonodajne zbirke ZDA) vsaka oseba pravico, da pridobi dostop do evidenc zvezne agencije in, ko izčrpa vsa upravna sredstva, zahteva izvršitev take pravice na sodišču, razen če take evidence pred javnim razkritjem varuje izjema ali posebno izvzetje za organe kazenskega pregona ([196]).

([191]) Člen 702 naslova 5 zakonodajne zbirke ZDA.

([192]) Običajno se sodna presoja opravi le za „končno" ukrepanje agencije in ne za „predhodno, postopkovno ali vmesno" ukrepanje agencije. Glej člen 704 naslova 5 zakonodajne zbirke ZDA.

([193]) Člen 706(2)(A) naslova 5 zakonodajne zbirke ZDA.

([194]) Členi 2701 do 2712 naslova 18 zakonodajne zbirke ZDA.

([195]) Zakon o zasebnosti elektronskih komunikacij (Electronic Communications Privacy Act) zagotavlja varstvo komunikacij, ki jih hranita dva opredeljena razreda ponudnikov omrežnih storitev, in sicer ponudniki: (i) storitev elektronske komunikacije, na primer telefonije ali elektronske pošte, in (ii) storitev daljinske obdelave, kot so storitve računalniškega shranjevanja ali obdelave.

([196]) Vendar so taka izvzetja opredeljena. Na primer v skladu s členom 552 (b)(7) naslova 5 zakonodajne zbirke ZDA so pravice iz zakona o dostopu do informacij javnega značaja (Freedom of Information Act) izvzete za „evidence ali informacije, zbrane za namene kazenskega pregona, vendar le, če se zaradi priprave evidenc ali informacij organov kazenskega pregona (A) lahko razumno pričakuje, da bo posegala v izvršilne postopke, (B) če bi bila zato oseba prikrajšana za pravico do poštenega ali nepristranskega sojenja, (C) če se lahko zato razumno pričakuje, da bo pomenila neupravičen poseg v zasebnost, (D) če se zato lahko razumno pričakuje, da se bodo razkrile identiteta zaupnega vira, vključno z državno, lokalno ali tujo agencijo ali organom ali katero koli zasebno institucijo, ki je predložila informacije kot zaupne, in, v primeru evidence ali informacij, ki jih je zbral organ kazenskega pregona med kazensko preiskavo ali agencija, ki opravlja zakonito obveščevalno dejavnost za zagotavljanje nacionalne varnosti, informacije, ki jih je zagotovil zaupni vir, (E) če bi se zato razkrile tehnike in postopki kazenskih preiskav ali pregona ali smernice za kazenske preiskave ali pregon, če se za tako razkritje lahko razumno pričakuje, da bi lahko povzročilo tveganje izogibanja pravu, ali (F) če se lahko razumno pričakuje, da se bo ogrozilo življenje ali fizična varnost katerega koli posameznika". Velja tudi, da „[č]e se predloži zahteva, ki vključuje dostop do evidenc [kadar se lahko razumno pričakuje, da bi njihova priprava posegala v kazenski postopek] in – če (A) preiskava ali postopek vključuje morebitno kršitev kazenskega prava in če (B) obstaja razlog za prepričanje, da (i) subjekt preiskave ali postopka ni seznanjen z njenim potekom in da (ii) bi lahko razkritje obstoja evidenc razumno poseglo v kazenski postopek, lahko agencija, dokler obstajajo navedene okoliščine, evidence obravnava tako, kot da zanje ne veljajo zahteve iz tega člena". (Člen 552 (c)(1) naslova 5 zakonodajne zbirke ZDA).

(134) Poleg tega več drugih zakonov dodeljuje posameznikom pravico, da vložijo tožbo zoper javni organ ali uslužbenca ZDA zaradi obdelave njihovih osebnih podatkov; taki zakoni so zakon o prisluškovanju telefonskim pogovorom ([197]) (Wiretap Act), zakon o računalniških goljufijah in zlorabah ([198]) (Computer Fraud and Abuse Act), zvezni zakon o odškodninskih zahtevkih ([199]) (Federal Torts Claim Act), zakon o pravici do finančne zasebnosti (Right to Financial Privacy Act) ([200]) in zakon o poštenem kreditnem poročanju (Fair Credit Reporting Act) ([201]).

(135) Komisija je zato sklenila, da so v ZDA vzpostavljena pravila, ki so namenjena omejitvi morebitnih posegov za namene kazenskega pregona ([202]) ali druge namene javnega interesa v temeljne pravice oseb, katerih osebni podatki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije v ZDA, na tisto, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, in ki zagotavljajo učinkovito pravno varstvo pred takimi posegi.

4. USTREZNA STOPNJA VARSTVA V OKVIRU ZASEBNOSTNEGA ŠČITA EU-ZDA

(136) Ob upoštevanju navedenih ugotovitev Komisija meni, da ZDA zagotavljajo ustrezno stopnjo varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije samocertificiranim organizacijam.

(137) Komisija zlasti meni, da načela, ki jih je izdalo Ministrstvo za trgovino ZDA, kot celota zagotavljajo raven varstva osebnih podatkov, ki je v bistvu enakovredna ravni, ki jo zagotavljajo osnovna načela, določena v Direktivi 95/46/ES.

(138) Poleg tega je učinkovita uporaba načel zagotovljena z obveznostmi glede preglednosti in upravljanjem zasebnostnega ščita s strani Ministrstva za trgovino.

(139) Komisija tudi meni, da nadzorni in pritožbeni mehanizmi, ki jih zagotavlja zasebnostni ščit, kot celota omogočajo ugotavljanje kršitev načel s strani organizacij v zasebnostnem ščitu in njihovo kaznovanje v praksi ter posamezniku, na katerega se nanašajo osebni podatki, ponujajo pravna sredstva za pridobitev dostopa do osebnih podatkov, povezanih z njim, in, na koncu, popravek ali izbris takih podatkov.

(140) Nenazadnje, Komisija na podlagi razpoložljivih informacij o pravnem redu ZDA, vključno z zavezami vlade ZDA, meni, da bodo kakršni koli posegi javnih organov ZDA v temeljne pravice oseb, katerih podatki se v okviru zasebnostnega ščita prenašajo iz Unije v ZDA za namene nacionalne varnosti, kazenskega pregona ali drugih javnih interesov, in iz tega izhajajoče omejitve, uvedene za samocertificirane organizacije v zvezi z njihovim spoštovanjem načel, omejeni na tisto, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, in da obstaja učinkovito pravno varstvo pred takim posegom.

([197]) Člen 2510 in naslednji naslova18 zakonodajne zbirke ZDA. V skladu z zakonom o prisluškovanju telefonskim pogovorom (Wiretap Act, člen 2520 naslova 18 zakonodajne zbirke ZDA) lahko oseba, katere telefonska, ustna ali elektronska komunikacija je prestrežena, razkrita ali namerno uporabljena, vloži civilno tožbo zaradi kršitve navedenega zakona, v nekaterih primerih tudi proti posameznemu vladnemu uslužbencu ali Združenim državam Amerike. V zvezi z zbiranjem podatkov o naslovu in o drugih nevsebinskih informacij (npr. naslov IP, naslov prejemnika/naslov pošiljatelja) glej tudi poglavje o snemalnikih klicev ter napravah za pasti in sledenje (Pen Registers and Trap and Trace Devices) v naslovu 18 (členi 3121–3127 naslova 18 zakonodajne zbirke ZDA ter člen 2707 v zvezi s civilno tožbo).

([198]) Člen 1030 naslova 18 zakonodajne zbirke ZDA. V skladu z zakonom o računalniških goljufijah in zlorabah (Computer Fraud and Abuse Act) lahko posameznik toži vsakega posameznika zaradi namernega nepooblaščenega dostopa (ali dostopa, ki presega pooblastila), da bi pridobil informacije od finančne institucije, računalniškega sistema vlade ZDA ali drugega določenega računalnika, med drugim v določenih primerih tudi proti posameznemu vladnemu uslužbencu.

([199]) Člen 2671 in naslednji naslova 28 zakonodajne zbirke ZDA. V skladu z zveznim zakonom o odškodninskih zahtevkih (Federal Torts Claim Act) lahko posameznik v določenih primerih toži Združene države Amerike zaradi „kaznivega dejanja, storjenega iz malomarnosti, ali nedopustnega dejanja ali opustitve katerega koli vladnega uslužbenca med opravljanjem nalog v okviru njegovega delovnega mesta ali zaposlitve“.

([200]) Člen 3401 in naslednji naslova 12 zakonodajne zbirke ZDA. V skladu z zakonom o pravici do finančne zasebnosti (Right to Financial Privacy Act) lahko posameznik v določenih primerih toži Združene države Amerike zaradi pridobitve ali razkritja varovanih finančnih podatkov v nasprotju z zakonom. Vladni dostop do varovanih finančnih podatkov je na splošno prepovedan, razen če vlada vloži zahtevo, ki vključuje zakonit poziv ali nalog za preiskavo, ali glede na omejitve uradno ustno zahtevo ter če je posameznik, o katerem se zahteva dostop do informacij, obveščen o taki zahtevi.

([201]) Členi 1681 do 1681x naslova 15 zakonodajne zbirke ZDA. V skladu z zakonom o poštenem kreditnem poročanju (Fair Credit Reporting Act) lahko posameznik toži katero koli osebo, ki ne izpolnjuje zahtev (zlasti zahteve po zakonitem dovoljenju) glede zbiranja, širjenja in uporabe poročil o kreditni sposobnosti potrošnika, ali v določenih primerih vladno agencijo.

([202]) Sodišče je potrdilo, da je kazenski pregon legitimni cilj politike. Glej združeni zadevi C-293/12 in C-594/12, Digital Rights Ireland in drugi, EU:C:2014:238, točka 42. Glej tudi člen 8(2) EKČP in sodbo Evropskega sodišča za človekove pravice v zadevi Weber in Saravia proti Nemčiji, tožba št. 54934/00, točka 104.

(141) Komisija je sklenila, da so s tem izpolnjeni standardi iz člena 25 Direktive 95/46/ES, ki se razlagajo ob upoštevanju Listine Evropske unije o temeljnih pravicah, kot je Sodišče pojasnilo zlasti v sodbi v zadevi Schrems.

5. UKREPI ORGANOV ZA VARSTVO PODATKOV IN OBVEŠČANJE KOMISIJE

(142) Sodišče je v sodbi v zadevi Schrems pojasnilo, da Komisija nima pristojnosti za omejevanje pooblastil organov za zaščito podatkov, ki izhajajo iz člena 28 Direktive 95/46/ES (vključno s pooblastili za začasno ustavitev prenosa podatkov), če oseba, ki vloži zahtevek na podlagi navedene določbe, izrazi dvom glede združljivosti sklepa Komisije o ustreznosti varstva z varstvom temeljne pravice do zasebnosti in varstva podatkov ([203]).

(143) Za učinkovito spremljanje delovanja zasebnostnega ščita bi morale države članice obveščati Komisija o pomembnih ukrepih organov za varstvo podatkov.

(144) Sodišče je tudi menilo, da morajo države članice in njihovi organi v skladu z drugim pododstavkom člena 25(6) Direktive 95/46/ES sprejeti ukrepe, ki so potrebni za skladnost z ukrepi institucij Unije, saj se za slednje načeloma šteje, da so zakoniti in da ustvarjajo pravne učinke, dokler niso ukinjeni, razveljavljeni v tožbi za razveljavitev ali razglašeni za neveljavne na podlagi predloga za sprejetje predhodne odločbe ali ugovora nezakonitosti. Zato je sklep Komisije o ustreznosti varstva, sprejet na podlagi člena 25(6) Direktive 95/46/ES, zavezujoč za vse organe držav članic, na katere je naslovljen, vključno z neodvisnimi nadzornimi organi teh držav članic ([204]). Če tak organ prejme pritožbo, ki zbuja dvom o skladnosti sklepa Komisije o ustreznosti varstva z varstvom temeljne pravice do zasebnosti in varstva podatkov, ter meni, da so predloženi ugovori dobro utemeljeni, mu mora nacionalna zakonodaja zagotavljati pravno sredstvo za predložitev teh ugovorov nacionalnemu sodišču, ki mora v primeru dvomov prekiniti postopek in Sodišču predložiti predlog za sprejetje predhodne odločbe ([205]).

6. REDNO PREVERJANJE UGOTOVITVE O USTREZNOSTI

(145) Ob upoštevanju dejstva, da se lahko stopnja varstva, ki jo zagotavlja pravni red ZDA, spreminja, bo Komisija po sprejetju tega sklepa redno preverjala, ali so ugotovitve v zvezi z ustreznostjo ravni varstva, ki jo zagotavljajo Združene države Amerike v okviru zasebnostnega ščita EU-ZDA, še vedno dejansko in pravno utemeljene. Tako preverjanje se v vsakem primeru zahteva, kadar Komisija pridobi kakršne koli informacije, ki zbujajo dvom v zvezi s tem ([206]).

(146) Zato bo Komisija stalno spremljala splošni okvir za prenos osebnih podatkov, ustvarjenih v okviru zasebnostnega ščita EU-ZDA, ter upoštevanje zagotovil in zavez, vsebovanih v dokumentih, ki so priloženi temu sklepu, s strani organov ZDA. Za olajšanje tega procesa so se ZDA zavezale, da bodo Komisijo obveščale o pomembnih spremembah prava ZDA, če so pomembne za zasebnostni ščit na področju varstva podatkov ter omejitev in zaščitnih ukrepov, ki se uporabljajo za dostop javnih organov do osebnih podatkov. Poleg tega bo ta sklep predmet skupnega letnega pregleda, ki bo zajemal vse vidike delovanja zasebnostnega ščita EU-ZDA, vključno z uporabo izjem glede nacionalne varnosti in kazenskega pregona pri načelih. Ker lahko na ugotovitev o ustreznosti vplivajo tudi pravne spremembe prava Unije, bo Komisija ocenila raven varstva, ki ga zagotavlja zasebnostni ščit po začetku uporabe Uredbe (EU) 2016/679 o splošnem varstvu podatkov.

(147) Za izvedbo skupnega letnega pregleda iz prilog I, II in VI se bo Komisija sestala z Ministrstvom za trgovino in FTC, po potrebi pa tudi z drugimi ministrstvi in agencijami, vključenimi v izvajanje ureditev zasebnostnega ščita, ter, glede zadev, ki se nanašajo na nacionalno varnost, s predstavniki ODNI, drugimi organi obveščevalne skupnosti in varuhom človekovih pravic. Tega sestanka se bodo lahko udeležili organi za varstvo podatkov iz EU in predstavniki delovne skupine iz člena 29.

([203]) Zadeva Schrems, točka 40 in naslednje, str. 101 do 103.
([204]) Zadeva Schrems, točke 51, 52 in 62.
([205]) Schrems, točka 65.
([206]) Schrems, točka 76.

(148) Komisija bo v okviru skupnega letnega pregleda zahtevala, da Ministrstvo za trgovino zagotovi izčrpne informacije o vseh ustreznih vidikih delovanja zasebnostnega ščita EU-ZDA, vključno z zadevami, ki jih Ministrstvo za trgovino prejme od organov za varstvo podatkov, in rezultati pregledov skladnosti po uradni dolžnosti. Komisija bo zahtevala tudi pojasnila v zvezi s kakršnimi koli vprašanji ali zadevami v zvezi z zasebnostnim ščitom EU-ZDA in njegovim delovanjem, ki izhajajo iz kakršnih koli razpoložljivih informacij, vključno s poročili o preglednosti, dovoljenimi na podlagi zakona ZDA o svobodi, javnimi poročili nacionalnih obveščevalnih organov ZDA, organov za varstvo podatkov in skupin za zasebnost, medijskimi poročili ali kakršnimi koli drugim možnim virom. Poleg tega bi morale države članice za olajšanje naloge Komisije v zvezi s tem obveščati Komisijo o primerih, v katerih ukrepi organov, pristojnih za zagotavljanje skladnosti z načeli v ZDA, ne zagotavljajo skladnosti, in o kakršnih koli znakih, da ukrepi javnih organov ZDA, pristojnih za nacionalno varnost ali preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj, ne zagotavljajo zahtevane ravni varstva.

(149) Komisija bo na podlagi skupnega letnega pregleda pripravila javno poročilo, ki ga bo predložila Evropskemu parlamentu in Svetu.

7. ZADRŽANJE IZVAJANJA SKLEPA O USTREZNOSTI VARSTVA

(150) Če Komisija na podlagi pregledov ali kakršnih koli drugih razpoložljivih informacij ugotovi, da se raven varstva, ki ga zagotavlja zasebnostni ščit, ne more več šteti za v bistvenem enako ravni varstva v Uniji ali da obstajajo jasni znaki, da dejanska skladnost z načeli v ZDA morda ni več zagotovljena ali da ukrepi javnih organov ZDA, pristojnih za nacionalno varnost ali preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj, ne zagotavljajo zahtevane ravni varstva, o tem obvesti Ministrstvo za trgovino in zahteva, da se sprejmejo ustrezni ukrepi za hitro odpravo morebitne neskladnosti z načeli v določenem, razumnem roku. Če organi ZDA po izteku določenega roka ne dokažejo zadovoljivo, da zasebnostni ščit EU-ZDA še naprej zagotavlja dejansko skladnost in ustrezno raven varstva, Komisija začne postopek, ki vodi do delnega ali popolnega zadržanja izvajanja ali razveljavitve tega sklepa ([207]). Druga možnost je, da Komisija predlaga spremembo tega sklepa, na primer z omejitvijo obsega ugotovitve o ustreznosti varstva samo na prenose podatkov, za katere veljajo posebni pogoji.

(151) Komisija bo začela postopek za zadržanje izvajanja ali razveljavitev zlasti v primeru:

(a) znakov, da organi ZDA ne izpolnjujejo zagotovil in zavez iz dokumentov, priloženih temu sklepu, vključno v zvezi s pogoji in omejitvami za dostop javnih organov ZDA za kazenski pregon, nacionalno varnost in druge namene javnega interesa do osebnih podatkov, ki se prenašajo v okviru zasebnostnega ščita;

(b) neučinkovitega obravnavanja pritožb posameznikov iz EU, na katere se nanašajo osebni podatki, Komisija pa bo v zvezi s tem upoštevala okoliščine, ki vplivajo na možnost uveljavljanja pravic posameznikov, na katere se nanašajo osebni podatki, vključno s prostovoljno zavezo samocertificiranih podjetij iz ZDA, da bodo sodelovala z organi za varstvo podatkov in upoštevala njihove nasvete, ali

(c) nepravočasnih in neustreznih odgovorov varuha človekovih pravic na področju zasebnostnega ščita na zahtevke posameznikov, na katere se nanašajo osebni podatki.

(152) Komisija bo razmislila tudi o začetku postopka za spremembo, odložitev izvajanja ali razveljavitev tega sklepa, če Ministrstvo za trgovino ali druga ministrstva ali agencije, vključeni v izvajanje zasebnostnega ščita, ali, za zadeve v zvezi z nacionalno varnostjo, predstavniki obveščevalne skupnosti ZDA ali varuh človekovih pravic v okviru skupnega letnega pregleda delovanja zasebnostnega ščita EU-ZDA ali kako drugače ne bodo zagotovili informacij

([207]) Kar zadeva datum začetka uporabe splošne uredbe o varstvu podatkov, bo Komisija v ustrezno utemeljenih nujnih primerih uporabila svoja pooblastila za sprejetje izvedbenega akta o zadržanju izvajanja tega sklepa, ki začne veljati takoj, brez njegove predhodne predložitve ustreznemu komitološkemu odboru, in velja največ šest mesecev.

ali pojasnil, potrebnih za oceno skladnosti z načeli, učinkovitost postopkov obravnavanja pritožb ali kakršno koli znižanje zahtevane ravni varstva zaradi ukrepov nacionalnih obveščevalnih organov ZDA, zlasti kot posledica zbiranja in/ali dostopanja do osebnih podatkov, ki ni omejeno na tisto, kar je nujno potrebno in sorazmerno. V zvezi s tem bo Komisija upoštevala obseg ustreznih informacij, ki se lahko pridobijo iz drugih virov, vključno s poročili samocertificiranih podjetij iz ZDA, kot je dovoljeno na podlagi zakona ZDA o svobodi.

(153) Delovna skupina za varstvo posameznikov glede obdelave osebnih podatkov, ustanovljena v skladu s členom 29 Direktive 95/46/ES, je izdala mnenje o ravni varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA ([208]), ki se je upoštevalo pri pripravi tega sklepa.

(154) Evropski parlament je sprejel resolucijo o čezatlantskem pretoku podatkov ([209]).

(155) Ukrepi, določeni s tem sklepom, so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 31(1) Direktive 95/46/ES –

SPREJELA NASLEDNJI SKLEP:

Člen 1

1. Za namene člena 25(2) Direktive 95/46/ES ZDA zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije organizacijam v ZDA.

2. Zasebnostni ščit EU-ZDA sestavljajo načela, ki jih je 7. julija 2016 izdalo Ministrstvo za trgovino ZDA, kakor so navedena v Prilogi II, ter uradna zagotovila in zaveze iz dokumentov, navedenih v prilogah I in III–VII.

3. Za namene odstavka 1 se osebni podatki prenašajo v okviru zasebnostnega ščita EU-ZDA, kadar se prenašajo iz Unije organizacijam v ZDA, ki so vključene na „seznam zasebnostnega ščita“, ki ga vodi in objavlja Ministrstvo za trgovino ZDA, v skladu s členoma I in III načel iz Priloge II.

Člen 2

Ta sklep ne vpliva na uporabo določb Direktive 95/46/ES, razen člena 25(1), ki se nanašajo na obdelavo osebnih podatkov v državah članicah, zlasti ne na določbe člena 4 Direktive.

Člen 3

Kadar pristojni organi v državah članicah izvajajo svoja pooblastila v skladu s členom 28(3) Direktive 95/46/ES za zadržanje izvajanja ali dokončno prepoved pritoka podatkov v organizacijo v ZDA, ki je vključena na seznam zasebnostnega ščita v skladu s členoma I in III načel iz Priloge II, da bi zaščitili posameznike pri obdelavi njihovih osebnih podatkov, zadevna država članica o tem nemudoma obvesti Komisijo.

Člen 4

1. Komisija bo stalno spremljala delovanje zasebnostnega ščita EU-ZDA, da bi ocenila, ali ZDA še naprej zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru ščita prenašajo iz Unije v ZDA.

([208]) Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (Mnenje 01/2016 o sklepu o ustreznosti osnutka zasebnostnega ščita EU-ZDA), sprejeto 13. aprila 2016.
([209]) Resolucija Evropskega parlamenta z dne 26. maja 2016 o čezatlantskem pretoku podatkov (2016/2727(RSP)).

2. Države članice in Komisija se medsebojno obveščajo o primerih, v katerih se zdi, da vladni organi v ZDA z zakonskimi pooblastili za uveljavljanje skladnosti z načeli iz Priloge II ne zagotavljajo učinkovitih mehanizmov odkrivanja in nadzora, ki bi v praksi omogočali ugotavljanje in sankcioniranje kršitev načel.

3. Države članice in Komisija se medsebojno obveščajo o kakršnih koli znakih, da posegi javnih organov ZDA, pristojnih za nacionalno varnost, kazenski pregon ali druge javne interese, v pravico posameznikov do varstva osebnih podatkov presegajo tisto, kar je nujno potrebno, in/ali da ni učinkovitega pravnega varstva pred takimi posegi.

4. Komisija bo v enem letu od uradnega obvestila o tem sklepu državam članicam in nato enkrat letno proučila ugotovitev iz člena 1(1) na podlagi vseh razpoložljivih informacij, vključno z informacijami, prejetimi v okviru skupnega letnega pregleda iz prilog I in II–VI.

5. Komisija bo o kakršnih koli zadevnih ugotovitvah poročala odboru, ustanovljenemu v skladu s členom 31 Direktive 95/46/ES.

6. Komisija bo predložila osnutek ukrepov, v skladu s postopkom iz člena 31(2) Direktive 95/46/ES, za zadržanje izvajanja, spremembo, razveljavitev ali omejitev področja uporabe tega sklepa,med drugim kadar obstajajo znaki:

— da javni organi ZDA ne izpolnjujejo zagotovil in zavez iz dokumentov, priloženih temu sklepu, tudi v zvezi s pogoji in omejitvami za dostop javnih organov ZDA za kazenski pregon, nacionalno varnost in druge namene javnega interesa do osebnih podatkov, ki se prenašajo v okviru zasebnostnega ščita EU-ZDA,

— sistematično neučinkovitega obravnavanja pritožb posameznikov iz EU, na katere se nanašajo osebni podatki, ali

— sistematičnega nezagotavljanja pravočasnih in ustreznih odgovorov varuha človekovih pravic na področju zasebnostnega ščita na zahtevke posameznikov iz EU, na katere se nanašajo osebni podatki, v skladu s členom 4(e) Priloge III.

Komisija bo tak osnutek ukrepov predložila tudi, če zaradi nezadostnega sodelovanja organov, vključenih v zagotavljanje delovanja zasebnostnega ščita EU-ZDA v Združenih državah, ne bo mogla ugotoviti, ali obstaja vpliv na ugotovitev iz člena 1(1).

Člen 5

Države članice sprejmejo vse potrebne ukrepe za uskladitev s tem sklepom.

Člen 6

Ta sklep je naslovljen na države članice.

V Bruslju, 12. julija 2016

Za Komisijo

Věra JOUROVÁ

Članica Komisije

PRILOGA I

Pismo ameriške ministrice za trgovino Penny Pritzker

7. julij 2016

Věra Jourová
Komisarka za pravosodje, potrošnike in enakost spolov
Evropska komisija
Rue de la Loi/Wetstraat 200
1049 Bruselj
Belgija

Spoštovana komisarka Jourová,

veseli me, da vam lahko v imenu Združenih držav pošljem sveženj gradiva v zvezi z zasebnostnim ščitom EU-ZDA, ki je plod dvoletnih produktivnih razprav med najinima ekipama. Ta sveženj in drugo gradivo, ki je na razpolago Komisiji iz javnih virov, zagotavljata trdno podlago za novo ugotovitev Evropske komisije o ustreznosti ([1]).

Ponosna sva lahko na izboljšave okvira. Zasebnostni ščit temelji na načelih, ki imajo podporo v trdnem konsenzu na obeh straneh Atlantika, delovanje teh načel pa smo še okrepili. S skupnim delom imamo resnično priložnost izboljšati zaščito zasebnosti po vsem svetu.

Sveženj o zasebnostnem ščitu vsebuje načela zasebnostnega ščita in pismo, priloženo kot Priloga 1, Uprave za mednarodno trgovino (ITA) ameriškega Ministrstva za trgovino, pristojne za program, v katerem so opisane zaveze našega ministrstva glede zagotavljanja učinkovitega delovanja zasebnostnega ščita. Sveženj vključuje tudi Prilogo 2, ki vsebuje druge zaveze Ministrstva za trgovino v zvezi z novim arbitražnim modelom, ki je na razpolago v okviru zasebnostnega ščita.

Svojim zaposlenim sem naročila, naj namenijo vsa potrebna sredstva za hitro in polno izvajanje okvira zasebnostnega ščita ter za pravočasno izpolnitev zavez iz Prilog 1 in 2.

Sveženj o zasebnostnem ščitu vključuje tudi druge dokumente agencij Združenih držav, in sicer:

— pismo Zvezne komisije za trgovino (Federal Trade Commission, v nadaljnjem besedilu: FTC), ki opisuje njeno izvrševanje zasebnostnega ščita;

— pismo Ministrstva za promet, ki opisuje njegovo izvrševanje zasebnostnega ščita;

— pismi urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence, v nadaljnjem besedilu: ODNI) v zvezi z zaščitnimi ukrepi in omejitvami, ki veljajo za ameriške nacionalne varnostne organe;

— pismo Ministrstva za zunanje zadeve ZDA s priloženim memorandumom, ki opisuje zavezo tega ministrstva, da uvede nov institut varuha človekovih pravic na področju zasebnostnega ščita za predložitev poizvedb v zvezi z obveščevalnimi dejavnostmi ZDA pri zaznavanju signalov (v nadaljnjem besedilu: SIGINT) in

— pismo, ki ga je pripravilo Ministrstvo za pravosodje ZDA v zvezi z zaščitnimi ukrepi in omejitvami dostopa vlade ZDA za potrebe kazenskega pregona in javnega interesa.

Prepričani ste lahko, da Združene države te zaveze jemljejo resno.

([1]) Če se bo sklep Komisije o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, uporabljal za Islandijo, Lihtenštajn in Norveško, bo sveženj o zasebnostnem ščitu zajemal tako Evropsko unijo kot tudi te tri države.

Popoln sveženj o zasebnostnem ščitu bo poslan v objavo *Zveznemu registru* v 30 dneh po končnem sprejetju ugotovitve o ustreznosti.

Veselimo se sodelovanja z vami pri uvajanju zasebnostnega ščita in pri skupnem delu na naslednji fazi tega procesa.

S spoštovanjem.

Penny Pritzker

Priloga 1

Pismo vršilca dolžnosti namestnika ministra za mednarodno trgovino Kena Hyatta

Věra Jourová
Komisarka za pravosodje, potrošnike in enakost spolov
Evropska komisija
Rue de la Loi/Wetstraat 200
1049 Bruselj
Belgija

Spoštovana komisarka Jourová,

veseli me, da lahko v imenu Uprave za mednarodno trgovino opišem izboljšano varstvo osebnih podatkov, ki ga zagotavlja okvir zasebnostnega ščita EU-ZDA (v nadaljnjem besedilu: zasebnostni ščit ali okvir), in zaveze, ki jih je Ministrstvo za trgovino ZDA (v nadaljnjem besedilu:Ministrstvo) sprejelo za zagotavljanje učinkovitega delovanja zasebnostnega ščita. Dokončanje tega zgodovinskega dogovora je velik dosežek za zasebnost in podjetja na obeh straneh Atlantskega oceana. Posameznikom v EU daje zaupanje, da bodo njihovi podatki zaščiteni in da bodo imeli na voljo pravna sredstva za obravnavo morebitnih vprašanj. Daje zagotovilo, ki bo pomagalo spodbuditi rast čezatlantskega gospodarstva, saj bo lahko na tisoče evropskih in ameriških podjetij še naprej vlagalo in poslovalo prek naših meja. Zasebnostni ščit je plod več kot dvoletnega trdega dela in sodelovanja z vami, našimi kolegi iz Evropske komisije (v nadaljnjem besedilu: Komisija). Veselimo se nadaljnjega sodelovanja s Komisijo z namenom zagotavljanja, da zasebnostni ščit deluje, kakor je predvideno.

S Komisijo smo sodelovali pri oblikovanju zasebnostnega ščita, da bi organizacijam, ustanovljenim v Združenih državah, omogočili izpolnjevanje zahtev glede ustreznosti varstva podatkov po zakonodaji EU. Novi okvir bo prinesel veliko pomembnih ugodnosti posameznikom in podjetjem. V prvi vrsti zagotavlja pomembne elemente varstva zasebnosti podatkov posameznikov iz EU. Od sodelujočih ameriških organizacij zahteva, da oblikujejo skladno politiko zasebnosti, se javno zavežejo k spoštovanju načel zasebnostnega ščita, tako da zaveza postane izvršljiva po zakonodaji ZDA, da vsako leto znova certificirajo svoje izpolnjevanje načel pri Ministrstvu, posameznikom iz EU zagotovijo brezplačno neodvisno reševanje sporov in da so pod pristojnostjo Zvezne komisije za trgovino (FTC), Ministrstva za promet ZDA (DOT) ali drugih organov pregona. Drugič, zasebnostni ščit bo tisočim podjetjem v Združenih državah in podružnicam evropskih podjetij v Združenih državah omogočil, da prejmejo osebne podatke iz Evropske unije in tako pospešijo pretok podatkov v podporo čezatlantski trgovini. Čezatlantski gospodarski odnosi so že zdaj najobsežnejši na svetu, saj predstavljajo polovico svetovne gospodarske proizvodnje in skoraj en bilijon ameriških dolarjev v trgovini blaga in storitev, pri čemer zagotavljajo milijone delovnih mest na obeh straneh Atlantskega oceana. Podjetja, ki se zanašajo na čezatlantski pretok podatkov, prihajajo iz vseh industrijskih sektorjev in vključujejo tako največja podjetja s seznama Fortune 500 kot tudi mala in srednja podjetja (MSP). Čezatlantski pretok podatkov ameriškim organizacijam omogoča, da obdelajo podatke, potrebne za zagotavljanje blaga, storitev in zaposlitvenih možnosti posameznikom iz Evrope. Zasebnostni ščit podpira skupna načela zasebnosti in premaguje razlike v pravnih pristopih, obenem pa spodbuja trgovino in gospodarske cilje Evrope in Združenih držav.

Medtem ko bo odločitev podjetja za samocertificiranje po tem novem okviru prostovoljna, pa bo za podjetja, ki se javno zavežejo k spoštovanju zasebnostnega ščita, takšna zaveza izvršljiva po zakonodaji ZDA s strani Zvezne komisije za trgovino ali Ministrstva za promet, odvisno od tega, kateri organ ima pristojnost nad organizacijo v zasebnostnem ščitu.

Izboljšave v okviru načel zasebnostnega ščita

Ta zasebnostni ščit krepi varstvo zasebnosti, s tem ko:

— v načelu obvestila zahteva, da se posameznikom zagotovijo dodatne informacije, vključno z izjavo o sodelovanju organizacije v zasebnostnem ščitu, izjavo o pravici posameznika do dostopa do osebnih podatkov in opredelitvijo ustreznega neodvisnega organa za reševanje sporov;

— krepi varstvo osebnih podatkov, ki se prenesejo od organizacije v zasebnostnem ščitu tretjemu upravljavcu, s tem da od strank zahteva, da sklenejo pogodbo, ki dovoljuje obdelavo takih podatkov le za omejene in natančno določene namene v skladu s soglasjem, ki ga poda posameznik, ter določa, da bo prejemnik zagotovil enako raven zaščite kot načela;

— krepi varstvo osebnih podatkov, ki se prenesejo iz organizacije v zasebnostnem ščitu posredniku tretje stranke, s tem ko med drugim zahteva, da organizacija v zasebnostnem ščitu: sprejme razumne in ustrezne ukrepe za zagotovitev, da posrednik dejansko obdela osebne prenesene informacije na način, ki je skladen z obveznostmi organizacije v okviru načel; po obvestilu sprejme razumne in ustrezne ukrepe za ustavitev in odpravo nepooblaščene obdelave ter na zahtevo Ministrstvu zagotovi povzetek ali reprezentativni izvod ustreznih določb o zasebnosti iz svoje pogodbe s tem posrednikom;

— določa, da je organizacija v zasebnostnem ščitu odgovorna za obdelavo osebnih informacij, ki jih prejme v okviru zasebnostnega ščita in nato prenese tretji osebi, ki deluje v vlogi posrednika v njenem imenu, ter da ostane odgovorna v skladu z načeli, če njen posrednik obdeluje take osebne informacije na način, ki ni skladen z načeli, razen če organizacija dokaže, da ni odgovorna za dogodek, ki je povzročil škodo;

— pojasnjuje, da morajo organizacije v zasebnostnem ščitu osebne informacije omejiti na informacije, ki so pomembne za namene obdelave;

— od organizacije, ki bi izstopila iz zasebnostnega ščita in bi se odločila obdržati takšne podatke,zahteva, da vsako leto pri Ministrstvu certificira svojo zavezo k uporabi načel pri informacijah, ki jih je prejela med svojim sodelovanjem v zasebnostnem ščitu;

— posamezniku zagotavlja brezplačne neodvisne pritožbene mehanizme;

— od organizacij in njihovih izbranih neodvisnih pritožbenih mehanizmov zahteva, da se pravočasno odzivajo na poizvedbe in zahteve Ministrstva po informacijah v zvezi z zasebnostnim ščitom;

— od organizacij zahteva, da se hitro odzivajo na pritožbe v zvezi z izpolnjevanjem načel, ki so jih organi držav članic EU predložili prek Ministrstva in

— od organizacije v zasebnostnem ščitu, za katero bi bila izdana odločba Zvezne komisije za trgovino ali sodišča zaradi neizpolnjevanja, zahteva, da objavi vse ustrezne dele poročila o skladnosti ali oceni v zvezi z zasebnostnim ščitom, ki ga je predložila Zvezni komisiji za trgovino.

Upravljanje in nadzor programa zasebnostnega ščita s strani Ministrstva za trgovino

Ministrstvo znova ponavlja svojo zavezo, da bo vzdrževalo in javnosti zagotovilo verodostojen seznam organizacij ZDA, ki so se samocertificirale pri Ministrstvu in razglasile svojo zavezo k spoštovanju načel („seznam zasebnostnega ščita“). Ministrstvo bo posodabljalo seznam zasebnostnega ščita, tako da bo odstranilo organizacije, kadar te prostovoljno izstopijo, ne uspejo zaključiti letnega samocertificiranja v skladu s postopki Ministrstva ali kadar je ugotovljeno, da vztrajno ne izpolnjujejo načel. Ministrstvo bo prav tako vzdrževalo in javnosti zagotovilo verodostojno evidenco organizacij ZDA, ki so se v preteklosti samocertificirale pri Ministrstvu, a so bile odstranjene s seznama zasebnostnega ščita, vključno s tistimi, ki so bile odstranjene zaradi vztrajnega neizpolnjevanja načel. Ministrstvo bo opredelilo razlog za odstranitev vsake posamezne organizacije.

Poleg tega se Ministrstvo zavezuje, da bo okrepilo upravljanje in nadzor zasebnostnega ščita. Natančneje bo Ministrstvo:

Zagotovilo dodatne informacije na spletni strani zasebnostnega ščita

— vzdrževalo seznam zasebnostnega ščita in evidenco organizacij, ki so predhodno samocertificirale zavezanost k načelom, toda niso več upravičene do ugodnosti zasebnostnega ščita;

— vključilo vidno pojasnilo, da vse organizacije, odstranjene s seznama varnostnega ščita, niso več upravičene do ugodnosti zasebnostnega ščita, toda morajo navkljub temu uporabljati načela pri osebnih informacijah, ki so jih prejele med sodelovanjem v zasebnostnem ščitu, dokler hranijo takšne informacije; in

— zagotovilo povezavo do seznama zadev Zvezne komisije za trgovino, povezanih z zasebnostnim ščitom, ki se vzdržuje na spletni strani FTC.

Preverilo zahteve za samocertificiranje

— pred dokončanjem samocertificiranja organizacije (ali vsakoletnega ponovnega certificiranja) in uvrstitvijo organizacije na seznam zasebnostnega ščita, bo preverilo, ali je organizacija:

  — zagotovila potrebne podatke za stik z organizacijo;

  — opisala dejavnosti organizacije v zvezi z osebnimi podatki, prejetimi iz EU;

  — navedla, kakšne osebne informacije zajema njena samocertifikacija;

  — če ima organizacija javno spletno stran, zagotovila spletni naslov, kjer je na voljo politika zasebnosti, in razpoložljivost slednje na navedeni spletni strani ali, v kolikor organizacija nima javne spletne strani, navedla, kje je javnosti na voljo politika zasebnosti;

  — vključila v svojo ustrezno politiko zasebnosti izjavo, da se zavezuje k spoštovanju načel, in če je politika zasebnosti na voljo na spletu, povezavo na spletno stran zasebnostnega ščita v okviru Ministrstva;

  — opredelila posebno zakonsko telo, ki je pristojno za obravnavanje vseh zahtevkov proti organizaciji v zvezi z morebitnim nepoštenim ali goljufivim ravnanjem in kršitvami zakonov ali predpisov, ki urejajo zasebnost (in ki je navedeno v načelih ali v prihodnji prilogi k načelom);

  — če se organizacija odloči izpolniti zahteve iz točk (a)(i) in (a)(iii) načela pritožbenega mehanizma, uveljavljanja in odgovornosti, tako da se zaveže k sodelovanju z ustreznimi organi EU za zaščito podatkov, navedla svojo namero po sodelovanju z organi za zaščito podatkov v preiskovanju in reševanju pritožb, vloženih v okviru zasebnostnega ščita, predvsem z namenom odgovarjanja na njihove poizvedbe, kadar posamezniki iz EU, na katere se nanašajo osebni podatki, vložijo svoje pritožbe neposredno svojemu nacionalnemu organu za zaščito podatkov;

  — navedla kakršen koli program zasebnosti, v katerega je včlanjena organizacija;

  — opredelila način za preverjanje zagotavljanja izpolnjevanja načel (npr. notranji, zunanji);

  — opredelila neodvisni pritožbeni mehanizem, ki je na voljo za preiskovanje in reševanje pritožb, v svoji predložitvi samocertifikacije in politiki zasebnosti;

  — vključila v svojo ustrezno politiko zasebnosti, če je ta na voljo na spletu, povezavo do spletne strani ali obrazca za predložitev pritožbe v okviru neodvisnega pritožbenega mehanizma, ki je na voljo za preiskave nerešenih pritožb; in

  — če je organizacija navedla, da namerava prejemati informacije o človeških virih, prenesene iz EU za uporabo v okviru zaposlitvenega razmerja, se zavezala k sodelovanju in upoštevanju organov za zaščito podatkov pri reševanju pritožb v zvezi s svojimi dejavnostmi, povezanimi s takšnimi podatki, predložila Ministrstvu izvod svoje politike zasebnosti v zvezi s človeškimi viri in navedla, kje si lahko zadevni zaposleni ogledajo politiko zasebnosti;

— sodeluje z neodvisnimi pritožbenimi mehanizmi, da bi preverilo, ali so se organizacije dejansko registrirale pri ustreznem mehanizmu, navedenem v predložitvah samocertifikacije, kjer je potrebna takšna registracija.

Okrepilo prizadevanja za nadaljnje spremljanje organizacij, ki so bile odstranjene s seznama zasebnostnega ščita

— obvestilo organizacije, ki so bile odstranjene s seznama zasebnostnega ščita zaradi „vztrajnega neizpolnjevanja načel“, da nimajo pravice hraniti informacij, zbranih v okviru zasebnostnega ščita; in

— poslalo vprašalnike organizacijam, ki jim poteče samocertifikacija ali ki so prostovoljno izstopile iz zasebnostnega ščita, da bi preverilo, ali se bo organizacija vrnila, izbrisala ali še naprej uporabljala načela pri osebnih informacijah, ki jih je prejela med sodelovanjem v zasebnostnem ščitu, ter – če bo hranila osebne informacije – preverilo, kdo v organizaciji bo deloval kot stalni stik za vprašanja, povezana z zasebnostnim ščitom.

Poiskalo in obravnavalo lažne navedbe o sodelovanju

— pregledalo politike zasebnosti organizacij, ki so prej sodelovale v programu zasebnostnega ščita, vendar so bile odstranjene s seznama zasebnostnega ščita, da bi odkrilo morebitne lažne navedbe glede sodelovanja v zasebnostnem ščitu;

— se sproti, kadar organizacija: (a) izstopi iz sodelovanja v zasebnostnem ščitu, (b) ne uspe ponovno certificirati zavezanosti k načelom ali (c) je odstranjena kot udeleženec v zasebnostnem ščitu predvsem zaradi „vztrajnega neizpolnjevanja načel", zaveže, da bo po uradni dolžnosti preverilo, ali je organizacija iz ustrezne objavljene politike zasebnosti odstranila vse sklice na zasebnostni ščit, ki nakazujejo, da organizacija še naprej dejavno sodeluje v zasebnostnem ščitu in je upravičena do njegovih ugodnosti. Kadar Ministrstvo ugotovi, da takšni sklici niso bili odstranjeni, bo organizacijo opozorilo, da bo po potrebi zadeve predalo ustrezni agenciji za morebitno uvedbo pregona, če se bo ta še naprej sklicevala na certifikacijo v okviru zasebnostnega ščita. Če organizacija ne odstrani sklicev in ne samocertificira izpolnjevanja svojih obveznosti v okviru zasebnostnega ščita, bo Ministrstvo po uradni dolžnosti predalo zadevo Zvezni komisiji za trgovino, Ministrstvu za promet ali drugemu organu pregona ali v ustreznih primerih ukrepalo, da bi uveljavilo certifikacijsko oznako zasebnostnega ščita;

— storilo vse, da bi odkrilo lažne navedbe glede sodelovanja v zasebnostnem ščitu in neprimerne uporabe certifikacijske oznake zasebnostnega ščita, tudi z iskanjem strani po internetu, kjer so prikazane slike certifikacijske oznake zasebnostnega ščita in sklici na zasebnostni ščit v politikah zasebnosti organizacij;

— sproti obravnavalo morebitna vprašanja, ki se zastavijo med našim spremljanjem lažnih navedb o sodelovanju in zlorabe certifikacijske oznake po uradni dolžnosti, in tudi opozarjalo organizacije, ki lažno navajajo svoje sodelovanje v programu zasebnostnega ščita, kakor je opisano zgoraj;

— sprejelo druge ustrezne popravne ukrepe, vključno z morebitnimi zakonskimi pritožbami, ki jih ima Ministrstvo na voljo, in predložitvijo zadev Zvezni komisiji za trgovino, Ministrstvu za promet ali drugemu ustreznemu organu pregona; in

— sproti pregledovalo in obravnavalo pritožbe o lažnih navedbah sodelovanja, ki jih prejme.

Ministrstvo bo pregledovalo politike zasebnosti organizacij, da bi učinkoviteje ugotavljalo in obravnavalo lažne navedbe sodelovanja v zasebnostnem ščitu. Ministrstvo bo zlasti pregledalo politike zasebnosti organizacij, ki jim je potekla samocertifikacija, ker niso uspele ponovno certificirati zavezanosti k načelom. Ministrstvo bo opravilo to vrsto pregleda z namenom preverjanja, ali so takšne organizacije odstranile vse sklice, ki nakazujejo, da organizacija še naprej dejavno sodeluje v zasebnostnem ščitu, iz ustrezne objavljene politike zasebnosti. S takšnimi pregledi bomo odkrili organizacije, ki niso odstranile takšnih sklicev, in jim poslali pismo urada glavnega pravnika Ministrstva z opozorilom o morebitni uvedbi pregona, če sklici ne bodo odstranjeni. Ministrstvo bo sprejelo nadaljnje ukrepe, s katerimi bo zagotovilo, da organizacije odstranijo neustrezne sklice ali pa ponovno certificirajo zavezanost k načelom. Poleg tega si bo Ministrstvo prizadevalo odkriti lažne navedbe o sodelovanju v zasebnostnem ščitu organizacij, ki nikoli niso sodelovale v programu zasebnostnega ščita, in bo v zvezi s takšnimi organizacijami sprejelo podobne popravne ukrepe.

Po uradi dolžnosti opravljalo redne preglede skladnosti z načeli in ocene programa

— redno spremljalo učinkovito izpolnjevanje načel, vključno s pošiljanjem podrobnih vprašalnikov sodelujočim organizacijam, da bi odkrilo težave, ki lahko zahtevajo nadaljnje ukrepe. Takšni pregledi skladnosti z načeli se zlasti izvedejo, kadar: (a) Ministrstvo prejme posebno resno pritožbo o izpolnjevanju načel organizacije, (b) organizacija ne odgovori zadovoljivo na poizvedbe Ministrstva po informacijah v zvezi z zasebnostnim ščitom ali (c) obstajajo verodostojni dokazi, da organizacija ne izpolnjuje svojih zavez v okviru zasebnostnega ščita. Ministrstvo se o takšnih pregledih skladnosti z načeli po potrebi posvetuje z ustreznimi organi za zaščito podatkov in

— redno ocenjuje upravljanje in nadzor programa zasebnostnega ščita, da bi zagotovilo ustrezno spremljanje pri obravnavanju novih vprašanj, ko se ta pojavijo.

Ministrstvo je povečalo sredstva, ki jih bo namenilo upravljanju in nadzoru programa zasebnostnega ščita in tudi podvojilo število zaposlenih, ki so odgovorni za upravljanje in nadzor programa. Še naprej bomo za takšna prizadevanja namenjali ustrezna sredstva in tako zagotovili učinkovito spremljanje in upravljanje programa.

Prilagodilo spletno stran zasebnostnega ščita ciljnim skupinam

Ministrstvo bo prilagodilo spletno stran zasebnostnega ščita trem ciljnim skupinam: posameznikom iz EU, podjetjem iz EU in podjetjem iz ZDA. Vključitev gradiva, namenjenega neposredno posameznikom in podjetjem iz EU, bo na več načinov omogočila preglednost. Posameznikom iz EU bo pojasnila: (1) pravice, zagotovljene posameznikom iz EU v okviru zasebnostnega ščita; (2) pritožbene mehanizme, ki so na voljo posameznikom iz EU, kadar menijo, da je organizacija kršila svojo zavezo k izpolnjevanju načel; in (3) kako poiskati informacije v zvezi s samocertifikacijo organizacije v okviru zasebnostnega ščita. Podjetjem iz EU bo omogočila preverjanje: (1) ali je organizacija upravičena do ugodnosti zasebnostnega ščita; (2) vrste informacij, ki jih zajema samocertifikacija organizacije v okviru zasebnostnega ščita; (3) politike zasebnosti, ki se nanaša na zajete informacije; in (4) metode, ki jo uporablja organizacija za preverjanje zavezanosti k načelom.

Povečalo sodelovanje z organi za zaščito podatkov

Za krepitev priložnosti za sodelovanje z organi za zaščito podatkov bo Ministrstvo določilo osebo za stike na Ministrstvu, ki bo imela vlogo uradnika za zvezo z organi za zaščito podatkov. V primerih, ko organ za zaščito podatkov meni, da organizacija ne izpolnjuje načel, tudi po pritožbi posameznika iz EU, se lahko organ za zaščito podatkov obrne na ustrezno osebo za stike na Ministrstvu in zahteva nadaljnji pregled organizacije. Ta oseba za stike bo prejela tudi predložitve v zvezi z organizacijami, ki lažno navajajo sodelovanje v zasebnostnem ščitu, čeprav niso nikoli samocertificirale zavezanosti k načelom. Oseba za stike bo organom za zaščito podatkov pomagala pri iskanju informacij v zvezi s samocertificiranjem posamezne organizacije ali njenem prejšnjem sodelovanju v programu ter bo odgovarjala na poizvedbe organa za zaščito podatkov v zvezi z izvajanjem posebnih zahtev zasebnostnega ščita. Drugič, Ministrstvo bo organom za zaščito podatkov zagotovilo gradivo v zvezi z zasebnostnim ščitom, ki ga vključijo na lastne spletne strani in s tem povečajo preglednost za posameznike in podjetja iz EU. Večja ozaveščenost v zvezi z zasebnostnim ščitom ter pravicami in odgovornostmi, ki jih prinaša, bi morala olajšati odkrivanje vprašanj, ko se ta pojavijo, tako da jih je mogoče ustrezno obravnavati.

Olajšalo reševanje pritožb o neizpolnjevanju načel

Ministrstvo bo prek osebe za stike prejemalo pritožbe, ki jih na Ministrstvo naslovi organ za zaščito podatkov, da organizacija v zasebnostnem ščitu ne izpolnjuje načel. Ministrstvo si bo kar najbolj prizadevalo olajšati reševanje pritožbe z organizacijo v zasebnostnem ščitu. Ministrstvo bo v 90 dneh po prejemu pritožbe obvestilo organ za zaščito podatkov. Za lažjo predložitev takšnih pritožb bo Ministrstvo izdelalo standardni obrazec za organe za zaščito podatkov, ki ga bodo predložili osebi za stike na Ministrstvu. Oseba za stike bo spremljala vse predložitve organov za zaščito podatkov, ki jih prejme Ministrstvo, slednje pa bo v letnem pregledu, opisanem spodaj, podalo poročilo z zbirno analizo pritožb, ki jih prejme vsako leto.

Sprejelo arbitražne postopke in izbralo arbitre po posvetovanju s Komisijo

Ministrstvo bo izpolnilo svoje zaveze iz Priloge I in objavilo postopke po sklenitvi dogovora.

Skupni mehanizem za pregled delovanja zasebnostnega ščita

Ministrstvo za trgovino, Zvezna komisija za trgovino in druge agencije, kakor primerno, bodo sklicale letne sestanke s Komisijo, zainteresiranimi organi za zaščito podatkov in ustreznimi predstavniki delovne skupine iz člena 29, kjer bo Ministrstvo zagotovilo najnovejše podatke o programu zasebnostnega ščita. Na letnih sestankih bodo obravnavana aktualna vprašanja v zvezi z delovanjem, izvajanjem, nadzorom in uveljavljanjem zasebnostnega ščita, vključno s predložitvami, ki jih Ministrstvo prejme od organov za zaščito podatkov, rezultati pregledov skladnosti z načeli, ki jih izvede po uradni dolžnosti, lahko tudi pomembne spremembe zakona. Prvi letni pregled in nadaljnji pregledi po potrebi bodo vključevali dialog o drugih vprašanjih, na primer na področju avtomatiziranega odločanja, vključno z vidiki, ki se nanašajo na podobnosti in razlike v pristopih v EU in ZDA.

Posodobitev zakonodaje

Ministrstvo si bo po najboljših močeh prizadevalo obveščati Komisijo o vsebinskem razvoju prava v Združenih državah, kolikor bo ta upošteven za zasebnostni ščit na področju varstva zasebnosti podatkov, in zaščitnih ukrepih, ki se uporabljajo za omejitev dostopa do osebnih podatkov s strani organov ZDA in njihovo naknadno uporabo.

Izjema v zvezi z nacionalno varnostjo

Glede na omejitve zavezanosti k načelom zasebnostnega ščita za potrebe nacionalne varnosti je glavni pravnik urada direktorja nacionalne obveščevalne službe Robert Litt poslal pismi Justinu Antonipillaiju in Tedu Deanu iz Ministrstva za trgovino, ki sta bili nato posredovani še vam. Ti pismi med drugim podrobno obravnavata politike, zaščitne ukrepe in omejitve, ki veljajo za obveščevalno dejavnost SIGINT, kakor jo izvajajo ZDA. Poleg tega pismi opisujeta preglednost, ki jo zagotavlja obveščevalna skupnost v teh zadevah. V času, ko Komisija ocenjuje okvir zasebnostnega ščita, informacije v teh dveh pismih dajejo zagotovilo za ugotovitev, da bo zasebnostni ščit ustrezno deloval v skladu z načeli, navedenimi v njiju. Razumemo, da boste morda v prihodnosti uporabili informacije, ki jih je obveščevalna skupnost javno objavila, z drugimi informacijami, ki bodo skupaj tvorile podlago za letni pregled okvira zasebnostnega ščita.

Na podlagi načel zasebnostnega ščita in spremljajočih pisem in gradiva, vključno z zavezami Ministrstva v zvezi z upravljanjem in nadzorom okvira zasebnostnega ščita, pričakujemo, da bo Komisija sklenila, da okvir zasebnostnega ščita EU-ZDA zagotavlja ustrezno zaščito za potrebe prava Unije, in da se bodo podatki še naprej prenašali iz Evropske unije organizacijam, ki sodelujejo v zasebnostnem ščitu.

S spoštovanjem.

Ken Hyatt

Priloga 2

Arbitražni model

PRILOGA I

Priloga I določa pogoje, pod katerimi so organizacije v zasebnostnem ščitu dolžne presoditi trditve v skladu z načelom pritožbenega mehanizma, uveljavljanja in odgovornosti. Možnost zavezujoče arbitraže, opisane spodaj, se nanaša na nekatere „preostale“ zahtevke glede podatkov, ki jih krije zasebnostni ščit EU-ZDA. Namen te možnosti je zagotoviti takojšnji neodvisni in pošteni mehanizem na izbiro posameznikov za reševanje zatrjevanih kršitev načel, ki niso bili razrešeni v okviru katerega koli drugega mehanizma zasebnostnega ščita.

A. **Področje uporabe**

Možnost arbitraže je posamezniku na voljo, da pri preostalih zahtevkih ugotovi, ali je organizacija v zasebnostnem ščitu kršila obveznosti do posameznika po načelih in ali je takšna kršitev ostala v celoti ali delno neodpravljena. Ta možnost je na voljo le za te namene. Ta možnost ni na voljo, denimo, v zvezi z izjemami pri načelih ([1]) ali v zvezi z obtožbo glede ustreznosti zasebnostnega ščita.

B. **Razpoložljiva pravna sredstva**

V okviru te možnosti arbitraže je senat zasebnostnega ščita (ki ga sestavlja en ali trije arbitri, kakor se dogovorita stranki) pristojen za odrejanje nedenarnega pravičnega nadomestila glede na vsakega posameznika (kot so dostop, popravek, izbris ali vrnitev zadevnih posameznikovih podatkov), potrebnega za odpravo kršitve načel samo v zvezi s posameznikom. To so edina pooblastila arbitražnega senata v zvezi s pravnimi sredstvi. Ob upoštevanju pravnih sredstev je arbitražni senat dolžan upoštevati druga pravna sredstva, ki so jih odredili že drugi mehanizmi v okviru zasebnostnega ščita. Na voljo ni odškodnin, stroškov, pristojbin ali drugih pravnih sredstev. Vsaka stranka nosi svoje odvetniške stroške.

C. **Predarbitražne zahteve**

Posameznik, ki se odloči uveljaviti možnost arbitraže, mora slediti naslednjim korakom, preden sproži arbitražni zahtevek: (1) predložiti zatrjevano kršitev neposredno organizaciji in ponuditi organizaciji možnost, da reši zadevo v časovnem okviru, določenem v členu III.11(d)(i) načel; (2) uporabiti neodvisni pritožbeni mehanizem v okviru načel, ki je brezplačen za posameznika; in (3) predložiti zadevo prek svojega organa za zaščito podatkov Ministrstvu za trgovino ter slednjemu ponuditi možnost, da po svojih najboljših močeh razreši zadevo v časovnih okvirih, določenih v pismu Uprave za mednarodno trgovino Ministrstva za trgovino, brezplačno za posameznika.

Ta možnost arbitraže ni na voljo, če je posameznikova ista zatrjevana kršitev načel (1) prej bila predmet zavezujoče arbitraže; (2) prej bila predmet pravnomočne sodbe, sprejete v sodnem postopku, v katerem je bil posameznik stranka; ali (3) bila prej poravnana med strankama. Poleg tega te možnosti ni mogoče uveljaviti, če ima organ EU za zaščito podatkov (1) pristojnost po členu III.5 ali III.9 načel; ali (2) pristojnost za reševanje zatrjevane kršitve neposredno z organizacijo. Pooblastilo organa za zaščito podatkov za reševanje istega zahtevka proti upravljavcu podatkov iz EU samo po sebi ne onemogoča uporabe te možnosti arbitraže proti drugi pravni osebi, ki je ne veže pooblastilo organa za zaščito podatkov.

D. **Zavezujoča narava sklepov**

Posameznikova odločitev, da uveljavi to možnost zavezujoče arbitraže, je v celoti prostovoljna. Arbitražni sklepi bodo zavezujoči za vse stranke v arbitražnem postopku. Ob njeni uporabi se posameznik odpove možnosti, da poišče nadomestilo za isto zatrjevano kršitev pri drugem forumu z izjemo, da, v kolikor nedenarno pravično nadomestilo ne odpravi v celoti zatrjevane kršitve, posameznikova uveljavitev arbitraže ne onemogoči zahtevka za odškodnino, ki je sicer na voljo na sodiščih.

([1]) Člen I.5 načel.

E. **Pregled in izvrševanje**

Posamezniki in organizacije v zasebnostnem ščitu bodo lahko zahtevali sodno presojo in izvršitev arbitražnih sklepov v skladu z zakonodajo ZDA, in sicer zveznim zakonom o arbitraži (Federal Arbitration Act) ([1]). Vse take zadeve je treba vložiti pri zveznem okrožnem sodišču, ki je krajevno pristojno za primarni kraj poslovanja organizacije v zasebnostnem ščitu.

Ta možnost arbitraže je namenjena reševanju posameznih sporov, namen arbitražnih sklepov pa ni, da služijo kot prepričljiv ali zavezujoč precedens v zadevah, ki vključujejo druge stranke, vključno v prihodnjih arbitražah ali na sodiščih v EU ali ZDA ali v postopkih Zvezne komisije za trgovino.

F. **Arbitražni senat**

Stranke bodo izbrale arbitre s seznama arbitrov, obravnavanega spodaj.

Skladno z veljavno zakonodajo bosta Ministrstvo za trgovino ZDA in Evropska komisija oblikovala seznam vsaj 20 arbitrov, izbranih na podlagi neodvisnosti, integritete in strokovnosti. V zvezi s tem postopkom velja naslednje:

Arbitri:

(1) bodo ostali na seznamu 3 leta, razen v izjemnih razmerah ali z razlogom, njihovo imenovanje pa se lahko podaljša za eno dodatno obdobje 3 let;

(2) ne sprejemajo navodil in niso povezani s katero koli stranko ali organizacijo v zasebnostnem ščitu ali z ZDA, EU ali katero koli državo članico EU ali morebitnim drugim vladnim organom, javnim organom ali organom pregona; in

(3) morajo biti pooblaščeni za opravljanje odvetniškega poklica v ZDA in strokovnjaki za zakonodajo ZDA na področju varstva zasebnosti ter imeti strokovno znanje in izkušnje v zakonodaji EU na področju zaščite podatkov.

G. **Arbitražni postopki**

Skladno z veljavno zakonodajo se bosta Ministrstvo za trgovino in Evropska komisija v roku 6 mesecev od sprejetja sklepa o ustreznosti dogovorila o sprejetju obstoječega ustaljenega niza ameriških arbitražnih postopkov (kot je AAA ali JAMS) za urejanje postopkov pred senatom zasebnostnega ščita v skladu z vsakim od naslednjih stališč:

1. Posameznik lahko sproži zavezujočo arbitražo v skladu z zgornjo določbo glede predarbitražnih zahtev, tako da organizaciji pošlje „obvestilo“. Obvestilo vsebuje povzetek ukrepov, izvedenih po odstavku C, za rešitev zahtevka, opis domnevne kršitve in po izbiri posameznika morebitna dokazila in materiale in/ali pravno razpravo v zvezi z domnevnim zahtevkom.

([1]) Poglavje 2 zveznega zakona o arbitraži (Federal Arbitration Act ali FAA) določa, da „arbitražni sporazum ali arbitražna odločba, ki izhaja iz pogodbenega ali nepogodbenega pravnega razmerja, ki se šteje za poslovnega, vključno s transakcijo, pogodbo ali sporazumom, opisanim v [členu 2 FAA], sodi v okvir Konvencije [o priznavanju in izvrševanju tujih arbitražnih odločb z dne 10. junija 1958, 21 U.S.T. 2519, T.I.A.S. št. 6997 (‚newyorška konvencija')].“ Člen 202 naslova 9 zakonodajne zbirke ZDA. FAA nadalje določa, da „[a] se šteje, da sporazum ali odločba na podlagi takšnega razmerja, v celoti med državljani Združenih držav, ne sodi v okvir [newyorške] konvencije, razen če to razmerje vključuje premoženje v tujini, predvideva učinkovitost ali izvrševanje v tujini ali ima neko drugo razumno povezavo z eno ali več tujimi državami.“ *Id.* V skladu s poglavjem 2 „lahko katera koli stranka v arbitraži uveljavi pri katerem koli sodišču, ki je pristojno po tem poglavju, sklep, ki potrjuje odločbo, kot proti kateri koli drugi stranki v arbitraži. Sodišče potrdi odločbo, razen če ugotovi obstoj enega od razlogov za zavrnitev ali odložitev priznanja ali izvrševanja odločbe, navedene v omenjeni [newyorški] konvenciji.“ *Id.* člen 207. Poglavje 2 nadalje določa, da „imajo okrožna sodišča Združenih držav … izvirno pristojnost nad … tožbo ali postopkom [po newyorški konvenciji] ne glede na sporen znesek.“ *Id.* člen 203.
Poglavje 2 določa tudi, da „Poglavje 1 velja za tožbe in postopke, vložene po tem poglavju, če tisto poglavje ni v nasprotju s tem poglavjem ali [newyorško] konvencijo, kakor so jo ratificirale Združene države.“ *Id.* člen 208. Poglavje 1 pa določa, da „je pisna določba v … pogodbi, ki dokazuje trgovski posel, da se z arbitražo reši spor, ki izhaja iz takšne pogodbe ali posla, ali zavrnitev izvedbe celotnega ali dela pogodbe ali posla, ali v pisnem sporazumu, da se obstoječi spor, ki izhaja iz takšne pogodbe, posla ali zavrnitve, predloži v arbitražo, veljavna, nepreklicna in izvršljiva, razen če obstajajo razlogi, kakor so določeni po zakonu ali v kapitalu za preklic katere koli pogodbe.“ *Id.* člen 2. Poglavje 1 nadalje določa, da „lahko katera koli stranka v arbitraži pri tako določenem sodišču vloži predlog za odločbo, ki potrjuje dodelitev, na podlagi tega pa mora sodišče ugoditi takšni odločbi, razen če je dodelitev razveljavljena, spremenjena ali popravljena, kakor je predpisano v členih 10 in 11 [FAA].“ *Id.* člen 9.

2. Oblikovani bodo postopki, ki bodo zagotovili, da ista zatrjevana kršitev ne postane predmet podvojenih pravnih sredstev ali postopkov.

3. Ukrep Zvezne komisije za trgovino se lahko nadaljuje vzporedno z arbitražo.

4. V teh arbitražah ne sme sodelovati noben predstavnik ZDA, EU ali katere koli države članice EU ali drugega vladnega organa, javnega organa ali organa pregona pod pogojem, da lahko na zahtevo posameznika iz EU organi za zaščito podatkov EU zagotovijo pomoč samo pri pripravi obvestila, ne smejo pa imeti dostopa do ugotavljanja ali morebitnega drugega gradiva v zvezi s temi arbitražami.

5. Kraj arbitraže bo v Združenih državah, posameznik pa lahko izbere sodelovanje po video prenosu ali telefonu, ki se posamezniku zagotovi brezplačno. Osebna udeležba ne bo potrebna.

6. Jezik arbitraže bo angleški, razen če se stranki dogovorita drugače. Na podlagi utemeljene zahteve in ob upoštevanju tega, ali posameznika zastopa odvetnik, se tolmačenje na arbitražni obravnavi kot tudi prevod arbitražnega gradiva posamezniku zagotovi brezplačno, razen če senat ugotovi, da bi to glede na okoliščine posamezne arbitraže privedlo do neupravičenih ali nesorazmernih stroškov.

7. Gradivo, predloženo arbitrom, bo obravnavano kot zaupno in bo uporabljeno samo v povezavi z arbitražo.

8. Po potrebi se dovoli posamezno odkritje, takšno odkritje pa stranki obravnavata kot zaupno in bo uporabljeno zgolj v povezavi z arbitražo.

9. Arbitraža mora biti zaključena v 90 dneh od dostave obvestila zadevni organizaciji, razen če se stranki dogovorita drugače.

H. **Stroški**

Arbitri morajo ustrezno ukrepati, da bi zmanjšali stroške ali pristojbine arbitraže.

V skladu z veljavno zakonodajo bo Ministrstvo za trgovino omogočilo ustanovitev sklada, v katerega bodo morale organizacije v zasebnostnem ščitu plačati letni prispevek, deloma na podlagi velikosti organizacije, ki bo kril strošek arbitraže, vključno s stroški arbitrov, do najvišjih dovoljenih zneskov („najvišje vrednosti“) v posvetovanju z Evropsko komisijo. Sklad bo upravljala tretja stranka, ki bo redno poročala o delovanju sklada. Na letnem pregledu bosta Ministrstvo za trgovino in Evropska komisija pregledala delovanje sklada, vključno s potrebo po prilagoditvi zneska prispevkov ali najvišjih vrednosti, in med drugim upoštevala število arbitraž ter stroške in časovni potek arbitraž ob vzajemnem razumevanju, da organizacijam v zasebnostnem ščitu ne bo naloženo čezmerno finančno breme. Ta določba ne krije stroškov odvetnikov ali morebitnih skladov.

PRILOGA II

NAČELA OKVIRA ZASEBNOSTNEGA ŠČITA EU-ZDA IZDALO MINISTRSTVO ZA TRGOVINO ZDA

I. PREGLED

1. Združene države in Evropska unija so si sicer zadale skupen cilj krepitve varstva zasebnosti, vendar se pristop Združenih držav do zasebnosti razlikuje od pristopa Evropske unije. V Združenih državah se uporablja sektorski pristop, ki temelji na mešanici zakonodaje, predpisov in samourejanja. Glede na te razlike in da bi organizacijam v Združenih državah zagotovili zanesljiv mehanizem za prenose osebnih podatkov iz Evropske unije v Združene države, obenem pa poskrbeli, da posamezniki iz EU, na katere se nanašajo osebni podatki, še naprej uživajo učinkovite zaščitne ukrepe in varstvo, kakor jih predpisuje evropska zakonodaja v zvezi z obdelavo njihovih osebnih podatkov, ko se ti prenesejo v države zunaj EU, Ministrstvo za trgovino izdaja ta načela zasebnostnega ščita, vključno z dopolnilnimi načeli (v nadaljnjem besedilu skupaj: načela) v okviru svoje zakonske pristojnosti, da omogoča, spodbuja in razvija mednarodno trgovino (člen 1512 naslova 15 zakonodajne zbirke ZDA). Načela so bila oblikovana v posvetovanju z Evropsko komisijo, predstavniki industrije in drugimi deležniki zaradi lajšanja trgovskih in gospodarskih stikov med Združenimi državami in Evropsko unijo. Namenjena so izključno organizacijam v Združenih državah, ki prejemajo osebne podatke iz Evropske unije, z namenom izpolnjevanja pogojev zasebnostnega ščita in s tem prejemanja ugodnosti iz sklepa Evropske komisije o ustreznosti ([1]). Načela ne vplivajo na uporabo nacionalnih določb, s katerimi se izvaja Direktivo 95/46/ES (v nadaljnjem besedilu: direktiva) in se nanašajo na obdelavo osebnih podatkov v državah članicah. Načela prav tako ne omejujejo obveznosti v zvezi z varstvom zasebnosti, ki sicer veljajo v skladu z zakonodajo ZDA.

2. Da bi organizacija za izvedbo prenosov osebnih podatkov iz EU lahko uporabila zasebnostni ščit, mora samocertificirati svojo zavezanost k načelom pri Ministrstvu za trgovino (ali njegovemu pooblaščenemu predstavniku) (v nadaljnjem besedilu: Ministrstvo). Medtem ko so odločitve organizacij, da tako vstopijo v zasebnostni ščit, popolnoma prostovoljne, pa je dejansko spoštovanje načel obvezno: organizacije, ki se samocertificirajo pri Ministrstvu in javno razglasijo svojo zavezanost k načelom, morajo načela spoštovati v celoti. Organizacija mora za pristop k zasebnostnem ščitu (a) soditi v okvir preiskovalnih in izvršilnih pooblastil Zvezne komisije za trgovino (v nadaljnjem besedilu: FTC), Ministrstva za promet ali drugega zakonsko določenega organa, ki bo učinkovito zagotovil spoštovanje načel *(drugi zakonsko določeni organi ZDA, ki jih prizna EU, se lahko vključijo pozneje s prilogo)*; (b) javno razglasiti svojo zavezanost k spoštovanju načel; (c) javno razkriti svoje politike zasebnosti v skladu s temi načeli in (d) jih v celoti izvajati. Če organizacija ne izpolnjuje načel, je mogoče zoper njo začeti postopek v skladu s členom 5 zakona o zvezni komisiji za trgovino (Federal Trade Commission Act), ki prepoveduje nepoštena in goljufiva dejanja v trgovini ali v zvezi s trgovino (člen 45(a) naslova 15), ali drugih zakonih ali predpisih, ki prepovedujejo takšna dejanja.

3. Ministrstvo za trgovino bo vodilo verodostojen seznam organizacij iz ZDA, ki so se samocertificirale pri Ministrstvu in razglasile svojo zavezanost k spoštovanju načel, (v nadaljnjem besedilu: seznam zasebnostnega ščita) ter javnosti omogočilo dostop do njega. Ugodnosti zasebnostnega ščita so zagotovljene od datuma, ko Ministrstvo uvrsti organizacijo na seznam varnostnega ščita. Ministrstvo s seznama zasebnostnega ščita organizacijo odstrani, če ta prostovoljno izstopi iz zasebnostnega ščita ali če ne opravi letne samocertifikacije pri Ministrstvu. Odstranitev organizacije s seznama zasebnostnega ščita pomeni, da ta ni več upravičena do ugodnosti, ki izhajajo iz sklepa Evropske komisije o ustreznosti, da bi prejemala osebne informacije iz EU. Dokler hrani osebne informacije, ki jih je prejela med sodelovanjem v zasebnostnem ščitu, mora organizacija v zvezi s takimi informacijami še naprej uporabljati načela in pri Ministrstvu vsako leto potrditi svojo zavezanost k takšnemu ravnanju; v nasprotnem primeru mora organizacija vrniti ali izbrisati informacije ali zagotoviti „ustrezno“ varstvo informacij z drugimi dovoljenimi sredstvi. Ministrstvo s seznama zasebnostnega ščita odstrani tudi tiste organizacije, ki vztrajno ne izpolnjujejo načel; te organizacije niso upravičene do ugodnosti zasebnostnega ščita in morajo vrniti ali izbrisati osebne informacije, ki so jih prejele v okviru zasebnostnega ščita.

4. Ministrstvo bo prav tako vodilo in dalo javnosti na voljo verodostojno evidenco organizacij iz ZDA, ki so se v preteklosti samocertificirale pri Ministrstvu, vendar so bile s seznama zasebnostnega ščita odstranjene. Ministrstvo bo izdalo jasno opozorilo, da te organizacije ne sodelujejo v zasebnostnem ščitu; da odstranitev s seznama zasebnostnega ščita pomeni, da take organizacije ne morejo trditi, da izpolnjujejo načela zasebnostnega ščita, ter da se morajo vzdržati morebitnih izjav ali zavajajočih ravnanj, ki bi nakazovala, da sodelujejo v zasebnostnem ščitu in da take organizacije niso več upravičene do ugodnosti, ki izhajajo iz sklepa Evropske komisije o ustreznosti in bi tem organizacijam omogočala prejemanje osebnih informacij iz EU. Proti organizaciji, ki še naprej trdi, da sodeluje

([1]) Če se bo sklep Komisije o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, uporabljal za Islandijo, Lihtenštajn in Norveško, bo sveženj o zasebnostnem ščitu zajemal tako Evropsko unijo kot tudi te tri države. Zato se bo za sklicevanja na EU in njene države članice štelo, da vključujejo Islandijo, Lihtenštajn in Norveško.

v zasebnostnem ščitu, ali daje druge lažne navedbe v zvezi z zasebnostnim ščitom, potem ko je že bila odstranjena s seznama zasebnostnega ščita, lahko Zvezna komisija za trgovino, Ministrstvo za promet ali drugih organi pregona uvedejo izvršilne ukrepe.

5. Zavezanost k tem načelom je lahko omejena: (a) če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa ali kazenskega pregona; (b) z zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdružljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel omejeno na obseg, ki je potreben za izpolnitev prevladujočih zakonitih interesov na podlagi takih pooblastil; ali (c) če direktiva ali pravo države članice dovoljuje izjeme in odstopanja, če se te izjeme in odstopanja uporabljajo v primerljivih okoliščinah. V skladu s ciljem krepitve varstva zasebnosti si morajo organizacije prizadevati, da načela uveljavijo v celoti in pregledno, vključno s tem, da v svoji politiki varstva zasebnosti navedejo, kdaj se bodo izjeme, dovoljene s točko (b) zgoraj, redno uporabljale. Iz istega razloga se od organizacij pričakuje, da se, kadar načela in/ali pravo ZDA dopuščajo izbiro, odločijo za možnost z večjim varstvom.

6. Organizacije morajo po vstopu v zasebnostni ščit načela uporabljati pri vseh osebnih podatkih, ki se prenesejo na podlagi uporabe zasebnostnega ščita. Organizacija, ki se odloči razširiti ugodnosti zasebnostnega ščita na osebne podatke o človeških virih, ki jih prejme iz EU, za uporabo v okviru zaposlitvenih razmerij, mora to navesti ob samocertificiranju pri Ministrstvu in izpolniti zahteve, ki so določene v dopolnilnem načelu o samocertificiranju.

7. Zakonodaja ZDA se bo uporabila za vprašanja glede razlage in izpolnjevanja načel ter ustreznih politik zasebnosti organizacij v zasebnostnem ščitu, razen če so se takšne organizacije zavezale k sodelovanju z evropskimi organi za zaščito podatkov. Če ni določeno drugače, se vse določbe načel uporabljajo v primerih, v katerih ustrezajo.

8. Opredelitev pojmov:

   a. „Osebni podatki“ in „osebne informacije“ so podatki o znanem ali prepoznavnem posamezniku, ki so zapisani v kateri koli obliki in sodijo na področje uporabe direktive ter jih organizacije v ZDA prejmejo iz Evropske unije.

   b. „Obdelava“ osebnih podatkov pomeni kakršno koli operacijo ali niz operacij, ki se izvedejo na osebnih podatkih z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, evidentiranje, organiziranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje ali širjenje in izbris ali uničenje.

   c. „Upravljavec“ je oseba ali organizacija, ki sama ali v sodelovanju z drugimi določa namene in sredstva za obdelavo osebnih podatkov.

9. Datum začetka veljavnosti načel je datum končne odobritve ugotovitve Evropske komisije o ustreznosti.

II. NAČELA

1. **Obvestilo**

   a. Organizacija mora posameznike obvestiti o:

      i. svojem sodelovanju v zasebnostnem ščitu in zagotoviti povezavo do ali spletni naslov seznama zasebnostnega ščita,

      ii. vrstah zbranih osebnih podatkov in, kjer je primerno, o subjektih in podružnicah organizacije, ki prav tako spoštujejo načela,

iii. svoji zavezanosti k temu, da pri vseh osebnih podatkih, ki jih prejme iz EU na podlagi zasebnostnega ščita, uporabi načela,

iv. namenih, za katere zbira in uporablja njihove osebne informacije,

v. kako stopiti stik s takšno organizacijo pri morebitnih poizvedbah ali pritožbah, vključno z katero koli ustrezno ustanovo v EU, ki lahko odgovori na takšne poizvedbe ali pritožbe,

vi. vrsti ali identiteti tretjih strank, katerim razkrije osebne informacije, in namene za njihovo razkritje,

vii. pravici posameznikov do dostopa do svojih osebnih podatkov,

viii. izbiri in sredstvih, ki jih organizacija ponuja posameznikom za omejevanje uporabe in razkritja njihovih osebnih podatkov,

ix. neodvisni službi za reševanje sporov, določeni za obravnavanje pritožb in brezplačno zagotavljanje ustreznega pritožbenega mehanizma posamezniku, in ali je to: (1) forum, ki ga ustanovijo organi za zaščito podatkov, (2) drugi izvajalec reševanja sporov s sedežem v EU ali (3) drugi izvajalec reševanja sporov s sedežem v Združenih državah,

x. tem, da zanje veljajo preiskovalna in izvršilna pooblastila Zvezne komisije za trgovino, Ministrstva za promet ali morebitnega drugega ameriškega zakonsko določenega organa,

xi. možnosti posameznika, da pod določenimi pogoji uveljavi zavezujočo arbitražo,

xii. zahtevi po razkritju osebnih informacij na podlagi zakonitih zahtev javnih organov, tudi z namenom izpolnjevanja zahtev nacionalne varnosti ali kazenskega pregona, in

xiii. svoji odgovornosti v primerih prenosa tretjemu.

b. To obvestilo organizacije mora biti jasno in nedvoumno, ko posameznika prvič prosi za zagotovitev osebnih podatkov ali kakor hitro je izvedljivo za tem, v vsakem primeru pa pred uporabo teh podatkov za namene, ki niso tisti, za katere jih je prvotno zbrala in obdelala pošiljajoča organizacija, ali pred prvim razkrijem tretji stranki.

2. **Možnost izbire**

a. Organizacija mora posameznikom ponuditi možnost izbire (zavrnitve) o tem, ali se bodo njihovi osebni podatki (i) razkrili tretji stranki ali (ii) se bodo uporabili za namen, ki se bistveno razlikuje od namenov, za katere so bili prvotno zbrani ali jih posamezniki pozneje odobrili. Posameznikom se morajo zagotoviti postopki izvršitve možnosti izbire, ki so jasni, razumljivi in dostopni.

b. Z odstopanjem od prejšnjega odstavka možnost izbire ni potrebna, kadar se podatki razkrivajo tretji stranki, ki v vlogi posrednika izvaja naloge v imenu in po navodilih organizacije. Vendar pa organizacija vedno sklene pogodbo s posrednikom.

c. Pri občutljivih podatkih (tj. osebnih podatkih, ki določajo zdravniško in zdravstveno stanje, rasno in etnično pripadnost, politična, verska in filozofska prepričanja, sindikalno članstvo, in podatkih o spolnem življenju posameznika) morajo organizacije od posameznikov pridobiti izrecno pozitivno soglasje (privolitev), kadar je takšne podatke treba (i) razkriti tretji stranki ali (ii) jih uporabiti za namen, ki ni tisti, za katerega so bili prvotno zbrani ali so ga posamezniki pozneje odobrili s svojo izbiro privolitve. Poleg tega mora organizacija obravnavati kot občutljive vse osebne informacije, ki jih je prejela od tretje stranke, kadar jih kot občutljive identificira in obravnava tretja stranka.

3. **Odgovornost za prenos tretjemu**

a. Za prenos osebnih informacij tretjemu, ki nastopa v vlogi upravljavca, morajo organizacije izpolniti načeli obvestila in možnosti izbire. Organizacije morajo skleniti tudi pogodbo s tretjim upravljavcem, ki določa, da se taki podatki smejo obdelovati le za omejene in natančno določene namene v skladu s soglasjem, ki ga podal posameznik, in da bo prejemnik zagotovil enako raven zaščite kot načela ter organizacijo obvestil, če ugotovi, da te obveznosti ne more več izpolnjevati. V tej pogodbi je določeno, da tretji upravljavec v primeru take ugotovitve preneha z obdelavo ali sprejme druge razumne in ustrezne ukrepe za odpravo.

b. Za prenos osebnih podatkov tretji stranki, ki nastopa v vlogi posrednika, morajo organizacije: (i) prenesti takšne podatke le za omejene in natančno določene namene; (ii) potrditi, da je posrednik dolžan zagotoviti vsaj enako raven varstva zasebnosti, kot jo zahtevajo načela; (iii) sprejeti razumne in ustrezne ukrepe, s katerimi zagotovijo, da posrednik dejansko obdela prenesene osebne informacije na način, ki je skladen z obveznostmi organizacije v skladu z načeli; (iv) od zastopnika zahtevati, da jih v primeru ugotovitve, da ne more več izpolnjevati obveznosti glede zagotavljanja enake ravni varstva, kot jo zahtevajo načela, o tem obvesti; (v) po obvestilu, vključno v skladu s točko iv, sprejeti razumne in ustrezne ukrepe za ustavitev in odpravo nepooblaščene obdelave ter na zahtevo Ministrstvu zagotovi povzetek ali reprezentativni izvod ustreznih določb o zasebnosti iz svoje pogodbe s tem posrednikom.

4. **Varnost**

a. Organizacije, ki pripravljajo, vzdržujejo, uporabljajo ali širijo osebne podatke, morajo sprejeti ustrezne in razumne ukrepe, da jih zavarujejo pred izgubo, zlorabo in nepooblaščenim dostopom, razkritjem, spreminjanjem in uničenjem ob ustreznem upoštevanju tveganj, vključenih v obdelavo, in naravo osebnih podatkov.

5. **Neokrnjenost podatkov in omejitev namena**

a. V skladu z načeli je treba osebne informacije omejiti na informacije, ki ustrezajo namenu obdelave ([1]). Organizacija ne sme obdelovati osebnih podatkov na način, ki je nezdružljiv z nameni, za katere so bili podatki zbrani ali jih je posameznik pozneje odobril. V obsegu, potrebnem za te namene, mora organizacija z ustreznimi ukrepi zagotoviti, da so osebni podatki zanesljivi za nameravano uporabo, točni, popolni in trenutni. Organizacija mora spoštovati načela, dokler hrani take informacije.

b. Informacije se lahko hranijo v obliki, s katero je posameznik določen ali določljiv ([2]), le dokler služijo namenu obdelave v smislu točke 5a. Ta obveznost organizacijam ne preprečuje obdelave osebnih podatkov za daljša obdobja, in sicer če čas in obseg take obdelave razumno služi namenom arhiviranja v javnem interesu, novinarstva, literature in umetnosti, znanstvenih in zgodovinskih raziskav ter statistične analize. V teh primerih za tako obdelavo veljajo druga načela in določbe okvira. Organizacije morajo sprejeti razumne in ustrezne ukrepe za uskladitev s to določbo.

6. **Dostop**

a. Posamezniki morajo imeti dostop do svojih osebnih podatkov, ki jih hrani organizacija, in možnost, da te podatke popravijo, spremenijo ali izbrišejo, kadar niso točni ali so bili obdelani ob kršitvi načel, razen kadar bi bili stroški ali izdatki za zagotovitev dostopa nesorazmerni s tveganjem za zasebnost zadevnega posameznika ali kadar bi bile kršene pravice drugih oseb.

([1]) Odvisno od okoliščin, primeri združljivih namenov obdelave lahko vključujejo tiste, ki razumno služijo za odnose s strankami, skladnost in pravne namene, revizije, varnost in preprečevanje goljufij, ohranjanje in obrambo pravnih pravic organizacije ali za druge namene, skladne s pričakovanji razumne osebe glede na kontekst zbiranja.

([2]) Posameznik je v tem kontekstu, če bi ga lahko glede na sredstva za identifikacijo, ki bodo pričakovano uporabljena, (ob upoštevanju, med drugim, stroškov in časa, potrebnega za identifikacijo ter razpoložljive tehnologija v času obdelave) in obliko, v kakršni se hranijo podatki, organizacija ali tretja oseba, če bi imela dostop do podatkov, razumno prepoznala, „prepoznaven."

7. **Pritožbeni mehanizem, uveljavljanje in odgovornost**

a. Učinkovita zaščita zasebnosti mora vključevati trdne mehanizme, ki zagotavljajo skladnost z načeli, pritožbene mehanizme za posameznike, ki jih neizpolnjevanje načel prizadene, in posledice za organizacije, kadar ne spoštujejo načel. Takšni mehanizmi morajo vključevati vsaj:

i. dostopne neodvisne pritožbene mehanizme, s katerimi se pritožbe in spori vsakega posameznika preiščejo in hitro razrešijo brez stroška za posameznika in s sklicevanjem na načela, ter se dodeli odškodnina na podlagi veljavne zakonodaje ali pobud javnega sektorja;

ii. postopke za preverjanje resničnosti izjav in zatrjevanj organizacij glede njihove prakse varovanja zasebnosti ter preverjanje izvajanja praks varstva zasebnosti na naveden način ter zlasti glede na primere neizpolnjevanja; in

iii. obveznosti odpravljanja težav, ki nastanejo, ker organizacije, ki so javno razglasile svojo zavezanost k načelom, teh ne spoštujejo, in posledice za te organizacije. Sankcije morajo biti dovolj stroge, da zagotovijo spoštovanje načel.

b. Organizacije in njihovi izbrani neodvisni pritožbeni mehanizmi se bodo pravočasno odzvali na poizvedbe in zahteve Ministrstva po informacijah v zvezi z zasebnostnim ščitom. Vse organizacije se morajo hitro odzvati na pritožbe v zvezi s skladnostjo z načeli, ki so jih organi držav članic EU poslali na Ministrstvo. Organizacije, ki so se odločile sodelovati z organi za zaščito podatkov, vključno z organizacijami, ki obdelujejo podatke o človeških virih, morajo neposredno odgovoriti takšnim organom v zvezi s preiskovanjem in reševanjem pritožb.

c. Organizacije so dolžne presoditi trditve in upoštevati pogoje, določene v Prilogi I, če je posameznik uveljavil zavezujočo arbitražo, s tem ko je zadevni organizaciji poslal obvestilo in upošteval postopke ter v skladu s pogoji, določenimi v Prilogi I.

d. V okviru prenosa tretjemu je organizacija v zasebnostnem ščitu odgovorna za obdelavo osebnih podatkov, ki jih prejme v okviru zasebnostnega ščita in naknadno prenese tretji stranki, ki nastopa v vlogi posrednika v njenem imenu. Organizacija v zasebnostnem ščitu ostane odškodninsko odgovorna po načelih, če njen posrednik obdeluje take osebne informacije na način, ki ni skladen z načeli, razen če organizacija dokaže, da ni odgovorna za dogodek, ki je povzročil škodo.

e. Ko organizacija postane predmet odloka FTC ali sodne odločbe zaradi neizpolnjevanja načel, organizacija objavi vse ustrezne dele poročila o skladnosti ali oceni v zvezi z zasebnostnim ščitom, ki se predloži Zvezni komisiji za trgovino, če je to skladno z zahtevami glede zaupnosti. Ministrstvo je imenovalo posebno osebo za stike z organi za zaščito podatkov v primeru težav glede izpolnjevanja načel s strani organizacij v zasebnostnem ščitu. Zvezna komisija za trgovino bo prednostno obravnavala predložitve glede neizpolnjevanja načel z Ministrstva in organov držav članic EU ter bo pravočasno izmenjala informacije o teh zadevah z državnimi organi, ki so jih predložili, v skladu z obstoječimi omejitvami glede zaupnosti.

III. DOPOLNILNA NAČELA

1. **Občutljivi podatki**

a. Organizacija ni dolžna pridobiti izrecnega pozitivnega soglasja (privolitve) v zvezi z občutljivimi podatki, kjer je obdelava:

i. v življenjskem interesu subjekta podatkov ali druge osebe;

ii. potrebna za uveljavitev pravnih zahtevkov ali obrambe;

iii. nujna za zagotovitev zdravstvene nege ali diagnoze;

iv. izvedena med potekom zakonitih dejavnosti politično, filozofsko, versko ali sindikalno usmerjenega sklada, združenja ali kake druge nepridobitne organizacije in pod pogojem, da obdelava zadeva izključno člane te organizacije ali osebe, ki so v zvezi z njenimi dejavnostmi z organizacijo v rednih stikih, ter da se podatki ne razkrijejo tretji stranki brez privolitve subjektov podatkov;

v. potrebna za izvajanje obveznosti organizacije na področju delovnega prava; ali

vi. povezana s podatki, ki jih je posameznik očitno dal v javnost sam.

2. **Izjeme za novinarsko področje**

a. Glede na ustavno varstvo svobode tiska v ZDA in izjemo direktive za novinarsko področje, kadar so pravice svobodnega tiska iz prvega amandmaja Ustave ZDA v koliziji z interesom varstva zasebnosti, mora prvi amandma uravnotežiti te interese glede na dejavnosti fizičnih in pravnih oseb v ZDA.

b. Za osebne podatke, ki se zbirajo za objavo v časopisu ali po radiu in televiziji ali za drugo obliko javnega sporočanja novinarskega gradiva, ne glede na to, ali so bili dejansko uporabljeni, pa tudi za podatke, najdene v predhodno objavljenem gradivu, razširjenem iz medijskih arhivov, ne veljajo zahteve načel zasebnostnega ščita.

3. **Sekundarna odgovornost**

a. Ponudniki internetnih storitev, telekomunikacijska podjetja in druge organizacije niso odgovorni po načelih zasebnostnega ščita, kadar v imenu druge organizacije zgolj prenašajo, usmerjajo, zamenjujejo ali pridobivajo informacije. Kakor utemeljuje sama direktiva, zasebnostni ščit ne ustvarja sekundarne odgovornosti. Kolikor je organizacija zgolj posrednik podatkov, ki jih prenaša tretja stranka ter pri tem ne določa namenov in načinov obdelave teh osebnih podatkov, ni odgovorna.

4. **Izvedba skrbnega pregleda in revizij**

a. Dejavnosti revizorjev in investicijskih bank lahko vključujejo obdelavo osebnih podatkov brez privolitve ali vednosti posameznika. To dovoljujejo načela obvestila, možnosti izbire in dostopa pod pogoji, opisanimi spodaj.

b. Javne delniške družbe in podjetja z omejenim številom lastnikov, vključno z organizacijami v zasebnostnem ščitu, so predmet rednih revizij. Takšne revizije, zlasti tiste, ki preiskujejo morebitna hudodelstva, so lahko ogrožene, če so razkrite prehitro. Podobno bo morala organizacija v zasebnostnem ščitu, ki je vpletena v morebitno združitev ali prevzem, izvesti ali prestati „skrbni pregled“. Ta bo pogosto vključeval zbiranje in obdelavo osebnih podatkov, kot so informacije o višjih izvršilnih delavcih in drugem ključnem osebju. Prehitro razkritje lahko ovira posel ali celo krši veljavni predpis glede vrednostnih papirjev. Investicijske banke in odvetniki, najeti za skrbni pregled, ali revizorji, ki izvajajo revizijo, lahko obdelujejo podatke brez vednosti posameznika samo v takšnem obsegu in tako dolgo, kolikor je potrebno, da se zadosti zakonskim ali javnim interesom, ter v drugih okoliščinah, v katerih bi uporaba teh načel škodovala zakonitim interesom organizacije. Ti zakoniti interesi vključujejo spremljanje izpolnjevanja zakonitih obveznosti in zakonitih računovodskih dejavnosti organizacij ter potrebo po zaupnosti v zvezi z morebitnimi nakupi, združitvami, skupnimi vlaganji ali drugo podobno transakcijo, ki jo opravijo investicijske banke in revizorji.

5. **Vloga organov za zaščito podatkov**

a. Organizacije bodo izvajale svojo zavezo k sodelovanju z organi EU za zaščito podatkov, kakor je opisano spodaj. V okviru zasebnostnega ščita se morajo organizacije ZDA, ki prejemajo osebne podatke iz EU, zavezati, da bodo uporabile učinkovite mehanizme za zagotavljanje izpolnjevanja načel zasebnostnega ščita. Kakor je navedeno v načelu pritožbenega mehanizma, uveljavljanja in odgovornosti, morajo sodelujoče organizacije zagotoviti: (a)(i) pritožbene mehanizme za posameznike, na katere se nanašajo podatki; (a)(ii) postopke za preverjanje resničnosti izjav in zatrjevanj glede njihove prakse varovanja zasebnosti; in (a)(iii) obveznosti odpravljanja težav, ki nastanejo zaradi neizpolnjevanja načel, in posledice za te organizacije. Organizacija lahko izpolni točki (a)(i) in (a)(iii) načela pritožbenega mehanizma, uveljavljanja in odgovornosti, če se zaveže k zahtevam, določenim tukaj, za sodelovanje z organi za zaščito podatkov.

b. Organizacija se zaveže, da bo sodelovala z organi za zaščito podatkov, tako da v predložitvi samocertifikacije Ministrstvu za trgovino (*glej* dopolnilno načelo o samocertificiranju) izjavi naslednje:

i. da se je organizacija odločila izpolniti zahteve iz točk (a)(i) in (a)(iii) načela pritožbenega mehanizma, uveljavljanja in odgovornosti z zavezo o sodelovanju z organi za zaščito podatkov;

ii. da bo sodelovala z organi za zaščito podatkov pri preiskavah in reševanju pritožb, s sklicevanjem na načela zasebnostnega ščita; in

iii. da bo upoštevala vsak nasvet organov za zaščito podatkov, kadar ti organi menijo, da mora organizacija s posebnim ukrepom poskrbeti za uskladitev z načeli zasebnostnega ščita, vključno z reševanjem pritožb in izplačilom odškodnin v korist posameznikov, ki so bili prizadeti zaradi kakršnega koli neizpolnjevanja načel, ter da bo organom za zaščito podatkov pisno potrdila, da je take ukrepe sprejela.

c. Delovanje forumov organov za zaščito podatkov

i. Sodelovanje z organi za zaščito podatkov EU bo potekalo prek informacij in nasvetov na naslednji način:

1. Nasvete organov za zaščito podatkov EU bo posredoval neuradni forum, ustanovljen na ravni Evropske unije, ki bo med drugim pomagal zagotoviti usklajen in skladen pristop.

2. Forum bo zadevnim organizacijam ZDA svetoval glede nerešenih pritožb posameznikov v zvezi z ravnanjem z osebnimi podatki, ki so bili preneseni iz Evropske unije v okviru zasebnostnega ščita. Nasvet bo oblikovan za zagotovitev pravilne uporabe načel zasebnostnega ščita in bo vključeval vsa pravna sredstva za zadevne posameznike, ki jih bodo organi za zaščito podatkov šteli za ustreznega.

3. Forum bo takšne nasvete zagotavljal v odgovor na posredovana stališča iz zadevnih organizacij in/ali na neposredne pritožbe posameznikov zoper organizacije, ki so se zavezale, da bodo sodelovale z organi za zaščito podatkov za namene zasebnostnega ščita, pri čemer bo spodbujal in po potrebi pomagal takim posameznikom, da na začetku uporabijo morebitni notranji mehanizem reševanja pritožb, ki ga lahko ima organizacija.

4. Nasvet bo izdan šele, ko bosta oba udeleženca v sporu imela ustrezno priložnost za predložitev pripomb in kakršnih koli dokazov. Forum bo poskušal dati nasvet tako hitro, kakor to dopušča zahteva po pravilnem postopku. Praviloma si bo forum prizadeval zagotoviti nasvet v 60 dneh po prejetju pritožbe ali posredovanega stališča in po možnosti še prej.

5. Forum bo javno objavil rezultate svojih preučevanj pritožb, če se mu bo to zdelo primerno.

6. Nasvet foruma ne povzroči odgovornosti za forum ali za posamezne organe za zaščito podatkov.

ii. Kakor je navedeno zgoraj, se morajo organizacije, ki se odločijo za tak način reševanja sporov, zavezati, da bodo ravnale po nasvetu organov za zaščito podatkov. Če organizacija tudi po 25 dneh po prejemu nasveta ne ravna v skladu z njim in če ne ponudi zadovoljive razlage za zamudo, forum sporoči svojo namero, da bo predložil zadevo Zvezni komisiji za trgovino, Ministrstvu za promet ali drugemu zveznemu ali državnemu organu ZDA, ki ima zakonska pooblastila za pregon v primeru goljufije ali zavajanja, ali da bo sklenil, da gre za resno kršitev sporazuma o sodelovanju, ki ga je zato treba šteti za ničnega in neveljavnega. V slednjem primeru bo forum obvestil Ministrstvo za trgovino, da ustrezno spremeni seznam zasebnostnega ščita. Vsako neizpolnjevanje zaveze o sodelovanju z organi za zaščito podatkov, pa tudi neizpolnjevanje načel zasebnostnega ščita pomeni goljufivo prakso in kršitev po členu 5 zakona o FTC (FTC Act) ali drugega podobnega zakona.

d. Organizacija, ki želi ugodnosti po zasebnostnem ščitu za podatke o človeških virih, ki se prenesejo iz EU v okviru zaposlitvenega razmerja, se mora zavezati k sodelovanju z organi za zaščito podatkov v zvezi s takšnimi podatki (glej dopolnilno načelo v zvezi s podatki o človeških virih).

e. Organizacije, ki se bodo odločile za sodelovanje, bodo morale plačati letno pristojbino za pokrivanje stroškov delovanja foruma, dodatno pa so lahko zaprošene za kritje vseh potrebnih stroškov za prevajanje, ki izhajajo iz obravnave forumu predloženih stališč ali pritožb posameznikov zoper organizacije. Letna pristojbina ne bo presegla 500 USD in bo nižja za manjša podjetja.

6. **Samocertificiranje**

a. Ugodnosti zasebnostnega ščita se zagotavljajo od datuma, na katerega Ministrstvo uvrsti predložitev samocertifikacije organizacije na seznam zasebnostnega ščita po tem, ko je ugotovilo, da je vloga popolna.

b. Če se želi organizacija samocertificirati za zasebnostni ščit, mora predložiti Ministrstvu samocertifikacijo, ki jo podpiše vodstveni delavec v imenu organizacije, ki pristopa k zasebnostnemu ščitu, in mora vsebovati vsaj naslednje podatke:

i. ime organizacije, poštni naslov, elektronski naslov, telefonsko številko in število faksa;

ii. opis dejavnosti organizacije v zvezi z osebnimi podatki, ki jih prejema iz EU; in

iii. opis politike organizacije glede varstva zasebnosti, vključno s podatki:

1. če ima organizacija javno spletno stran, ustrezni spletni naslov, kjer je na voljo politika zasebnosti, ali, v kolikor organizacija nima javne spletne strani, kje je javnosti na voljo politika zasebnosti;

2. datum začetka izvajanja;

3. kontaktno službo, ki se ukvarja s pritožbami, zahtevami po dostopu in drugimi vprašanji, ki izhajajo iz načel zasebnostnega ščita;

4. posebno zakonsko telo, ki je pristojno za obravnavanje morebitnih pritožb proti organizaciji v zvezi z morebitno nepošteno ali zavajajočo prakso in kršitvami zakonov ali predpisov, ki urejajo zasebnost (in ki je navedena na seznamu načel ali v prihodnji prilogi k načelom);

5. ime katerega koli programa za varstvo zasebnosti, katerega član je organizacija;

6. metodo preverjanja (npr. znotraj organizacije, tretja stran) (glej dopolnilno načelo glede preverjanja); in

7. neodvisni pritožbeni mehanizem, ki je na voljo za preiskave nerešenih pritožb.

c. Kadar organizacija želi, da bi ugodnosti varnega pristana zajele tudi podatke o človeških virih, prenesene iz Evropske unije za uporabo v okviru zaposlitvenih razmerij, lahko to stori, kadar obstaja zakonsko telo, pristojno za obravnavo pritožb v zvezi s podatki o človeških virih, ki je navedeno v načelih ali prihodnji prilogi k načelom. Organizacija mora to navesti tudi v svoji predložitvi samocertifikacije ter se zavezati, da bo sodelovala z zadevnim organom ali organi EU v skladu z dopolnilnimi načeli glede podatkov o človeških virih in vloge organov za zaščito podatkov, kakor primerno, ter da bo upoštevala nasvet, ki ga bo dobila od teh organov. Organizacija mora Ministrstvu predložiti tudi izvod svoje politike za varstvo zasebnosti človeških virov in informacije o tem, kje je politika zasebnosti na voljo zadevnim zaposlenim.

d. Ministrstvo bo vzdrževalo seznam organizacij v okviru zasebnostnega ščita, ki predložijo popolne samocertifikacije, s čimer bo zagotovilo razpoložljivost ugodnosti zasebnostnega ščita, ter bo letno ažuriralo podatke na seznamu na podlagi letnih predložitev samocertifikacije in uradnih obvestil, ki jih prejme v skladu z dopolnilnim načelom glede reševanja sporov in uveljavljanja. Takšne samocertifikacije se predložijo najmanj enkrat letno, sicer je organizacija odstranjena s seznama zasebnostnega ščita in ji ugodnosti zasebnostnega ščita ne bodo več zagotovljene. Seznam zasebnostnega ščita in samocertifikacijske predložitve organizacij bodo na voljo javnosti. Vse organizacije, ki jih Ministrstvo uvrsti na seznam zasebnostnega ščita, morajo tudi v ustreznih objavljenih izjavah o svoji politiki zasebnosti navesti, da spoštujejo načela zasebnostnega ščita. Če je politika zasebnosti

organizacije na voljo na spletu, mora vključevati povezavo na spletno stran Ministrstva v zvezi z zasebnostnim ščitom in povezavo na spletno stran ali obrazec za predložitev pritožbe neodvisnega pritožbenega mehanizma, ki je na voljo za preiskovanje nerešenih pritožb.

e. Načela zasebnosti začnejo veljati takoj po certifikaciji. Ob priznavanju, da bodo načela vplivala na trgovinska razmerja s tretjimi strankami, organizacije, ki se potrdijo v okviru zasebnostnega ščita v prvih dveh mesecih po datumu začetka veljavnosti okvira, uskladijo obstoječa trgovinska razmerja s tretjimi strankami z načelom odgovornosti za prenos tretjemu čim prej, vendar najpozneje v devetih mesecih od datuma, na katerega se potrdijo v okviru zasebnostnega ščita. Kadar organizacije v tem vmesnem obdobju prenesejo podatke tretji stranki, (i) uporabijo načeli obvestila in možnosti izbire, ter (ii) kadar se osebni podatki prenesejo tretji stranki, ki nastopa v vlogi posrednika, zagotovijo, da je posrednik dolžan zagotoviti vsaj enako raven zaščite, kot jo predpisujejo načela.

f. Organizacija mora za vse osebne podatke, ki jih prejme iz EU na podlagi zasebnostnega ščita, uporabiti načela zasebnostnega ščita. Pri podatkih, ki jih organizacija prejme v času, ko uživa ugodnosti zasebnostnega ščita, zavezanost k načelom zasebnostnega ščita ni časovno omejena. Ta zaveza pomeni, da bo organizacija uporabljala načela, dokler take podatke hrani, uporablja ali razkriva, četudi pozneje iz kakršnega koli razloga izstopi iz zasebnostnega ščita. Organizacija, ki izstopi iz zasebnostnega ščita, a želi hraniti takšne podatke, mora vsako leto pri Ministrstvu potrditi svojo zavezo, da bo še naprej spoštovala načela ali zagotovila „ustrezno“ zaščito za informacije z drugimi dovoljenimi sredstvi (na primer, s pogodbo, ki v celoti odraža zahteve ustreznih standardnih pogodbenih klavzul, ki jih sprejema Evropska komisija); sicer mora organizacija vrniti ali izbrisati informacije. Organizacija, ki izstopi iz zasebnostnega ščita. mora iz ustrezne politike zasebnosti odstraniti vse sklice na zasebnostni ščit, ki nakazujejo, da organizacija še naprej dejavno sodeluje v zasebnostnem ščitu in je upravičena do njegovih ugodnosti.

g. Organizacija, ki zaradi združitve ali prevzema preneha obstajati kot ločena pravna oseba, mora o tem vnaprej uradno obvestiti Ministrstvo. V uradnem obvestilu mora tudi navesti, ali bo prevzemna ali združena organizacija (i) še naprej zavezana k načelom zasebnostnega ščita po zakonu o prevzemu ali združitvi ali (ii) se bo odločila, da samocertificira zavezanost k načelom zasebnostnega ščita ali uvede druge varovalke, kot je pisni sporazum, ki bo zagotovil zavezanost k načelom. Kadar se ne uporabljata ne (i) ne (ii), se morajo takoj zbrisati vsi osebni podatki, ki so bili pridobljeni v okviru zasebnostnega ščita.

h. Kadar organizacija iz kakršnega koli razloga izstopi iz zasebnostnega ščita, mora odstraniti vse izjave, ki nakazujejo, da ta še naprej sodeluje v zasebnostnem ščitu ali je upravičena do ugodnosti zasebnostnega ščita. Prav tako je treba odstraniti certifikacijsko oznako zasebnostnega ščita EU-ZDA, če je uporabljena. Za vsako zavajanje širše javnosti v zvezi z zavezanostjo k načelom zasebnostnega ščita lahko Zvezna komisija za trgovino ali drug pristojni državni organ ukrepa proti kršitvi. Zavajanje Ministrstva se lahko kaznuje po zakonu o lažnih navedbah (False Statements Act) (člen 1001 naslova 18 zakonodajne zbirke ZDA).

7. **Preverjanje**

a. Organizacije morajo zagotoviti postopke za preverjanje resničnosti izjav in zatrjevanj, ki jih dajo organizacije glede svojih praks zasebnosti v okviru zasebnostnega ščita, ter izvajanja teh praks na naveden način in v skladu z načeli zasebnostnega ščita.

b. Da organizacija izpolni zahteve preverjanja iz načela pritožbenega mehanizma, uveljavljanja in odgovornosti, mora takšne izjave in zatrjevanja preveriti s samoocenjevanjem ali zunanjim pregledom skladnosti z načeli.

c. Pri samoocenjevanju mora tako preverjanje pokazati, da je objavljena politika organizacije glede zasebnosti osebnih podatkov, prejetih iz EU, točna, celovita, prikazana na vidnem mestu, v celoti izvedena in dostopna. Pokazati mora tudi, da je njena politika zasebnosti v skladu z načeli zasebnostnega ščita; da so posamezniki obveščeni o kakršnem koli notranjem mehanizmu organizacije za obravnavo pritožb in o neodvisnih mehanizmih, prek katerih se lahko pritožijo; da je vzpostavila postopke za izobraževanje zaposlenih o izvajanju politike ter za disciplinske ukrepe v primeru kršitve te politike; ter da je vzpostavila notranje postopke za redno

objektivno pregledovanje usklajenosti z zgoraj navedenim. Izjavo o samooceni mora podpisati vodstveni delavec ali drug pooblaščeni predstavnik organizacije vsaj enkrat na leto in mora biti na voljo posameznikom na njihovo zahtevo ali v okviru preiskave ali pritožbe zaradi neskladnosti z načeli.

d. Kadar se organizacija odloči za zunanji pregled skladnosti z načeli, mora tak pregled pokazati, da je njena politika zasebnosti v zvezi z osebnimi podatki, prejetimi iz EU, v skladu z načeli zasebnostnega ščita, da organizacija ravna v skladu z njo ter da so posamezniki obveščeni o mehanizmih za pritožbe. Metode pregledovanja so neomejene in lahko obsegajo revizijo, naključne preglede, uporabo „vab“ ali tehnoloških orodij. Izjavo o uspešno končanem zunanjem pregledu mora podpisati bodisi izvajalec pregleda bodisi vodstveni delavec ali drug pooblaščeni predstavnik organizacije vsaj enkrat na leto in mora biti na voljo posameznikom na njihovo zahtevo ali organom za preiskavo ali pritožbe zaradi skladnosti z načeli.

e. Organizacije morajo voditi evidenco o svojem izvajanju prakse zasebnosti v okviru zasebnostnega ščita in jo v primeru preiskave ali pritožbe zaradi neskladnosti izročiti neodvisnemu organu, ki je pristojen za preiskavo pritožb, ali agenciji, ki je pristojna za obravnavo nepoštenih in goljufivih praks. Organizacije se morajo prav tako hitro odzvati na poizvedbe in druge zahteve za informacije iz Ministrstva v zvezi z zavezanostjo organizacije k spoštovanju načel.

8. **Dostop**

a. Načelo dostopa v praksi

i. Po načelih zasebnostnega ščita je pravica do dostopa temeljna za varstvo zasebnosti. Posameznikom zlasti omogoča, da preverijo točnost svojih podatkov, ki jih hrani organizacija. Načelo dostopa pomeni, da imajo posamezniki pravico:

1. pridobiti od organizacije potrditev o tem, ali organizacija obdeluje njihove osebne podatke ali ne ([1]);

2. da jim sporočijo takšne podatke, da lahko preverijo njihovo točnost in zakonitost obdelave; in

3. da spremenijo, popravijo ali izbrišejo podatke, kadar so ti netočni ali obdelani ob kršitvi načel.

ii. Posameznikom ni treba upravičevati zahtev za dostop do njihovih osebnih podatkov. Organizacije naj pri odzivu na posameznikovo zahtevo po dostopu najprej pogledajo težave, ki so vodile do zahteve. Če je na primer zahteva po dostopu nejasna in se nanaša na več področij, lahko organizacija v pogovoru s posameznikom poskuša bolje razumeti motiv za njegovo zahtevo ter poišče ustrezne podatke. Organizacija lahko poizve, na katere dele organizacije se je posameznik obrnil ali na katere vrste podatkov ali njihovo uporabo se nanaša zahteva po dostopu.

iii. V skladu s temeljno naravo pravice do dostopa bi si organizacije morale vedno dobronamerno prizadevati zagotoviti dostop. Na primer kadar je treba določeno informacijo zavarovati in jo je mogoče zlahka ločiti od drugih osebnih informacij, na katere se nanaša zahteva po dostopu, mora organizacija prekriti zaščiteno informacijo in dati na voljo preostale podatke. Če organizacija ugotovi, da je treba v določenem posebnem primeru omejiti dostop, mora posamezniku, ki ga zahteva, pojasniti razloge za svojo odločitev in navesti ime službe za dajanje nadaljnjih informacij.

b. Stroški in izdatki za zagotovitev dostopa

i. Pravico dostopa do osebnih podatkov je mogoče omejiti v izjemnih okoliščinah, kjer bi bile kršene zakonite pravice drugih oseb ali kjer bi bili stroški ali izdatki za zagotovitev dostopa nesorazmerni s tveganji za zasebnost posameznika v zadevnem primeru. Stroški in izdatki so pomemben dejavnik, ki ga je treba upoštevati, vendar niso prevladujoči dejavniki pri ugotavljanju, ali je zagotovitev dostopa razumna ali ne.

([1]) Organizacija mora odgovoriti na zahteve posameznika v zvezi z nameni obdelave, kategorijami zadevnih osebnih podatkov in prejemniki ali kategorijami prejemnikov, katerim se razkrijejo podatki.

ii. Na primer, če se bodo osebne informacije uporabile za odločitve, ki bodo pomembno vplivale na posameznika (npr. zavrnitev ali dodelitev pomembnih ugodnosti, kot so zavarovanje, hipoteka in zaposlitev), potem mora organizacija v skladu z drugimi določbami teh dopolnilnih načel razkriti navedene podatke, četudi je zagotovitev njihovega dostopa razmeroma težka ali draga. Če zahtevane osebne informacije niso občutljive ali se ne uporabijo za odločitve, ki bodo pomembno vplivale na posameznika, temveč so dostopne in poceni, mora organizacija zagotoviti dostop do takih informacij.

c. Zaupne tržne informacije

i. Zaupne tržne informacije so informacije, ki jih je organizacija zavarovala pred razkritjem, saj bi slednje pomagalo konkurentu na trgu. Organizacije lahko zavrnejo ali omejijo dostop, kadar bi z odobritvijo polnega dostopa razkrile svoje zaupne tržne informacije, kot so v organizaciji narejeni tržni koncepti ali klasifikacije, ali zaupne tržne informacije drugega, kadar zanje velja pogodbena obveznost o zaupnosti.

ii. Kadar je zaupno tržno informacijo mogoče brez težav ločiti od drugih osebnih informacij, na katere se nanaša zahteva po dostopu, mora organizacija na novo prekriti zaupno tržno informacijo in omogočiti dostop do podatkov, ki niso zaupni.

d. Organiziranost podatkovnih zbirk

i. Dostop se lahko zagotovi tako, da organizacija posamezniku razkrije ustrezne osebne informacije, za kar ni potreben dostop posameznika do podatkovne zbirke organizacije.

ii. Dostop je treba zagotoviti samo do osebnih informacij, ki jih hrani organizacija. Načelo dostopa samo po sebi ne obvezuje organizacije, da hrani, vzdržuje, ponovno organizira ali ponovno strukturira datoteke z osebnimi podatki.

e. Kdaj je mogoče omejiti dostop

i. Ker si morajo organizacije vedno v dobri veri prizadevati, da posameznikom zagotovijo dostop do njihovih osebnih podatkov, so okoliščine, v katerih lahko organizacije omejijo tak dostop, omejene, vsak razlog za omejitev dostopa pa mora biti natančno naveden. V skladu z direktivo lahko organizacija omeji dostop do podatkov, samo kadar obstaja verjetnost, da bi njihovo razkritje poseglo v zaščito pomembnih nasprotujočih si javnih interesov, kot je nacionalna varnost, obramba ali javna varnost. Poleg tega se lahko dostop zavrne, kadar se osebni podatki obdelujejo izključno za namene raziskav ali statistike. Drugi razlogi za zavrnitev ali omejitev dostopa so:

1. poseg v izvrševanje ali uveljavljanje prava ali v zasebne pravne interese, vključno s preprečevanjem, preiskovanjem ali odkrivanjem kaznivih dejanj in pravico do poštenega sojenja;

2. razkritje, kadar bi bile kršene zakonite pravice ali pomembni pravni interesi drugih;

3. kršitev zakonskih in drugih poklicnih privilegijev in obveznosti;

4. vplivanje na preiskave o varnosti zaposlenih in pritožbene postopke ali v zvezi z načrtovanjem zamenjav zaposlenih in z reorganizacijo podjetja; ali

5. vplivanje na zaupnost, ki je potrebna v zvezi s spremljanjem, inšpekcijo in nadzornimi funkcijami, povezanimi s trdnim upravljanjem, ali v prihodnosti ali tekočih pogajanjih, v katera je vključena organizacija.

ii. Organizacija, ki se sklicuje na izjemo, mora dokazati potrebo po njej ter navesti razloge za omejitev dostopa in ime službe za dajanje nadaljnjih informacij posameznikom.

f. Pravica do pridobivanja potrditve in zaračunavanja pristojbine za pokrivanje stroškov za zagotovitev dostopa

i. Posameznik ima pravico pridobiti potrditev o tem, ali ima ta organizacija osebne podatke, ki se nanašajo nanj. Posameznik ima tudi pravico, da mu sporočijo njegove osebne podatke. Organizacija lahko zaračuna pristojbino, ki ni previsoka.

ii. Zaračunavanje pristojbine je lahko upravičeno, denimo, kadar so zahteve za dostop očitno previsoke, zlasti zaradi njihove ponavljajoče narave.

iii. Dostopa se ne sme zavrniti zaradi stroškov, če jih je posameznik pripravljen plačati.

g. Ponavljajoče in nadležne zahteve za dostop

Organizacija lahko postavi razumne omejitve glede številka poskusov v določenem obdobju, v katerem bodo izpolnjene zahteve za dostop nekega posameznika. Pri postavljanju takšnih omejitev mora organizacija upoštevati takšne dejavnike, kot je pogostost posodabljanja informacij, namen njihove uporabe in njihova narava.

h. Goljufive zahteve za dostop

Organizaciji ni treba zagotoviti dostopa, dokler nima v rokah dovolj podatkov, da lahko potrdi istovetnost osebe, ki zahteva dostop.

i. Časovni okvir za odgovore

Organizacije morajo odgovoriti na zahteve za dostop v razumnem roku, na razumen način in v obliki, ki je razumljiva posamezniku. Organizacija, ki redno zagotavlja informacije posameznikom, na katere se osebni podatki nanašajo, lahko izpolni posamezno zahtevo za dostop z rednim razkritjem, če to ne pomeni čezmerne zamude.

9. **Podatki o človeških virih**

a. Kritje zasebnostnega ščita

i. Kadar organizacija v EU prenese osebne podatke o svojih zaposlenih (nekdanjih ali sedanjih), zbrane v okviru zaposlitvenega razmerja, matičnemu, odvisnemu ali neodvisnemu izvajalcu storitev v Združenih državah, ki sodeluje v okviru zasebnostnega ščita, veljajo za prenos ugodnosti zasebnostnega ščita. V takih primerih velja za zbiranje in obdelavo podatkov pred prenosom nacionalno pravo države EU, v kateri so bili zbrani, pri prenosu pa je treba spoštovati vse pogoje in omejitve po navedenem pravu.

ii. Načela zasebnostnega ščita se uporabljajo samo za prenos ali dostop do podatkov, ki so individualno določeni ali določljivi. Pri statističnem poročanju, ki temelji na zbirnih podatkih o zaposlenosti, in ne vsebuje osebnih podatkov ali vključuje uporabo anonimnih podatkov, se vprašanje varstva zasebnosti ne pojavlja.

b. Uporaba načel obvestila in možnosti izbire

i. Organizacija ZDA, ki je dobila podatke o zaposlenih iz EU v okviru zasebnostnega ščita, jih lahko razkrije tretji stranki ali uporabi za drugačne namene samo v skladu z načeloma obvestila in možnosti izbire. Na primer, kadar organizacija namerava uporabiti podatke, zbrane v zaposlitvenem razmerju, za namene, ki niso povezani z zaposlitvenim razmerjem, kot so tržne komunikacije, mora organizacija ZDA pred tem prizadetim posameznikom zagotoviti predpisano možnost izbire, razen če so že odobrili uporabo podatkov v take namene. Taka uporaba ne sme biti nezdružljiva s prvotnimi nameni, zaradi katerih so bili osebni podatki zbrani ali jih je posameznik pozneje odobril. Poleg tega se take možnosti izbire ne smejo izkoristiti za omejevanje zaposlitvenih možnosti ali za sankcioniranje takih zaposlenih.

ii. Treba je navesti, da nekateri splošno uporabni pogoji za prenos iz nekaterih držav članic EU, lahko izključijo drugačno uporabo takih podatkov tudi po prenosu v državah zunaj EU, in take pogoje bo treba spoštovati.

iii. Poleg tega bi si morali delodajalci razumno prizadevati ustreči prednostnim pravicam zaposlenih po zasebnosti. Sem sodi na primer omejitev dostopa do osebnih podatkov, anonimnost nekaterih podatkov ali uporaba šifer in psevdonimov, kadar se za namene upravljanja ne zahtevajo dejanska imena.

iv. Organizaciji ni treba spoštovati načela obvestila in možnosti izbire v obsegu in obdobju, potrebnem za preprečitev oškodovanja zmožnosti organizacije pri odločitvah o napredovanju delavcev, imenovanjih in drugih podobnih zaposlitvenih odločitvah.

c. Uporaba načela dostopa

Dopolnilno načelo o dostopu določajo smernice o razlogih, ki lahko v okviru človeških virov upravičijo zavrnitev ali omejitev dostopa na zahtevo posameznika. Delodajalci v Evropski uniji morajo seveda ravnati v skladu z lokalnimi predpisi in poskrbeti, da imajo zaposleni v Evropski uniji dostop do takih podatkov, kakor zahteva pravo v njihovih državah, ne glede na lokacijo obdelave in hrambe podatkov. Režim zasebnostnega ščita zahteva, da organizacija, ki v Združenih državah Amerike obdeluje take podatke, sodeluje pri zagotavljanju takšnega dostopa bodisi neposredno bodisi prek delodajalca v EU.

d. Uveljavljanje

i. Dokler se osebne informacije uporabljajo samo v okviru zaposlitvenega razmerja, je zaposlenemu za podatke v prvi vrsti odgovorna organizacija v EU. Iz tega sledi, da je treba, kadar se zaposleni iz EU pritožijo zaradi kršenja njihovih pravic do zaščite podatkov ter niso zadovoljni z rezultati postopkov notranjega pregleda in pritožbenih postopkov (ali drugih predvidenih pritožbenih postopkov v okviru kolektivne pogodbe), te zaposlene napotiti na državni ali nacionalni organ za zaščito podatkov ali delovnopravni organ, ki je pristojen tam, kjer delajo zaposleni. Sem sodijo tudi primeri, ko je za zatrjevano zlorabo osebnih informacij odgovorna organizacija ZDA, ki je prejela informacije od delodajalca, in tako vključuje domnevno kršitev načel zasebnostnega ščita. To bo najbolj učinkovit način za uskladitev pogosto prekrivajočih se pravic in obveznosti, ki jih določajo lokalno delovno pravo in kolektivne pogodbe ter pravo o zaščiti podatkov.

ii. Organizacija ZDA, ki je pristopila k zasebnostnemu ščitu in uporablja podatke o človeških virih, prenesene iz EU v okviru zaposlitvenih razmerij, ter želi, da za ta prenos veljajo načela zasebnostnega ščita, se mora zato zavezati, da bo v takih primerih sodelovala v preiskavah pristojnih organov EU in upoštevala njihov nasvet.

e. Uporaba načela odgovornosti za prenos tretjemu

Za občasne potrebe, povezane z zaposlovanjem, organizacije v zasebnostnem ščitu v zvezi z osebnimi podatki, ki se prenesejo v okviru zasebnostnega ščita, kot je rezervacija leta, hotelske sobe ali zavarovalno kritje, se lahko osebni podatki manjšega števila zaposlenih prenesejo upravljavcem brez uporabe načela dostopa ali sklenitve pogodbe s tretjim upravljavcem, kakor je sicer predpisano v okviru načela odgovornosti za prenos tretjemu, pod pogojem, da je organizacija v zasebnostnem ščitu izpolnila načeli obvestila in možnosti izbire.

10. **Obvezne pogodbe za prenos tretjemu**

a. Pogodbe za obdelavo podatkov

i. Kadar se osebni podatki prenesejo iz EU v Združene države zgolj zaradi njihove obdelave, je potrebna pogodba ne glede na to, ali izvajalec obdelave sodeluje v zasebnostnem ščitu.

ii. Od upravljavcev podatkov v EU se vedno zahteva podpis pogodbe, kadar se podatki prenašajo zgolj zaradi obdelave, bodisi da se obdelujejo znotraj bodisi zunaj EU, in ne glede na to, ali izvajalec obdelave sodeluje v zasebnostnem ščitu ali ne. Namen pogodbe je zagotoviti, da izvajalec obdelave:

1. deluje samo po navodilih upravljavca;

2. zagotavlja ustrezne tehnične in organizacijske ukrepe za zaščito osebnih podatkov pred slučajnim ali nezakonitim uničenjem ali slučajno izgubo, predelavo, nepooblaščenim razkritjem ali dostopom, in razume, ali je prenos tretjemu dovoljen; in

3. upošteva naravo obdelave, pomaga upravljavcu pri odgovorih posameznikom, ki uveljavljajo svoje pravice po načelih.

iii. Ker pristopnice zasebnostnega ščita zagotavljajo ustrezno zaščito podatkov, se za pogodbe, sklenjene s pristopnicami zasebnostnega ščita samo zaradi obdelave podatkov, ne zahteva predhodno dovoljenje (ali pa bodo države članice EU tako dovoljenje dale avtomatično), kakršno se zahteva za pogodbe s prejemniki podatkov, ki niso pristopili k zasebnostnemu ščitu ali kako drugače ne zagotavljajo ustrezne zaščite podatkov.

b. Prenosi znotraj skupine odvisnih družb ali subjektov

Pri prenosu osebnih informacij med dvema upravljavcema znotraj skupine odvisnih družb ali subjektov pogodba po načelu odgovornosti za prenos tretjemu ni vedno potrebna. Upravljavci podatkov v skupini odvisnih družb ali subjektov lahko takšne prenose utemeljijo na drugih instrumentih, kot so zavezujoča poslovna pravila EU ali drugi instrumenti znotraj skupine (npr. programi skladnosti in nadzora), pri čemer zagotovijo neprekinjeno zaščito osebnih informacij po načelih zasebnostnega ščita. V primeru takih prenosov organizacija v zasebnostnem ščitu ostane odgovorna za spoštovanje načel zasebnostnega ščita.

c. Prenosi med upravljavci

Pri prenosih med upravljavci ni potrebno, da je upravljavec, ki prejme podatke, organizacija v zasebnostnem ščitu ali da ima neodvisni pritožbeni mehanizem. Organizacija v zasebnostnem ščitu mora skleniti pogodbo s tretjim upravljavcem, ki prejme podatke, s katero zagotovi enako raven zaščite, kakor je na voljo po zasebnostnem ščitu, pri čemer ni nujno, da je tretji upravljavec organizacija v zasebnostnem ščitu ali da ima neodvisni pritožbeni mehanizem, pod pogojem, da ima na razpolago enakovredni mehanizem.

11. **Reševanje sporov in uveljavljanje**

a. Načelo pritožbenega mehanizma, uveljavljanja in odgovornosti navaja zahteve za uveljavljanje zasebnostnega ščita. Načine izpolnjevanja zahtev iz točke (a)(ii) tega načela določa dopolnilno načelo o preverjanju. To dopolnilno načelo obravnava točki (a)(i) in (a)(iii), ki zahtevata neodvisne pritožbene mehanizme. Ti mehanizmi so lahko različni, morajo pa izpolnjevati zahteve načela pritožbenega mehanizma, uveljavljanja in odgovornosti. Organizacije izpolnijo te zahteve z: (i) usklajenostjo ravnanja s programi varstva zasebnosti zasebnega sektorja, ki v svojih pravilih vsebujejo načela zasebnostnega ščita in vključujejo učinkovite mehanizme uveljavljanja, kakor so opisani v načelu pritožbenega mehanizma, uveljavljanja in odgovornosti; (ii) usklajenostjo ravnanja z zakonskimi ali z drugimi predpisi predvidenimi nadzornimi organi, ki zagotavljajo obravnavo posameznikovih pritožb in reševanje sporov; ali (iii) zavezo za sodelovanje z organi za zaščito podatkov v Evropski uniji ali z njihovimi pooblaščenimi predstavniki.

b. Ta seznam je ilustrativen in ne omejuje. Zasebni sektor lahko oblikuje tudi dodatne mehanizme za zagotovitev uveljavljanja, če izpolnjujejo zahteve načela pritožbenega mehanizma, uveljavljanja in odgovornosti ter

dopolnilnih načel. Treba je paziti, da so zahteve načela pritožbenega mehanizma, uveljavljanja in odgovornosti dodatek k zahtevi, da mora biti samourejanje izvedljivo po členu 5 Federal Trade Commission Act, ki prepoveduje nepošteno in goljufivo ravnanje, ali drugem zakonu ali predpisu, ki prepoveduje takšno ravnanje.

c. Da bi pomagale zagotoviti izpolnjevanje zavez v okviru zasebnostnega ščita in podprle upravljanje programa, morajo organizacije in njihovi neodvisni pritožbeni mehanizmi na zahtevo Ministrstva zagotoviti informacije v zvezi z zasebnostnim ščitom. Poleg tega morajo organizacije hitro odgovoriti na pritožbe v zvezi z njihovim izpolnjevanjem načel, ki so jih Ministrstvu predložili organi za zaščito podatkov. Odgovor mora obravnavati, ali je pritožba utemeljena in, če je, na kakšen način bo organizacija odpravila težavo. Ministrstvo bo zaščitilo zaupnost informacij, ki jih prejme v skladu z zakonodajo ZDA.

d. Pritožbeni mehanizmi

i. Potrošnike je treba spodbujati, da se s svojimi pritožbami najprej obrnejo na ustrezno organizacijo in šele nato uporabijo neodvisne pritožbene mehanizme. Organizacije morajo odgovoriti potrošniku v 45 dneh od prejema pritožbe. Neodvisnost pritožbenega mehanizma je konkretno vprašanje, na katerega se lahko odgovori predvsem z nepristranskostjo, pregledno sestavo in financiranjem ter z dokazi o preteklem poslovanju. Kakor zahteva načelo pritožbenega mehanizma, uveljavljanja in odgovornosti, mora biti pritožbeni mehanizem za posameznika zlahka dostopen in brezplačen. Službe za reševanje sporov morajo proučiti vse pritožbe, ki jih prejmejo od posameznikov, razen kadar so očitno neutemeljene in neresne. To ne izključuje možnosti, da organizacija, ki izvaja pritožbeni mehanizem, vzpostavi izločitvene pogoje, vendar morajo biti ti pogoji pregledni in upravičeni (na primer izključitev pritožb, ki ne sodijo na področje uporabe programa ali jih mora preučiti drug forum) ter ne smejo spodkopavati zavezanosti k proučevanju zakonitih pritožb. Pritožbeni mehanizmi morajo poleg tega zagotoviti, da posamezniki ob vložitvi pritožbe dobijo celotne in zlahka dostopne informacije o postopkih reševanja sporov. Takšna informacija mora v skladu z načeli zasebnostnega ščita vsebovati obvestilo o praksi varstva zasebnosti tega mehanizma. Pritožbeni mehanizmi morajo tudi sodelovati pri oblikovanju sredstev, ki lajšajo postopek reševanja pritožb, kot je standardni obrazec za pritožbe.

ii. Neodvisni pritožbeni mehanizmi morajo na svojih spletnih straneh vsebovati informacije o načelih zasebnostnega ščita in storitvah, ki jih zagotavljajo v okviru zasebnostnega ščita. Te informacije morajo vsebovati: (1) informacijo o ali povezavo do zahtev načel zasebnostnega ščita za neodvisne pritožbene mehanizme; (2) povezavo do spletne strani Ministrstva v zvezi z zasebnostnim ščitom; (3) pojasnilo, da so njihove storitve v zvezi z reševanjem sporov v okviru zasebnostnega ščita za posameznike brezplačne; (4) opis načina za vložitev pritožbe, povezane z zasebnostnim ščitom; (5) časovni okvir, v katerem se obravnavajo pritožbe v zvezi z zasebnostnim ščitom; in (6) opis možnih pravnih sredstev.

iii. Neodvisni pritožbeni mehanizmi morajo objaviti letno poročilo, v katerem zagotovijo zbirne statistične podatke v zvezi s svojimi storitvami reševanja sporov. Letno poročilo mora vsebovati: (1) skupno število pritožb v zvezi z zasebnostnim ščitom, prejetih v letu poročanja; (2) vrste prejetih pritožb; (3) ukrepe za kakovost reševanja sporov, kot je čas, potreben za obravnavo pritožb; in (4) izide prejetih pritožb, zlasti število in vrste pravnih sredstev ali naloženih sankcij.

iv. Kakor je določeno v Prilogi I je posamezniku na voljo možnost arbitraže, kjer se pri preostalih zahtevkih ugotovi, ali je organizacija v zasebnostnem ščitu kršila svoje obveznosti do posameznika po načelih in ali je takšna kršitev ostala v celoti ali delno neodpravljena. Ta možnost je na voljo le za te namene. Ta možnost ni na voljo, denimo, v zvezi z izjemami pri načelih ([1]) ali v zvezi z obtožbo glede ustreznosti zasebnostnega ščita. V okviru te možnosti arbitraže je senat zasebnostnega ščita (ki ga sestavlja en ali trije arbitri, kakor se dogovorita stranki) pristojen za odrejanje nedenarnega pravičnega nadomestila glede na vsakega posameznika (kot so dostop, popravek, izbris ali vrnitev zadevnih posameznikovih podatkov), potrebnega za odpravo kršitve načel samo v zvezi s posameznikom. Posamezniki in organizacije v zasebnostnem ščitu bodo lahko zahtevali sodno presojo in izvršitev arbitražnih sklepov v skladu z zakonodajo ZDA, in sicer zveznim zakonom o arbitraži (Federal Arbitration Act).

([1]) Člen I.5 načel.

e. Pravna sredstva in sankcije

Vsako pravno sredstvo, ki ga zagotovi služba za reševanje sporov, bi moralo učinkovati tako, da organizacija, če je to izvedljivo, spremeni ali popravi posledice neizpolnjevanja načel in da so njeni nadaljnji postopki v skladu z načeli ali da se ustavi obdelava osebnih podatkov posameznika, ki je vložil pritožbo. Sankcije morajo biti dovolj stroge, da zagotovijo ravnanje organizacije v skladu z načeli. Razpon različno strogih sankcij bo službam za reševanje sporov omogočil ustrezen odziv na različne stopnje neizpolnjevanja načel. Sankcije morajo vključevati javno objavo ugotovitev o neizpolnjevanju načel in zahtevo za izbris podatkov v nekaterih okoliščinah ([1]). Druge sankcije lahko vključujejo tudi začasni odvzem in odstranitev pečata, odškodnine za posameznike za škodo, nastalo zaradi neizpolnjevanja načel, ter sodno prepoved. Kadar organizacije v zasebnostnem ščitu ne upoštevajo odločitev služb, morajo službe za reševanje sporov in samourejevalne službe iz zasebnega sektorja o tem obvestiti državne organe z ustreznimi pristojnostmi ali sodišča in Ministrstvo.

f. Ukrepi Zvezne komisije za trgovino

Zvezna komisija za trgovino se je zavezala, da bo prednostno pregledovala predložitve o domnevnem neizpolnjevanju načel, ki jih preme od: (i) organizacij s samourejevalnim sistemom varstva zasebnosti in drugih neodvisnih organov za reševanje sporov; (ii) držav članic EU; in (iii) Ministrstva, da bi ugotovila, ali je bil kršen člen 5 zakona o FTC, ki prepoveduje nepoštena in goljufiva dejanja in ravnanje v trgovini. Če Zvezna komisija za trgovino ugotovi, da obstaja razlog za prepričanje, da je bil kršen člen 5, lahko zadevo reši tako, da izda upravni odlok, ki prepoveduje sporno ravnanje, ali da se pritoži na zvezno okrožno sodišče, kjer lahko, če uspe, doseže odločbo zveznega sodišča z enakim učinkom. To vključuje lažne navedbe organizacij, ki niso več na seznamu zasebnostnega ščita ali se nikoli niso samocertificirale pri Ministrstvu, glede zavezanosti k načelom zasebnostnega ščita ali sodelovanja v zasebnostnem ščitu. Zvezna komisija za trgovino lahko uveljavi denarne kazni za kršitev upravnega odloka o prepovedi in lahko sproži civilni ali kazenski postopek za kršitev odločbe zveznega sodišča. Zvezna komisija za trgovino obvesti Ministrstvo o vsakem takem ukrepu. Ministrstvo spodbuja druga vladna telesa, da ga obvestijo o končnem razpletu predloženih zadev in drugih odločitev v zvezi z izpolnjevanjem načel zasebnostnega ščita.

g. Vztrajno neizpolnjevanje načel

i. Pri vztrajnem neizpolnjevanju načel organizacija ni več upravičena do ugodnosti zasebnostnega ščita. Organizacije, ki vztrajno ne izpolnjujejo načel, bo Ministrstvo zbrisalo s seznama zasebnostnega ščita in morajo vrniti ali zbrisati osebne informacije, ki so jih prejele v okviru zasebnostnega ščita.

ii. O vztrajnem neizpolnjevanju načel govorimo, kadar organizacija, ki se je samocertificirala pri Ministrstvu, noče ravnati v skladu s končno ugotovitvijo službe s samourejevalnim sistemom za varstvo zasebnosti, neodvisne službe za reševanje sporov ali vladne službe ali kadar taka služba ugotovi, da organizacija tako pogosto ravna proti načelom, da njena izjava o usklajenosti z načeli ni več verodostojna. V teh primerih mora organizacija o takih dejstvih takoj obvestiti Ministrstvo. Če tega ne stori, se lahko kaznuje po zakonu o lažnih navedbah (False Statements Act) (člen 1001 naslova 18 zakonodajne zbirke ZDA). Izstop organizacije iz samourejevalnega programa za varstvo zasebnosti v zasebnem sektorju ali neodvisnega mehanizma za reševanje sporov le-te ne razbremeni obveznosti do spoštovanja načel in bi pomenil vztrajno neizpolnjevanje načel.

iii. Ministrstvo bo s svojega seznama zasebnostnega ščita odstranilo organizacijo na podlagi vsakega uradnega obvestila o vztrajnem neizpolnjevanju načel, ki ga prejme od same organizacije, službe s samourejevalnim sistemom za varstvo zasebnosti ali od vladne službe, vendar šele po izteku 30-dnevnega roka, v katerem ima

([1]) Službe za reševanje sporov po svoji presoji odločijo, v katerih okoliščinah bodo uporabile te sankcije. Občutljivost zadevnih podatkov je dejavnik, ki ga je treba upoštevati pri odločitvi o zahtevi za izbris podatkov, tak dejavnik je tudi, ali je organizacija zbirala, uporabljala ali razkrivala podatke v očitnem nasprotju z načeli zasebnostnega ščita.

organizacija, ki ni ravnala v skladu z načeli, možnost odziva. Seznam zasebnostnega ščita, ki ga vodi Ministrstvo, bo torej jasno pokazal, katerim organizacijam so zagotovljene in katerim organizacijam niso več zagotovljene ugodnosti zasebnostnega ščita.

iv. Organizacija, ki se prijavi za sodelovanje v samourejevalni službi z namenom, da izpolni pogoje za ponovno sodelovanje v zasebnostnem ščitu, mora navedeni službi predložiti vse podatke o svojem prejšnjem sodelovanju v zasebnostnem ščitu.

12. **Možnost izbire – časovna omejitev zavrnitve**

a. Splošni namen načela izbire je zagotoviti, da se osebni podatki uporabljajo in razkrivajo v skladu s pričakovanji in odločitvami posameznika. Posameznik mora torej vedno imeti možnost „zavrnitve“, da se njegovi osebni podatki uporabljajo za neposredno trženje, ob upoštevanju razumnih rokov, ki jih postavi organizacija in so potrebni za učinkovito upoštevanje zavrnitve. Organizacija lahko tudi od posameznika, ki se je odločil za zavrnitev, zahteva, da z zadostnimi podatki potrdi svojo istovetnost. V Združenih državah lahko posamezniki uresničijo to možnost prek osrednjega programa „zavrnitve“, kot je Direct Marketing Association's Mail Preference Service. Organizacije, ki sodelujejo v Direct Marketing Association's Mail Preference Service, bi morale na razpoložljivost teh storitev opozarjati tiste potrošnike, ki ne želijo prejemati trgovskih informacij. Vsekakor bi moral imeti posameznik za uresničitev te možnosti na voljo dostopen in stroškovno ugoden mehanizem.

b. Podobno lahko organizacija uporabi informacije za nekatere namene neposrednega trženja, kadar ni izvedljivo, da bi posamezniku zagotovila možnost zavrnitve pred uporabo podatkov, če organizacija posamezniku takoj ponudi možnost, da sočasno (na zahtevo pa kadar koli) zavrne (brez stroškov za posameznika) nadaljnje prejemanje neposrednih tržnih komunikacij in organizacija ravna v skladu s posameznikovimi željami.

13. **Potovalne informacije**

a. Podatki o rezervacijah na potniških letalih in druge potovalne informacije, kot so podatki o pogostih letalskih ali hotelskih rezervacijah in posebni oskrbi, na primer o posebnih obrokih zaradi verskih zahtev ali fizični pomoči, se lahko prenesejo organizacijam zunaj Evropske unije pod različnimi okoliščinami. Po členu 26 direktive se lahko osebni podatki prenesejo v tretjo državo, ki ne zagotavlja ustrezne ravni varstva podatkov v smislu člena 25(2), pod pogojem, (i) da je treba zagotoviti storitve, ki jih zahteva potrošnik, ali izpolniti pogoje dogovora, kakršen je dogovor o „pogostem letalskem potniku“; ali (ii) da potrošnik s tem nedvoumno soglaša. Ameriške organizacije, podpisnice zasebnostnega ščita, zagotavljajo ustrezno varstvo osebnih podatkov in torej lahko prejmejo podatke iz Evropske unije, ne da bi jim bilo treba izpolnjevati navedene pogoje ali druge pogoje iz člena 26 Direktive. Ker zasebnostni ščit vključuje posebna pravila za občutljive podatke, se takšni podatki (ki jih je na primer treba zbrati v zvezi z potrošnikovo potrebo po fizični pomoči) lahko prenesejo udeleženkam zasebnostnega ščita. V vsakem primeru pa mora organizacija, ki prenaša podatke, spoštovati pravo države članice EU, v kateri deluje, ki lahko med drugim vsebuje tudi posebne pogoje glede ravnanja z občutljivimi podatki.

14. **Farmacevtski in medicinski izdelki**

a. Uporaba zakonov držav članic EU ali načel zasebnostnega ščita

Pravo držav članic EU se uporablja za zbiranje osebnih podatkov in za vsako njihovo obdelavo, ki se izvede pred prenosom v Združene države. Načela zasebnostnega ščita se uporabijo takoj, ko so podatki preneseni v Združene države. Podatki, ki se uporabljajo za farmacevtske raziskave in druge namene, morajo biti po potrebi brezimni.

b. Prihodnje znanstvene raziskave

i. Osebni podatki, pridobljeni v posebnih medicinskih ali farmacevtskih raziskovalnih študijah, imajo pogosto dragoceno vlogo v prihodnjih znanstvenih raziskovanjih. Kadar se osebni podatki, zbrani za eno raziskavo, prenesejo organizaciji ZDA v zasebnostnem ščitu, lahko organizacija uporabi te podatke za nove znanstveno-raziskovalne dejavnosti, če sta bila najprej zagotovljena primerno obvestilo in možnost izbire. Takšno obvestilo mora vsebovati informacijo o vseh prihodnjih posebnih uporabah podatkov, kot so občasno spremljanje, sorodne študije ali trženje.

ii. Razume se, da ni mogoče podrobno navesti vseh prihodnjih uporab podatkov, ker lahko uporaba podatkov za novo raziskavo izhaja iz novega razumevanja prvotnih podatkov, novih medicinskih odkritij in napredka ter razvoja na področju javnega zdravja in urejanja. Po potrebi mora zato obvestilo vsebovati pojasnilo, da se osebni podatki v prihodnosti morda uporabijo za medicinske in farmacevtske raziskave, ki niso predvidene. Če uporaba podatkov ni v skladu s splošnimi raziskovalnimi nameni, za katere so bili osebni podatki prvotno zbrani ali za katere je posameznik naknadno dal soglasje, je treba pridobiti novo soglasje.

c. Umik iz kliničnega poskusa

Udeleženci se lahko kadar koli odločijo za umik iz kliničnega poskusa ali so zaprošeni, da tako storijo. Vsi osebni podatki, ki so zbrani pred umikom, se lahko še naprej obdelujejo skupaj z drugimi podatki, zbranimi med kliničnim poskusom, vendar samo, če je bil udeleženec jasno seznanjen s tem, ko je privolil v sodelovanje pri poskusu.

d. Prenosi za regulativne in nadzorne namene

Podjetja za farmacevtske in medicinske pripomočke smejo zagotoviti osebne podatke iz kliničnih poskusov, izvedenih v EU, nadzornim organom v Združenih državah za regulativne in nadzorne namene. Podobni prenosi so dovoljeni tudi strankam, ki niso nadzorni organi, kot so sedeži podjetij in drugi raziskovalci, v skladu z načeloma obvestila in možnosti izbire.

e. „Slepe“ študije

i. Zaradi zagotovitve objektivnosti pri mnogih kliničnih poskusih udeleženci, pa tudi raziskovalci, nimajo dostopa do podatkov o vrsti zdravljenja posameznega udeleženca. To bi namreč lahko ogrozilo veljavnost raziskovalne študije in rezultatov. Udeležencem takšnih kliničnih poskusov (imenovanih „slepe“ študije) ni treba zagotoviti dostopa do podatkov o njihovem zdravljenju med poskusom, če je bila ta omejitev obrazložena, ko je udeleženec pristopil k poskusu in bi razkritje takšnih informacij ogrozilo celovitost raziskovalnega dela.

ii. Privolitev udeleženca, da sodeluje pri poskusu pod takšnimi pogoji, je razumen razlog za opustitev pravice do dostopa. Po končanem poskusu in opravljeni analizi rezultatov bi morali udeleženci dobiti dostop do svojih podatkov, če tako zahtevajo. Zahtevati bi jih morali najprej pri zdravniku ali drugem zdravstvenem delavcu, ki je vodil zdravljenje med kliničnim poskusom, potem pa pri nosilni organizaciji.

f. Spremljanje varnosti in učinkovitosti izdelkov

Podjetju za farmacevtske ali medicinske pripomočke ni treba uporabiti načela zasebnostnega ščita o obvestilu, izbiri, odgovornosti za prenos tretjemu in dostopu pri spremljanju varnosti in učinkovitosti svojih izdelkov, vključno s poročanjem o neugodnih dogodkih in sledenjem pacientov/subjektov, ki uporabljajo nekatera zdravila

ali medicinske pripomočke, če spoštovanje načel posega v izpolnjevanje zakonskih zahtev. To velja za poročanje, na primer, zdravstvenih delavcev podjetjem za farmacevtske in medicinske pripomočke, pa tudi za poročanje podjetij za farmacevtske in medicinske pripomočke vladnim agencijam, kot je Food and Drug Administration.

g. Podatki, kodirani s šifrirnim ključem

Ob nastanku raziskovalnih podatkov jih vodja raziskave nespremenljivo kodira z edinstvenimi šifrirnim ključem, tako da ni mogoče odkriti istovetnosti posameznih subjektov podatkov. Farmacevtske družbe, ki so nosilke takih raziskav, ne dobijo šifrirnega ključa. Samo raziskovalec ima edinstveni šifrirni ključ, s katerim lahko v posebnih okoliščinah prepozna subjekt raziskave (na primer, če se zahteva nadaljnja zdravniška pozornost). Pri prenosu tako šifriranih podatkov iz EU v Združene države tako ne gre za prenos osebnih podatkov, za katerega veljajo načela zasebnostnega ščita.

15. **Informacije iz javnih evidenc in javnosti dostopnih podatkov**

a. Organizacija mora pri osebnih podatkih iz javno dostopnih virov uporabiti načela zasebnostnega ščita glede varnosti, neokrnjenosti podatkov in omejitvi namena ter o pritožbenem mehanizmu, uveljavljanju in odgovornosti. Ta načela veljajo tudi za osebne podatke, zbrane iz javnih evidenc, tj. tiste, ki jih hranijo državne agencije ali subjekti na kateri koli ravni in so odprte na vpogled širši javnosti.

b. Pri podatkih iz javnih evidenc ni treba uporabiti načel obvestila, izbire ali odgovornosti za prenos tretjemu, če niso povezani s podatki iz evidenc, ki niso javne, in se spoštujejo vsi pogoji glede vpogleda v podatke, ki jih je določil ustrezni pristojni organ. Prav tako na splošno ni treba uporabiti načel obvestila, izbire ali odgovornosti za prenos tretjemu pri javnosti dostopnih podatkih, razen če evropski pošiljatelj navede, da pri teh podatkih veljajo omejitve, ki zahtevajo, da organizacija uporabi navedena načela pri nameravani uporabi podatkov. Organizacije niso odgovorne za način, kako take podatke uporabljajo tisti, ki jih pridobijo iz objavljenih gradiv. Če se ugotovi, da je organizacija v nasprotju z načeli namenoma objavila osebne podatke, zato da bi ona ali druge organizacije izkoristile te izjeme, organizacija ne bo več upravičena do ugodnosti varnega pristana.

c. Če se ugotovi, da je organizacija v nasprotju z načeli namenoma objavila osebne informacije, zato da bi ona ali druge organizacije izkoristile te izjeme, organizacija ne bo več upravičena do ugodnosti zasebnostnega ščita.

d. Dokler informacije iz javnih evidenc niso povezane z drugimi osebnimi informacijami, ni treba uporabiti načela dostopa (razen manjših delov, ki se uporabljajo za indeksiranje in organiziranje informacij javnih evidenc); vendar se morajo spoštovati vse določbe, ki jih za vpogled določa ustrezni predpis. Kadar pa je podatek iz javnih evidenc povezan z drugimi podatki iz evidenc, ki niso javne, (razen tistih, ki so podrobno navedene zgoraj), mora organizacija zagotoviti dostop do vseh takih podatkov, če zanje ne veljajo druge dovoljene izjeme.

e. Kakor pri podatkih iz javnih evidenc, ni treba zagotoviti dostopa do podatkov, do katerih ima javnost na splošno dostop, razen če so povezani s podatki, ki javnosti niso dostopni. Organizacije, ki se ukvarjajo s prodajo javno dostopnih informacij, lahko zaračunajo svojo običajno pristojbino za izpolnitev zahteve po dostopu. Posamezniki pa lahko zahtevajo dostop do svojih podatkov tudi pri organizaciji, ki je prvotno zbrala podatke.

16. **Zahteve javnih organov za dostop**

a. Da bi zagotovili preglednost v zvezi z zakonitimi zahtevami javnih organov za dostop do osebnih informacij, lahko organizacije v zasebnostnem ščitu prostovoljno izdajo redna poročila o številu zahtev za osebne informacije, ki jih prejmejo od javnih organov za namene kazenskega pregona ali nacionalne varnosti, če so takšna razkritja dovoljena po veljavni zakonodaji.

b. Informacije, ki jih v teh poročilih zagotovijo organizacije v zasebnostnem ščitu, in informacije, ki jih objavi obveščevalna skupnost, in druge informacije je mogoče uporabiti kot podlago za letni skupni pregled delovanja zasebnostnega ščita v skladu z načeli.

c. Zaradi odsotnosti obvestila v skladu s točko (a)(xii) načela obvestila organizaciji ni preprečena ali oslabljena možnost, da se odzove na morebitno zakonito zahtevo.

Priloga I

Arbitražni model

Priloga I določa pogoje, pod katerimi so organizacije v zasebnostnem ščitu dolžne presoditi trditve v skladu z načelom pritožbenega mehanizma, uveljavljanja in odgovornosti. Možnost zavezujoče arbitraže, opisane spodaj, se nanaša na nekatere „preostale“ zahtevke glede podatkov, ki jih krije zasebnostni ščit EU-ZDA. Namen te možnosti je zagotoviti takojšnji neodvisni in pošteni mehanizem na izbiro posameznikov za reševanje zatrjevanih kršitev načel, ki niso bili razrešeni v okviru katerega koli drugega mehanizma zasebnostnega ščita.

A. **Področje uporabe**

Možnost arbitraže je posamezniku na voljo, da pri preostalih zahtevkih ugotovi, ali je organizacija v zasebnostnem ščitu kršila obveznosti do posameznika po načelih in ali je takšna kršitev ostala v celoti ali delno neodpravljena. Ta možnost je na voljo le za te namene. Ta možnost ni na voljo, denimo, v zvezi z izjemami pri načelih ([1]) ali v zvezi z obtožbo glede ustreznosti zasebnostnega ščita.

B. **Razpoložljiva pravna sredstva**

V okviru te možnosti arbitraže je senat zasebnostnega ščita (ki ga sestavlja en ali trije arbitri, kakor se dogovorita stranki) pristojen za odrejanje nedenarnega pravičnega nadomestila glede na vsakega posameznika (kot so dostop, popravek, izbris ali vrnitev zadevnih posameznikovih podatkov), potrebnega za odpravo kršitve načel samo v zvezi s posameznikom. To so edina pooblastila arbitražnega senata v zvezi s pravnimi sredstvi. Ob upoštevanju pravnih sredstev je arbitražni senat dolžan upoštevati druga pravna sredstva, ki so jih odredili že drugi mehanizmi v okviru zasebnostnega ščita. Na voljo ni odškodnin, stroškov, pristojbin ali drugih pravnih sredstev. Vsaka stranka nosi svoje odvetniške stroške.

C. **Predarbitražne zahteve**

Posameznik, ki se odloči uveljaviti možnost arbitraže, mora slediti naslednjim korakom, preden sproži arbitražni zahtevek: (1) predložiti zatrjevano kršitev neposredno organizaciji in ponuditi organizaciji možnost, da reši zadevo v časovnem okviru, določenem v členu III.11(d)(i) načel; (2) uporabiti neodvisni pritožbeni mehanizem v okviru načel, ki je brezplačen za posameznika; in (3) predložiti zadevo prek svojega organa za zaščito podatkov Ministrstvu za trgovino ter slednjemu ponuditi možnost, da po svojih najboljših močeh razreši zadevo v časovnih okvirih, določenih v pismu Uprave za mednarodno trgovino Ministrstva za trgovino, brezplačno za posameznika.

Ta možnost arbitraže ni na voljo, če je posameznikova ista zatrjevana kršitev načel (1) prej bila predmet zavezujoče arbitraže; (2) prej bila predmet pravnomočne sodbe, sprejete v sodnem postopku, v katerem je bil posameznik stranka; ali (3) bila prej poravnana med strankama. Poleg tega te možnosti ni mogoče uveljaviti, če ima organ EU za zaščito podatkov (1) pristojnost po členu III.5 ali III.9 načel; ali (2) pristojnost za reševanje zatrjevane kršitve neposredno z organizacijo. Pooblastilo organa za zaščito podatkov za reševanje istega zahtevka proti upravljavcu podatkov iz EU samo po sebi ne onemogoča uporabe te možnosti arbitraže proti drugi pravni osebi, ki je ne veže pooblastilo organa za zaščito podatkov.

D. **Zavezujoča narava sklepov**

Posameznikova odločitev, da uveljavi to možnost zavezujoče arbitraže, je v celoti prostovoljna. Arbitražni sklepi bodo zavezujoči za vse stranke v arbitražnem postopku. Ob njeni uporabi se posameznik odpove možnosti, da poišče nadomestilo za isto zatrjevano kršitev pri drugem forumu z izjemo, da, v kolikor nedenarno pravično nadomestilo ne odpravi v celoti zatrjevane kršitve, posameznikova uveljavitev arbitraže ne onemogoči zahtevka za odškodnino, ki je sicer na voljo na sodiščih.

([1]) Člen I.5 načel.

E. **Pregled in izvrševanje**

Posamezniki in organizacije v zasebnostnem ščitu bodo lahko zahtevali sodno presojo in izvršitev arbitražnih sklepov v skladu z zakonodajo ZDA, in sicer zveznim zakonom o arbitraži (Federal Arbitration Act ([1])). Vse take zadeve je treba vložiti pri zveznem okrožnem sodišču, ki je krajevno pristojno za primarni kraj poslovanja organizacije v zasebnostnem ščitu.

Ta možnost arbitraže je namenjena reševanju posameznih sporov, namen arbitražnih sklepov pa ni, da služijo kot prepričljiv ali zavezujoč precedens v zadevah, ki vključujejo druge stranke, vključno v prihodnjih arbitražah ali na sodiščih v EU ali ZDA ali v postopkih Zvezne komisije za trgovino.

F. **Arbitražni senat**

Stranke bodo izbrale arbitre s seznama arbitrov, obravnavanega spodaj.

Skladno z veljavno zakonodajo bosta Ministrstvo za trgovino ZDA in Evropska komisija oblikovala seznam vsaj 20 arbitrov, izbranih na podlagi neodvisnosti, integritete in strokovnosti. V zvezi s tem postopkom velja naslednje:

Arbitri:

(1) bodo ostali na seznamu 3 leta, razen v izjemnih razmerah ali z razlogom, njihovo imenovanje pa se lahko podaljša za eno dodatno obdobje 3 let;

(2) ne sprejemajo navodil in niso povezani s katero koli stranko ali organizacijo v zasebnostnem ščitu ali z ZDA, EU ali katero koli državo članico EU ali morebitnim drugim vladnim organom, javnim organom ali organom pregona; in

(3) morajo biti pooblaščeni za opravljanje odvetniškega poklica v ZDA in strokovnjaki za zakonodajo ZDA na področju varstva zasebnosti ter imeti strokovno znanje in izkušnje v zakonodaji EU na področju zaščite podatkov.

G. **Arbitražni postopki**

Skladno z veljavno zakonodajo se bosta Ministrstvo za trgovino in Evropska komisija v roku 6 mesecev od sprejetja sklepa o ustreznosti dogovorila o sprejetju obstoječega ustaljenega niza ameriških arbitražnih postopkov (kot je AAA ali JAMS) za urejanje postopkov pred senatom zasebnostnega ščita v skladu z vsakim od naslednjih stališč:

1. Posameznik lahko sproži zavezujočo arbitražo v skladu z zgornjo določbo glede predarbitražnih zahtev, tako da organizaciji pošlje „obvestilo“. Obvestilo vsebuje povzetek ukrepov, izvedenih po odstavku C, za rešitev zahtevka, opis domnevne kršitve in po izbiri posameznika morebitna dokazila in materiale in/ali pravno razpravo v zvezi z domnevnim zahtevkom.

([1]) Poglavje 2 zveznega zakona o arbitraži (Federal Arbitration Act ali FAA) določa, da „arbitražni sporazum ali arbitražna odločba, ki izhaja iz pogodbenega ali nepogodbenega pravnega razmerja, ki se šteje za poslovnega, vključno s transakcijo, pogodbo ali sporazumom, opisanim v [členu 2 FAA], sodi v okvir Konvencije [o priznavanju in izvrševanju tujih arbitražnih odločb z dne 10. junija 1958, 21 U.S.T. 2519, T.I.A.S. št. 6997 (‚newyorška konvencija')].“ Člen 202 naslova 9 zakonodajne zbirke ZDA. FAA nadalje določa, da „[a] se šteje, da sporazum ali odločba na podlagi takšnega razmerja, v celoti med državljani Združenih držav, ne sodi v okvir [newyorške] konvencije, razen če to razmerje vključuje premoženje v tujini, predvideva učinkovitost ali izvrševanje v tujini ali ima neko drugo razumno povezavo z eno ali več tujimi državami.“ *Id.* V skladu s poglavjem 2 „lahko katera koli stranka v arbitraži uveljavi pri katerem koli sodišču, ki je pristojno po tem poglavju, sklep, ki potrjuje odločbo, kot proti kateri koli drugi stranki v arbitraži. Sodišče potrdi odločbo, razen če ugotovi obstoj enega od razlogov za zavrnitev ali odložitev priznanja ali izvrševanja odločbe, navedene v omenjeni [newyorški] konvenciji.“ *Id.* člen 207. Poglavje 2 nadalje določa, da „imajo okrožna sodišča Združenih držav … izvirno pristojnost nad … tožbo ali postopkom [po newyorški konvenciji] ne glede na sporen znesek.“ *Id.* člen 203.
Poglavje 2 določa tudi, da „Poglavje 1 velja za tožbe in postopke, vložene po tem poglavju, če tisto poglavje ni v nasprotju s tem poglavjem ali [newyorško] konvencijo, kakor so jo ratificirale Združene države.“ *Id.* člen 208. Poglavje 1 pa določa, da „je pisna določba v … pogodbi, ki dokazuje trgovski posel, da se z arbitražo reši spor, ki izhaja iz takšne pogodbe ali posla, ali zavrnitev izvedbe celotnega ali dela pogodbe ali posla, ali v pisnem sporazumu, da se obstoječi spor, ki izhaja iz takšne pogodbe, posla ali zavrnitve, predloži v arbitražo, veljavna, nepreklicna in izvršljiva, razen če obstajajo razlogi, kakor so določeni po zakonu ali v kapitalu za preklic katere koli pogodbe.“ *Id.* člen 2. Poglavje 1 nadalje določa, da „lahko katera koli stranka v arbitraži pri tako določenem sodišču vloži predlog za odločbo, ki potrjuje dodelitev, na podlagi tega pa mora sodišče ugoditi takšni odločbi, razen če je dodelitev razveljavljena, spremenjena ali popravljena, kakor je predpisano v členih 10 in 11 [FAA].“ *Id.* člen 9.

2. Oblikovani bodo postopki, ki bodo zagotovili, da ista zatrjevana kršitev ne postane predmet podvojenih pravnih sredstev ali postopkov.

3. Ukrep Zvezne komisije za trgovino se lahko nadaljuje vzporedno z arbitražo.

4. V teh arbitražah ne sme sodelovati noben predstavnik ZDA, EU ali katere koli države članice EU ali drugega vladnega organa, javnega organa ali organa pregona pod pogojem, da lahko na zahtevo posameznika iz EU organi za zaščito podatkov EU zagotovijo pomoč samo pri pripravi obvestila, ne smejo pa imeti dostopa do ugotavljanja ali morebitnega drugega gradiva v zvezi s temi arbitražami.

5. Kraj arbitraže bo v Združenih državah, posameznik pa lahko izbere sodelovanje po video prenosu ali telefonu, ki se posamezniku zagotovi brezplačno. Osebna udeležba ne bo potrebna.

6. Jezik arbitraže bo angleški, razen če se stranki dogovorita drugače. Na podlagi utemeljene zahteve in ob upoštevanju tega, ali posameznika zastopa odvetnik, se tolmačenje na arbitražni obravnavi kot tudi prevod arbitražnega gradiva posamezniku zagotovi brezplačno, razen če senat ugotovi, da bi to glede na okoliščine posamezne arbitraže privedlo do neupravičenih ali nesorazmernih stroškov.

7. Gradivo, predloženo arbitrom, bo obravnavano kot zaupno in bo uporabljeno samo v povezavi z arbitražo.

8. Po potrebi se dovoli posamezno odkritje, takšno odkritje pa stranki obravnavata kot zaupno in bo uporabljeno zgolj v povezavi z arbitražo.

9. Arbitraža mora biti zaključena v 90 dneh od dostave obvestila zadevni organizaciji, razen če se stranki dogovorita drugače.

H. **Stroški**

Arbitri morajo ustrezno ukrepati, da bi zmanjšali stroške ali pristojbine arbitraže.

V skladu z veljavno zakonodajo bo Ministrstvo za trgovino omogočilo ustanovitev sklada, v katerega bodo morale organizacije v zasebnostnem ščitu plačati letni prispevek, deloma na podlagi velikosti organizacije, ki bo kril strošek arbitraže, vključno s stroški arbitrov, do najvišjih dovoljenih zneskov („najvišje vrednosti“) v posvetovanju z Evropsko komisijo. Sklad bo upravljala tretja stranka, ki bo redno poročala o delovanju sklada. Na letnem pregledu bosta Ministrstvo za trgovino in Evropska komisija pregledala delovanje sklada, vključno s potrebo po prilagoditvi zneska prispevkov ali najvišjih vrednosti, in med drugim upoštevala število arbitraž ter stroške in časovni potek arbitraž ob vzajemnem razumevanju, da organizacijam v zasebnostnem ščitu ne bo naloženo čezmerno finančno breme. Ta določba ne krije stroškov odvetnikov ali morebitnih skladov.

PRILOGA III

Pismo zunanjega ministra ZDA Johna Kerryja

7. julij 2016

Spoštovana komisarka Jourová!

Veseli me, da sva dosegla dogovor o zasebnostnem ščitu EU-ZDA, ki bo vključeval mehanizem varuha človekovih pravic, kateremu bodo lahko organi v EU predložili zahteve v imenu posameznikov iz EU v zvezi s prakso ZDA v obveščevalni dejavnosti pri zaznavanju signalov (SIGINT).

Predsednik Barack Obama je 17. januarja 2014 razglasil, da so v predsedniško politično direktivo 28 (Presidential Policy Directive 28 ali PPD-28) vnesli pomembne reforme obveščevalne dejavnosti. V skladu s PPD-28 sem imenoval namestnico zunanjega ministra Catherine A Novelli, ki je prav tako višja koordinatorka za mednarodno diplomacijo v informacijski tehnologiji, kot našo osebo za stike s tujimi vladami, ki želijo sprožiti vprašanja v zvezi z ameriško obveščevalno dejavnostjo SIGINT. Na podlagi tega sem ustanovil mehanizem varuha človekovih pravic na področju zasebnostnega ščita v skladu s pogoji, določenimi v Prilogi A, ki so bili po mojem pismu z 22. februarja 2016 posodobljeni. Izvajanje te funkcije sem dodelil namestnici ministra ge. Novelli. Namestnica ministra ga. Novelli deluje neodvisno od ameriške obveščevalne skupnosti in poroča neposredno meni.

Svojim zaposlenim sem naročil, naj namenijo vse potrebne vire za izvedbo tega novega mehanizma varuha človekovih pravic, in prepričan sem, da bo ta učinkovito sredstvo za obravnavo vprašanj posameznikov iz EU.

S spoštovanjem.

John F. Kerry

Priloga A

Mehanizem varuha človekovih pravic na področju zasebnostnega ščita EU-ZDA V zvezi z obveščevalno dejavnostjo SIGINT

Ob priznanju pomembnosti okvira zasebnostnega ščita EU-ZDA ta memorandum določa proces za izvedbo novega mehanizma, skladno s predsedniško politično direktivo 28 (Presidential Policy Directive 28 ali PPD-28), v zvezi z obveščevalno dejavnostjo SIGINT ([1]).

Predsednik Obama je 17. januarja 2014 v svojem govoru razglasil pomembne reforme obveščevalne dejavnosti. V tem govoru je poudaril, da „naše delo ne pomaga varovati le naš narod, temveč tudi naše prijatelje in zaveznike. Naše delo bo učinkovito le, če navadni državljani v drugih državah verjamejo, da Združene države spoštujejo tudi njihovo zasebnost." Predsednik Obama je objavil, da bo izdal novo predsedniško direktivo – PPD-28 –, s katero bo „jasno predpisal, kaj počnemo in česa ne počnemo pri našem čezmorskem nadzoru."

Člen 4(d) PPD-28 določa, da mora zunanji minister imenovati „višjega koordinatorja za mednarodno diplomacijo v informacijski tehnologiji" (višji koordinator) „ki bo … služil kot oseba za stike s tujimi vladami, ki želijo sprožiti vprašanja v zvezi z obveščevalnimi dejavnostmi SIGINT, ki jih izvajajo Združene države." Od januarja 2015 deluje kot višja koordinatorka namestnica ministra C. Novelli.

Ta memorandum opisuje novi mehanizem, ki ga bo upošteval višji koordinator pri lajšanju obravnave zahtev v zvezi z dostopom za potrebe nacionalne varnosti do podatkov, prenesenih iz EU v Združene države v skladu z zasebnostnim ščitom, standardnimi pogodbenimi klavzulami, zavezujočimi poslovnimi pravili, odstopanji ([2]) ali morebitnimi prihodnjimi odstopanji ([3]) po ustaljenih poteh v skladu z veljavnimi zakoni in politiko Združenih držav, ter odgovor na te zahteve.

1. **Varuh človekovih pravic na področju zasebnostnega ščita.** Višji koordinator bo deloval kot varuh človekovih pravic na področju zasebnostnega ščita in po potrebi imenoval dodatne uradnike na zunanjem Ministrstvu, ki mu bodo pomagali pri izvajanju dolžnosti, navedenih v tem memorandumu. (V nadaljnjem besedilu bodo koordinator in morebitni uradniki, ki izvajajo takšne dolžnosti, imenovani „varuh človekovih pravic na področju zasebnostnega ščita.") Varuh človekovih pravic na področju zasebnostnega ščita bo tesno sodeloval z ustreznimi uradniki iz drugih Ministrstev in agencij, ki so odgovorni za obdelavo zahtevkov v skladu z veljavno zakonodajo in politiko Združenih držav. Varuh človekovih pravic je neodvisen od obveščevalnih skupnosti. Varuh človekovih pravic poroča neposredno zunanjemu ministru, ki zagotovi, da varuh človekovih pravic opravlja svoje funkcije objektivno in neodvisno od neprimernega vpliva, ki bi lahko imel učinek na odgovor.

2. **Učinkovito usklajevanje.** Varuh človekovih pravic na področju zasebnostnega ščita bo lahko učinkovito uporabil spodaj opisane nadzorne organe in se z njimi usklajeval, da bi zagotovil, da bo imel njegov odgovor na zahtevke

([1]) Če se bo sklep Komisije o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, uporabljal za Islandijo, Lihtenštajn in Norveško, bo sveženj o zasebnostnem ščitu zajemal tako Evropsko unijo kot tudi te tri države. Zato se bo za sklicevanja na EU in njene države članice štelo, da vključujejo Islandijo, Lihtenštajn in Norveško.

([2]) „Odstopanja" v tem okviru pomenijo poslovni prenos ali prenose, ki se izvedejo pod pogojem, da: (a) je posameznik, na katerega se osebni podatki nanašajo, nedvoumno dal svojo privolitev k predlaganemu prenosu; ali (b) je prenos potreben za izvedbo pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem ali za izvajanje predpogodbenih ukrepov, sprejetih kot odgovor na zahtevo posameznika, na katerega se nanašajo osebni podatki; ali (c) je prenos potreben za sklenitev ali izpolnitev pogodbe med upravljavcem in tretjo stranko, ki je v korist posameznika, na katerega se osebni podatki nanašajo; ali (d) je prenos potreben oziroma ga zahteva zakon na temelju pomembnega javnega interesa ali pa za uveljavitev, uresničevanje ali varstvo pravice do vlaganja pravnih zahtevkov; ali (e) je prenos potreben, da bi zaščitili življenjske interese posameznikov, na katere se osebni podatki nanašajo; ali (f) se prenos opravi iz registra, ki je skladno z zakoni ali predpisi namenjen zagotavljanju informacij javnosti in je na voljo za vpogled javnosti na splošno ali kateri koli osebi, ki lahko izkaže zakoniti interes, če so v posameznem primeru izpolnjeni pogoji, ki jih za vpogled določa zakon.

([3]) „Morebitna prihodnja odstopanja" v tem okviru pomenijo poslovni prenos ali prenose, ki se izvedejo pod enim od naslednjih pogojev, če ta pogoj tvori zakonito podlago za prenos osebnih podatkov iz EU v ZDA: (a) posameznik, na katerega se nanašajo osebni podatki, je izrecno privolil v predlagani prenos, potem ko je bil obveščen o morebitnih tveganjih, ki jih zaradi nesprejetja sklepa o ustreznosti in ustreznih zaščitnih ukrepov takšni prenosi pomenijo zanj; ali (b) prenos je potreben za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugih oseb, kadar posameznik, na katerega se nanašajo osebni podatki, fizično ali pravno ni sposoben dati privolitve; ali (c) v primeru prenosa v tretjo državo ali mednarodni organizaciji in če se ne uporabljajo nobena druga obstoječa ali morebitna prihodnja odstopanja, in sicer samo, če se prenos ne ponavlja, če zadeva le omejeno število posameznikov, na katere se nanašajo podatki, je potreben za namene nujnih zakonitih interesov, ki jih zasleduje upravljavec in nad katerimi ne prevladajo interesi ali pravice in svobode posameznika, na katerega se nanašajo podatki, ter če je upravljavec ocenil vse okoliščine v zvezi s prenosom podatkov in na podlagi te ocene navedel ustrezne zaščitne ukrepe v zvezi z zaščito osebnih podatkov.

predložitvenega organa EU za obravnavanje pritožb posameznikov podlago v potrebnih informacijah. Kadar se zahteva nanaša na skladnost nadzora z zakonodajo ZDA, lahko varuh človekovih pravic na področju zasebnostnega ščita sodeluje z enim od neodvisnih nadzornih organov, ki imajo preiskovalna pooblastila.

a. Varuh človekovih pravic na področju zasebnostnega ščita bo tesno sodeloval z drugimi ameriškimi vladnimi uradniki, tudi z ustreznimi neodvisnimi nadzornimi organi, da bi zagotovil obdelavo in reševanje zaključenih zahtev v skladu z veljavnimi zakoni in politikami. Varuh človekovih pravic na področju zasebnostnega ščita bo zlasti lahko tesno sodeloval z Uradom direktorja nacionalne obveščevalne službe, Ministrstvom za pravosodje in po potrebi drugimi Ministrstvi in agencijami, vključenimi v nacionalno varnost Združenih držav, ter generalnimi inšpektorji, uradniki, pooblaščenimi po zakonu o dostopu do informacij javnega značaja, in uradniki na področju državljanskih svoboščin in zasebnosti.

b. Vlada Združenih držav se bo oprla na mehanizme za usklajevanje in nadzor nad zadevami nacionalne varnosti na vseh Ministrstvih in agencijah ter tako pomagala omogočiti, da varuh človekovih pravic na področju zasebnostnega ščita odgovori v smislu člena 4(e) na zaključene zahtevke po členu 3(b).

c. Varuh človekovih pravic na področju zasebnostnega ščita lahko zadeve v zvezi z zahtevami preda v obravnavo odboru za nadzor zasebnosti in državljanskih svoboščin.

3. **Predložitev zahtev**

a. Zahtevek bo najprej poslan nadzornim organom v državah članicah, pristojnim za nadzor nad nacionalnimi varnostnimi službami in/ali obdelavo osebnih podatkov s strani javnih organov. Zahtevek varuhu človekovih pravic na področju zasebnostnega ščita predloži centralizirani organ EU (v nadaljnjem besedilu skupaj: „organ za obravnavo pritožb posameznikov iz EU“).

b. Organ za obravnavo pritožb posameznikov iz EU bo v skladu s spodnjimi ukrepi zagotovil, da je zahtevek popoln:

(i) Preverjanje identitete posameznika ter da posameznik nastopa v svojem imenu in ne kot predstavnik vladne ali medvladne organizacije.

(ii) Zagotovitev, da je zahteva v pisni obliki in da vsebuje spodnje osnovne informacije:

— vse informacije, ki tvorijo osnovo zahteve,

— naravo informacij ali zahtevanega nadomestila,

— morebitni vladni subjekti ZDA, ki naj bi bili vpleteni, in

— drugi ukrepi, izvedeni za pridobivanje informacij ali zahtevanega nadomestila, ter odgovori, prejeti na podlagi teh drugih ukrepov.

(iii) Preverjanje, ali se zahteva nanaša na podatke, za katere obstaja utemeljen sum, da so bili preneseni iz EU v Združene države v skladu z zasebnostnim ščitom, standardnimi pogodbenimi klavzulami, zavezujočimi poslovnimi pravili, odstopanji ali morebitnimi prihodnjimi odstopanji.

(iv) Sprejem začetne ugotovitve, da zahtevek ni neresen, nadležen ali predložen v slabi veri.

c. Da je zahteva popolna in jo lahko nadalje obravnava varuh človekovih pravic na področju zasebnostnega ščita v okviru tega memorandumu, ni treba, da je v njej dokazano, da je vlada Združenih držav z obveščevalnimi dejavnostmi SIGINT dejansko dostopala do podatkov vložnika.

4. **Zaveze h komunikaciji s službami, ki obravnavajo pritožbe posameznikov iz EU**

a. Varuh človekovih pravic na področju zasebnostnega ščita bo potrdil prejem zahteve organu za obravnavo pritožb posameznikov iz EU.

b. Varuh človekovih pravic na področju zasebnostnega ščita bo opravil začetni pregled in preveril, ali je zahteva popolna v skladu s členom 3(b). Če varuh človekovih pravic na področju zasebnostnega ščita opazi morebitne pomanjkljivosti ali ima kakršno koli vprašanje v zvezi s popolnostjo zahteve, bo varuh človekovih pravic te zadeve naslovil in skušal rešiti z organom za obravnavo pritožb posameznikov iz EU.

c. Če za omogočanje ustrezne obravnave zahteve varuha človekovih pravic na področju zasebnostnega ščita potrebuje več informacij o zahtevi ali če mora posameznik, ki je prvotno predložil zahtevo, izvesti poseben ukrep, bo varuh človekovih pravic na področju zasebnostnega ščita o tem obvestil organ za obravnavo pritožb posameznikov iz EU.

d. Varuh človekovih pravic na področju zasebnostnega ščita bo spremljal stanje zahtev in po potrebi zagotovil nove podatke organu za obravnavo pritožb posameznikov iz EU.

e. Ko je zahteva izpolnjena, kakor je opisano v oddelku 3 tega memoranduma, bo varuh človekovih pravic na področju zasebnostnega ščita pravočasno zagotovil ustrezen odgovor organu za obravnavo pritožb posameznikov iz EU v skladu z stalno obveznostjo varovanja informacij po veljavnih zakonih in politikah. Varuh človekovih pravic na področju zasebnostnega ščita bo podal odgovor organu za obravnavo pritožb posameznikov iz EU, v katerem bo potrdil, (i) da je bila pritožba primerno preiskana in (ii) da bodo upoštevani pravo, zakoni, odredbe, predsedniške direktive in politike agencij ZDA, ki določajo omejitve in zaščitne ukrepe, opisane v pismu urada direktorja obveščevalne službe, ali da je v primeru neupoštevanja le-to bilo odpravljeno. Varuh človekovih pravic na področju zasebnostnega ščita ne bo ne potrdil ne zanikal, ali je posameznik tarča nadzora, prav tako pa varuh človekovih pravic na področju zasebnostnega ščita ne bo potrdil posebnega pravnega sredstva, ki je bil uporabljen. Kakor je nadalje opisano v oddelku 5, bodo zahteve po zakonu o dostopu do informacij javnega značaja obdelane, kakor je določeno po tem zakonu in veljavnih predpisih.

f. Varuh človekovih pravic na področju zasebnostnega ščita bo organu za obravnavo pritožb posameznikov iz EU neposredno sporočil, kdo bo odgovoren za komuniciranje s posameznikom, ki je predložil zahtevo. Če je neposredna komunikacija del enega od temeljnih procesov, opisanih spodaj, potem bo ta komunikacija izvedena v skladu z obstoječimi postopki.

g. Zaveze v tem memorandumu se ne bodo nanašale na splošne zahtevke, da je zasebnostni ščit EU-ZDA neskladen z zahtevami Evropske unije za zaščito podatkov. Zaveze v tem memorandumu so sprejete na podlagi vzajemnega razumevanja Evropske komisije in vlade ZDA, da lahko glede na obseg zavez v okviru tega mehanizma obstajajo omejitve sredstev, ki se med drugim pojavijo tudi v zvezi z zahtevami zakona o dostopu do informacij javnega značaja (Freedom of Information Act ali FOIA). Če bi izvajanje funkcij varuha človekovih pravic na področju zasebnostnega ščita preseglo razumne omejitve sredstev in zaviralo izpolnjevanje teh zavez, bo vlada ZDA skupaj z Evropsko komisijo obravnavala morebitne prilagoditve, ki bi lahko ustrezno uredile situacijo.

5. **Zahteve za informacije** Zahteve za dostop do evidenc vlade Združenih držav so lahko vložene in obravnavane v okviru zakona o dostopu do informacij javnega značaja (FOIA).

a. Zakon o dostopu do informacij javnega značaja zagotavlja vsem osebam sredstvo, da zahtevajo dostop do evidenc zveznih agencij ne glede na državljanstvo vložnika zahteve. Ta zakon je kodificiran v zakonodajni zbirki ZDA pod členom 552 naslova 5. Zakon skupaj z dodatnimi informacijami o zakonu o dostopu do informacij javnega značaja je na voljo na www.FOIA.gov in http://www.justice.gov/oip/foia-resources. Vsaka agencija ima vodstvenega delavca, ki je zadolžen za izvrševanje zakona o dostopu do informacij javnega značaja, in je zagotovila informacije na svoji javni spletni strani o tem, kako agenciji predložiti zahtevo v okviru zakona o dostopu do informacij javnega značaja. Agencije imajo vzpostavljene postopke za medsebojno posvetovanje glede zahtev v okviru zakona o dostopu do informacij javnega značaja v zvezi z evidencami, ki jih vodi druga agencija.

b. Na primer:

(i) Urad direktorja nacionalne obveščevalne službe (ODNI) je zase vzpostavil portal ODNI FOIA: http://www.dni.gov/index.php/about-this-site/foia. Ta portal zagotavlja informacije o predložitvi zahteve, preverjanju statusa obstoječe zahteve in dostopu do informacij, ki jih objavil urad predsednika nacionalne obveščevalne službe v skladu z zakonom o dostopu do informacij javnega značaja. Portal ODNI FOIA vsebuje povezave do drugih spletne strani FOIA za člane obveščevalne skupnosti: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

(ii) Urad za informacijsko politiko Ministrstva za pravosodje zagotavlja celovite informacije o zakonu o dostopu do informacij javnega značaja: http://www.justice.gov/oip. To vključuje ne le informacije o predložitvi zahteve v okviru zakona o dostopu do informacij javnega značaja Ministrstvu za pravosodje, temveč daje tudi navodila vladi Združenih držav glede razlage in uporabe zahtev zakona o dostopu do informacij javnega značaja.

c. Po zakonu o dostopu do informacij javnega značaja veljajo za dostop do vladnih evidenc določene naštete izjeme. Te vključujejo omejitve dostopa do tajnih informacij v zvezi z nacionalno varnostjo, osebnih informacij tretjih strank in informacij v zvezi s kazenskimi preiskavami ter so primerljive z omejitvami, ki jih vsaka država članica odredi s svojim zakonom o dostopu do informacij. Te omejitve veljajo enako za Američane in Neameričane.

d. Na spore v zvezi z objavo zahtevanih evidenc v skladu z zakonom o dostopu do informacij javnega značaja se je mogoče pritožiti upravno in nato na zveznem sodišču. Sodišče mora na novo ugotoviti, ali so bile evidence ustrezno zadržane (člen 552(a)(4)(B) naslova 5 zakonodajne zbirke ZDA), in lahko vladi odredi, da zagotovi dostop do evidenc. V nekaterih primerih so sodišča ovrgla trditve vlade, da je treba te informacije pridržati kot tajne. Čeprav ni na voljo nobenih denarnih odškodnin, lahko sodišča prisodijo odvetniške stroške.

6. **Zahteve za nadaljnje ukrepe** Zahteva, ki navaja domnevno kršitev zakona ali drugo neustrezno ravnanje, bo predložena ustreznemu organu vlade Združenih držav, vključno z neodvisnimi nadzornimi organi, s pooblastilom, da preišče ustrezni zahtevek in obravnava neizpolnjevanje načel, kakor je opisano spodaj.

a. Generalni inšpektorji so zakonsko neodvisni; imajo široka pooblastila za izvajanje preiskav, revizij in pregledov programov, vključno z goljufijami in zlorabo ali kršitvijo zakona, in lahko priporočajo popravne ukrepe.

(i) Zakon o generalnih inšpektorji (Inspector General Act) iz leta 1978, s spremembami, je zakonsko ustanovil zvezne generalne inšpektorje kot neodvisne in objektivne enote znotraj večine agencij, ki so zadolžene za boj proti potratni porabi, goljufijam in zlorabah v programih in operacijah svojih agencij. V ta namen je vsak zvezni generalni inšpektor dolžan izvajati revizije in preiskave v zvezi s programi in operacijami svoje agencije. Poleg tega zvezni generalni inšpektorji prevzamejo vodilno vlogo in usklajevanje ter priporočajo politike za dejavnosti, namenjene za spodbujanje gospodarstva, učinkovitosti in uspešnosti ter preprečevanje in odkrivanje goljufij in zlorab v programih in delovanju agencij.

(ii) Vsak član obveščevalne skupnosti ima svoj urad generalnega inšpektorja, ki je med drugim odgovoren za nadzor tujih obveščevalnih dejavnosti. Številna poročila generalnih inšpektorjev o programih obveščevalnih dejavnosti so javno objavljena.

(iii) Na primer:

— Urad generalnega inšpektorja obveščevalne skupnosti je bil ustanovljen v skladu s členom 405 zakona o pooblastilih za obveščevalno dejavnost oz. Intelligence Authorization Act – http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf – za davčno leto 2010. Ta urad je odgovoren za izvajanje revizij, preiskav, inšpekcijskih nadzorov in pregledov po vsej obveščevalni skupnosti, v katerih ugotavlja in obravnava sistemska tveganja, ranljivost in pomanjkljivosti v več nalogah agencij obveščevalne skupnosti, da bi pozitivno vplival na gospodarnost in učinkovitost celotne obveščevalne skupnosti. Urad generalnega inšpektorja je pooblaščen za preiskovanje pritožb ali informacij v zvezi z domnevnimi kršitvami zakona, pravila, predpisa, glede potratne porabe, goljufije, zlorabe pooblastil ali precejšnje ali posebne nevarnosti za javno zdravje in varnost v povezavi z uradom direktorja nacionalne obveščevalne službe in/ali obveščevalnimi programi in dejavnostmi obveščevalne skupnosti. Urad zagotavlja informacije o tem, kako z njim vzpostaviti neposredni stik za predložitev poročila: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Urad generalnega inšpektorja na Ministrstvu za pravosodje ZDA – https://www.justice.gov/ – je zakonsko ustanovljen neodvisni subjekt z nalogo, da odkriva in odvrača od potratne porabe, goljufij, zlorab in kršitev v programih in pri zaposlenih na Ministrstvu za pravosodje ter da spodbuja gospodarnost in učinkovitost v teh programih. Urad generalnega inšpektorja preišče domnevne kršitve kazenskega in civilnega prava s strani zaposlenih na Ministrstvu za pravosodje ZDA ter izvede revizijske in inšpekcijske preglede programov Ministrstva za pravosodje. Urad generalnega inšpektorja je pristojen za vse pritožbe glede nepravilnega ravnanja proti zaposlenim na Ministrstvu za pravosodje, tudi na Zveznem preiskovalnem uradu (FBI); Uradu za boj proti drogam (DEA); Zveznem uradu za zapore; Uradu ameriških zveznih šerifov; Uradu za alkohol, tobak, strelno orožje in eksploziv; Ameriškemu državnemu tožilstvu; in zaposlenim, ki delajo na drugih oddelkih in uradih Ministrstva za pravosodje. (Edina izjema je, da je za

domnevno nepravilno ravnanje odvetnika na Ministrstvu ali oseb, ki izvajajo kazenski pregon, v zvezi z izvrševanjem pooblastil odvetnika Ministrstva za preiskavo, pravdni spor ali dajanje pravnih nasvetov odgovoren urad za poklicno odgovornost na Ministrstvu.) Poleg tega člen 1001 ameriškega zakona o domovinski varnosti (USA Patriot Act), vpisanega v zakonodajo 26. oktobra 2001, nalaga generalnemu inšpektorju, da pregleda informacije in sprejema pritožbe o domnevnih zlorabah državljanskih pravic in svoboščin zaposlenih na Ministrstvu za pravosodje. Urad generalnega inšpektorja vzdržuje javno spletno stran – https://www.oig.justice.gov –, ki vsebuje prijavno točko za predložitev pritožb – https://www.oig.justice.gov/hotline/index.htm.

b. Ustrezne odgovornosti imajo tudi uradi in subjekti na področju varstva zasebnosti in državljanskih svoboščin v vladi ZDA. Na primer:

(i) Člen 803 izvedbenih priporočil zakona 9/11 Commission Act iz leta 2007, kodificiranega v zakonodajni zbirki ZDA pod členom 2000-ee1 naslova 42, uvaja uradnike na področju varstva zasebnosti in državljanskih svoboščin na določenih Ministrstvih in agencijah (vključno z Ministrstvom za zunanje zadeve, Ministrstvom za pravosodje in Uradom direktorja nacionalne obveščevalne službe). Člen 803 določa, da bodo ti uradniki na področju varstva zasebnosti in državljanskih svoboščin delovali kot glavni svetovalec in s tem med drugim zagotovili, da ima tako Ministrstvo, agencija ali član ustrezne postopke za obravnavo pritožb posameznikov, ki trdijo, da je tako Ministrstvo, agencija ali član kršil njihovo zasebnost ali državljanske svoboščine.

(ii) Urad za državljanske svoboščine in zasebnost v okviru Urada direktorja nacionalne obveščevalne službe (ODNI CLPO) vodi uradnik za zaščito državljanskih svoboščin v Uradu direktorja nacionalne obveščevalne službe – položaj, ki je bil uveden z zakonom o nacionalni varnosti (National Security Act) iz leta 1948, s spremembami. Ena od dolžnosti ODNI CLPO je zagotoviti, da politike in postopki članov obveščevalne skupnosti vsebujejo ustrezne elemente za zaščito zasebnosti in državljanskih svoboščin, ter pregledovati in preiskovati pritožbe o domnevnih zlorabah ali kršitvah državljanskih svoboščin in zasebnosti v programih in dejavnostih Urada direktorja nacionalne obveščevalne službe. ODNI CLPO na svoji spletni strani zagotavlja javnosti informacije, vključno z navodili za predložitev pritožbe: www.dni.gov/clpo. Če ODNI CLPO prejme pritožbo v zvezi z varstvom zasebnosti ali državljanskih svoboščin, ki se nanaša na programe in dejavnosti obveščevalne skupnosti, bo z drugimi člani obveščevalne skupnosti uskladil način, kako nadalje obravnavati pritožbo znotraj obveščevalne skupnosti. Pri tem je treba poudariti, da ima tudi Agencija ZDA za nacionalno varnost (NSA) urad za državljanske svoboščine in zasebnost, ki zagotavlja informacije o svojih dolžnostih na svoji spletni strani – https://www.nsa.gov/civil_liberties/. Če informacije navajajo, da agencija ne izpolnjuje zahtev glede varstva zasebnosti (npr. zahteva iz člena 4 PPD-28), imajo agencije mehanizme za pregledovanje izpolnjevanja in odpravljanje zapleta. Agencije morajo poročati Uradu direktorja nacionalne obveščevalne službe o primerih neizpolnjevanja po PPD-28.

(iii) Urad za varstvo zasebnosti in državljanskih svoboščin (OPCL) na Ministrstvu za pravosodje podpira dolžnosti in odgovornosti glavnega uradnika za nadzor zasebnosti in državljanskih svoboščin na Ministrstvu (CPCLO). Glavna naloga OPCL je zaščititi zasebnost in državljanske svoboščine Američanov skozi pregled, nadzor in usklajevanje delovanja Ministrstva na področju varstva zasebnosti. OPCL daje pravne nasvete in navodila službam na Ministrstvu; zagotavlja spoštovanje zasebnosti na Ministrstvu, tudi zakona o zasebnosti (Privacy Act) iz leta 1974, določb o zasebnosti iz zakonov E-Government Act iz leta 2002 in Federal Information Security Management Act ter z direktivami vladne politike, izdanimi v podporo tem zakonom; oblikuje in zagotavlja usposabljanje glede varstva zasebnosti na Ministrstvu; pomaga CPCLO pri oblikovanju politike glede varstva zasebnosti na Ministrstvu; pripravlja poročila v zvezi z varstvom zasebnosti za predsednika in kongres; in pregleduje prakse ravnanja z informacijami na Ministrstvu, da bi zagotovilo skladnost takšnih praks z zaščito zasebnosti in državljanskih svoboščin. OPCL daje javnosti informacije o svojih odgovornostih na http://www.justice.gov/opcl.

(iv) V skladu s členom 2000ee *et seq*. naslova 42 zakonodajne zbirke ZDA Odbor za nadzor zasebnosti in državljanskih svoboščin nenehno pregleduje (i) politike in postopke Ministrstev, agencij in članov izvršilne veje ter njihovo izvajanje v zvezi s prizadevanji za zaščito naroda pred terorizmom ter s tem zasebnosti in državljanskih svoboščin, ter (ii) druge ukrepe izvršilne veje v zvezi s takimi prizadevanji, da bi ugotovil, ali taki ukrepi ustrezno ščitijo zasebnost in državljanske svoboščine ter so skladni z zakoni, predpisi in politikami, ki urejajo varstvo zasebnosti in državljanskih svoboščin. Sprejemal in pregledoval bo poročila in druge informacije uradnikov na področju varstva zasebnosti in državljanskih svoboščin ter jim po potrebi dajal priporočila v zvezi z njihovimi dejavnostmi. Člen 803 izvedbenih priporočil zakona 9/11 Commission Act iz leta 2007, kodificiranega v zakonodajni zbirki ZDA pod členom 2000ee-1 naslova 42, uradnikom na področju varstva zasebnosti in državljanskih svoboščin osmih zveznih agencij (vključno z ministrom za obrambo, ministrom za domovinsko varnost, direktorjem nacionalne obveščevalne službe in direktorjem ameriške obveščevalne agencije CIA) ter morebitnim dodatnim agencijam, ki jih imenuje Odbor, nalaga predložitev rednih poročil Odboru za nadzor zasebnosti in državljanskih svoboščin, vključno s številom,

naravo in razpletom pritožb, ki jih prejme zadevna agencija za domnevne kršitve. Zakon, ki daje pooblastila Odboru za nadzor zasebnosti in državljanskih svoboščin, slednjemu nalaga, da sprejme ta poročila in, kjer je ustrezno, da priporočila uradnikom za nadzor zasebnosti in državljanskih svoboščin v zvezi z njihovimi dejavnostmi.

PRILOGA IV

Pismo predsednice Zvezne komisije za trgovino Edith Ramirez

7. julij 2016

PO ELEKTRONSKI POŠTI

Věra Jourová
Komisarka za pravosodje, potrošnike in enakost spolov
Evropska komisija
Rue de la Loi/Wetstraat 200
1049 Bruselj
Belgija

Spoštovana komisarka Jourová,

Zvezna komisija za trgovino ZDA (Federal Trade Commission ali FTC) se zahvaljuje za priložnost, da opiše uveljavljanje novega okvira zasebnostnega ščita EU-ZDA („okvir zasebnostnega ščita" ali „okvir"). Verjamemo, da bo okvir igral ključno vlogo pri spodbujanju trgovinskih poslov, ki ščitijo zasebnost v tem vedno bolj medsebojno povezanem svetu. Podjetjem bo omogočil izvajanje pomembnih operacij v svetovnem gospodarstvu, obenem pa bo zagotovil, da potrošniki iz EU ohranijo pomembno varstvo zasebnosti. Zvezna komisija za trgovino je že dlje časa zavezana k zaščiti zasebnosti prek meja in bo prednostno obravnavala uveljavljanje novega okvira. Spodaj na splošno opisujemo preteklo odločno uveljavljanje varstva zasebnosti Zvezne komisije za trgovino, vključno z uveljavljanjem prvotnega programa varnega pristana, kot tudi pristop Zvezne komisije za trgovino k uveljavljanju novega okvira.

Zvezna komisija za trgovino je svojo zavezanost k uveljavljanju programa varnega pristana prvič izrazila leta 2000. Takratni predsednik Zvezne komisije za trgovino Robert Pitofsky je takrat poslal Evropski komisiji pismo, v katerem navaja obljubo Zvezne komisije za trgovino, da odločno uveljavi načela zasebnosti varnega pristana. Zvezna komisija za trgovino še naprej izpolnjuje to zavezo z uvedbo pregona v skoraj 40 zadevah ter številnimi preiskavami in sodelovanjem s posameznimi evropskimi organi za zaščito podatkov v zadevah skupnega interesa.

Potem ko je Evropska komisija novembra 2013 sprožila vprašanja o upravljanju in uveljavljanju programa varnega pristana, smo skupaj z Ministrstvom za trgovino ZDA začeli posvetovanja z uradniki iz Evropske komisije, da bi raziskali načine za njegovo okrepitev. Medtem ko so potekala posvetovanja, je Sodišče 6. oktobra 2015 izdalo sklep v zadevi Schrems, ki je med drugim razveljavil sklep Evropske komisije o ustreznosti programa varnega pristana. Po tem sklepu smo še naprej tesno sodelovali z Ministrstvom za trgovino in Evropsko komisijo, da bi okrepili varstvo zasebnosti posameznikov iz EU. Okvir zasebnostnega ščita je plod teh nenehnih posvetovanj. Kakor pri programu varnega pristana, se Zvezna komisija za trgovino zavezuje k odločnemu uveljavljanju novega okvira. To pismo je zapis te zaveze.

Zlasti potrjujemo svojo zavezo na štirih ključnih področjih: (1) prednostna obravnava in preiskave predloženih zadev; (2) obravnavanje lažnih ali goljufivih trditev glede članstva v zasebnostnem ščitu; (3) nenehno spremljanje odločb; in (4) okrepljeno sodelovanje z organi za zaščito podatkov EU pri vključevanju in uveljavljanju. Spodaj podajamo podrobne informacije o vsaki od teh zavez ter ustrezno ozadje vloge Zvezne komisije za trgovino pri zaščiti zasebnosti potrošnikov in uveljavljanju varnega pristana, kot tudi o širšem področju zasebnosti v Združenih državah ([1]).

I. OZADJE

A. **Izvrševanje in politika Zvezne komisije za trgovino na področju varstva zasebnosti**

Zvezna komisija za trgovino ima široka pooblastila za izvrševanje civilnega prava z namenom spodbujanja varstva potrošnikov in konkurenčnosti v trgovini. V okviru svojega pooblastila za zaščito potrošnikov Zvezna komisija za

([1]) Dodatne informacije o zveznih in državnih zakonih v ZDA glede varstva zasebnosti podajamo v Prilogi A. Poleg tega je povzetek naših nedavnih ukrepov pregona zaradi varstva zasebnosti in varnosti na voljo na spletni stran Zvezne komisije za trgovino na naslovu https://www.ftc.gov/reports/privacy-data-security-update-2015.

trgovino izvaja široko paleto zakonov za zaščito zasebnosti in varnost podatkov o potrošnikih. Glavni zakon, ki ga izvaja Zvezna komisija za trgovino, tj. zakon o FTC ali FTC Act, prepoveduje „nepoštena“ in „goljufiva“ dejanja ali ravnanje v trgovini ali v zvezi z njo ([1]). Predstavitev, opustitev ali ravnanje je goljufivo, če je pomembno in verjetno zavede potrošnike, ki se vedejo razumno v danih okoliščinah ([2]). Dejanje ali ravnanje je nepošteno, če potrošnikom povzroči ali je verjetno, da bo povzročilo, bistveno škodo, ki se ji ni mogoče razumno izogniti in je ne odtehtajo kompenzacijske ugodnosti za potrošnike ali konkurenco ([3]). Zvezna komisija za trgovino izvaja tudi ciljne zakone, ki ščitijo informacije v zvezi z zdravstvenimi, kreditnimi in drugimi finančnimi zadevami, kot tudi informacije na spletu o otrocih, ter izdaja predpise za izvajanje vsakega od teh zakonov.

Pristojnost Zvezne komisije za trgovino po zakonu o FTC se nanaša na zadeve „v ali v zvezi s trgovino“. Zvezna komisija za trgovino nima pristojnosti nad zadevami kazenskega pregona ali nacionalne varnosti. Zvezna komisija za trgovino prav tako ne more doseči večino drugih vladnih ukrepov. Poleg tega obstajajo izjeme v pristojnosti Zvezne komisije za trgovino nad trgovinskimi dejavnostmi, tudi v zvezi z bankami, letalskimi prevozniki, zavarovalništvom in dejavnostmi splošnih telekomunikacijskih operaterjev. Zvezna komisija za trgovino prav tako nima pristojnosti nad večino neprofitnih organizacij, vendar pa ima pristojnost nad lažnimi dobrodelnimi in drugimi neprofitnimi organizacijami, ki v resnici poslujejo za dobiček. Zvezna komisija za trgovino ima pristojnost tudi nad neprofitnimi organizacijami, ki poslujejo za dobiček svojih članov, usmerjenih v dobiček, vključno tako, da zagotavljajo precejšnje gospodarske koristi tem članom ([4]). V nekaterih primerih pristojnost Zvezne komisije za trgovino sovpada s pristojnostjo drugih organov kazenskega pregona.

Razvili smo trdne delovne odnose z zveznimi in državnimi organi ter z njimi tesno sodelujemo pri usklajevanju preiskav ali predložitvi zadev, kjer je primerno.

Uveljavljanje je hrbtenica pristopa Zvezne komisije za trgovino k zaščiti zasebnosti. Do danes je Zvezna komisija za trgovino vložila več kot 500 tožb za zaščito zasebnosti in varstvo informacij o potrošnikih. Te zadeve zajemajo tako informacije na spletu kot tudi na nepovezanih sredstvih ter vključujejo uvedbo pregona proti velikim in malim podjetjem, ki trdijo, da niso uspela ustrezno odstraniti občutljivih podatkov o potrošnikih, niso uspela zavarovati osebnih informacij potrošnikov, so goljufivo sledila potrošnikom po spletu, pošiljala neželeno pošto potrošnikom, namestila vohunsko ali drugo zlonamerno programsko opremo na računalnike potrošnikov, kršila pravila prepovedi klicanja in drugega trženja po telefonu ter neprimerno zbirala in izmenjevala informacije o potrošnikih na mobilnih napravah. Uvedba pregona Zvezne komisije za trgovino v teh zadevah – tako v fizičnem kot tudi v digitalnem svetu – je podjetjem poslala pomembno sporočilo o potrebi, da zaščitijo zasebnost potrošnikov.

Zvezna komisija za trgovino prav tako izvaja številne politične pobude, namenjene krepitvi varstva zasebnosti potrošnikov, ki tvorijo podlago za njeno delu pri uveljavljanju. Zvezna komisija za trgovino izvaja delavnice in izdaja poročila, v katerih priporoča dobre prakse, namenjene izboljšanju varstva zasebnosti v mobilnem okolju, povečanju preglednosti v panogi posrednikov podatkov, povečanju koristi velikih podatkov ob zmanjševanju tveganj, zlasti za potrošnike z nizkimi dohodki in manjšo dostopnostjo, in poudarjanju posledic, med drugim, prepoznavanja obraza in interneta stvari na zasebnost in varnost.

Zvezna komisija za trgovino izvaja tudi izobraževanje potrošnikov in podjetij, da bi okrepila učinek svojih pobud za uveljavljanje in oblikovanje politik. Zvezna komisija za trgovino uporablja različna orodja – objave, spletni viri, delavnice in družbena omrežja – za zagotavljanje izobraževalnega gradiva za zelo različne teme, vključno z mobilnimi aplikacijami, zasebnostjo otrok in varnostjo podatkov. Nazadnje je Zvezna komisija za trgovino sprožila svojo pobudo „Začnimo pri varnosti“ (Start With Security), ki vsebuje nova navodila za podjetja, pripravljena na podlagi izkušenj v zadevah agencije v zvezi varovanjem podatkov, in delavnice, ki se izvajajo po vsej državi. Poleg tega Zvezna komisija za trgovino že dolgo igra vodilno vlogo pri izobraževanju potrošnikov o osnovni računalniški varnosti. Lani sta imeli spletna stran OnGuard in njena španska različica Alerta en Linea več kot 5 milijonov ogledov.

B. **Pravno varstvo ZDA v korist potrošnikom iz EU**

Okvir deluje v sklopu širšega področja zasebnosti v ZDA, ki na več načinov ščiti potrošnike iz EU.

([1]) Člen 45(a) naslova 15 zakonodajne zbirke ZDA.
([2]) Glej izjavo Zvezne komisije za trgovino o politiki glede goljufij, priloženo Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), na voljo na https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
([3]) Glej člen 45(n) naslova 15 zakonodajne zbirke ZDA. Izjava Zvezne komisije za trgovino o politiki glede nepoštenosti, priložena Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), na voljo na https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
([4]) Glej California Dental Ass'n v. FTC, Zbirka odločb vrhovnega sodišča št. 526, str. 756 (1999).

Prepoved nepoštenih ali goljufivih dejanji ali ravnanja v zakonu o FTC (FTC Act) ni omejena na zaščito potrošnikov iz ZDA pred podjetji iz ZDA, saj vključuje prakse, ki (1) povzročijo ali je verjetno, da bodo povzročile, razumno predvidljivo škodo v Združenih državah ali (2) vključujejo bistveno ravnanje v Združenih državah. Poleg tega lahko Zvezna komisija za trgovino pri zaščiti tujih potrošnikov uporabi vsa pravna sredstva, vključno s povračilom, ki so na voljo za zaščito domačih potrošnikov.

Delo Zvezne komisije za trgovino pri uveljavljanju zares pomembno koristi potrošnikom v ZDA kot tudi tujim potrošnikom. Denimo, naše zadeve, ki uveljavljajo člen 5 zakona o FTC, so enako zaščitile zasebnost ameriških in tujih potrošnikov. V zadevi proti posredniku podatkov Accusearch je Zvezna komisija za trgovino trdila, da je prodaja zaupnih telefonskih evidenc podjetja tretjim strankam brez vednosti ali privolitve potrošnikov nepošteno ravnanje, ki krši člen 5 zakona o FTC. Družba Accusearch je prodala informacije v zvezi z ameriškimi in tujimi potrošniki ([1]). Sodišče je odobrilo sodno prepoved proti družbi Accusearch, s katero je med drugim prepovedalo trženje ali prodajo osebnih informacij potrošnikov brez pisnega soglasja, razen če so te bile pridobljene zakonito iz javno dostopnih informacij, ter odredilo plačilo skoraj 200 000 USD ([2]).

Drug primer je poravnava Zvezne komisije za trgovino z družbo TRUSTe. Ta zagotavlja, da se lahko potrošniki, tudi tisti v Evropski uniji, zanesejo na predstavitve, da svetovna organizacija s samourejevalnim sistemom komentira svoje preglede in certifikacijo domačih in tujih spletnih storitev ([3]). Pomembno je, da naš postopek proti družbi širše krepi tudi samourejevalni sistem varstva zasebnosti, s tem ko zagotavlja odgovornost subjektov, ki igrajo pomembno vlogo v samourejevalnih shemah, vključno z okviri za čezmejno varstvo zasebnosti.

Zvezna komisija za trgovino uveljavlja tudi druge ciljne zakone, ki varujejo tudi potrošnike zunaj ZDA, kot je zakon Children's Online Privacy Protection Act („COPPA"). Zakon COPPA med drugim od upravljavcev spletnih strani in storitev, namenjenih otrokom, ali strani za splošno občinstvo, ki zavestno zbirajo osebne informacije otrok, starih do 13 let, zahteva, da obvestijo starše in pridobijo preverljivo soglasje staršev. Ameriške spletne strani in storitve, za katere velja zakon COPPA in ki zbirajo osebne informacije tujih otrok, so dolžne upoštevati zakon COPPA. Tuje spletne strani in storitve morajo prav tako upoštevati zakon COPPA, če so usmerjene v otroke v Združenih državah ali če zavestno zbirajo osebne informacije otrok v Združenih državah. Poleg ameriških zveznih zakonov, ki jih uveljavlja Zvezna komisija za trgovino, lahko potrošnikom iz EU prinesejo dodatne ugodnosti tudi nekateri drugi zvezni in državni zakoni na področju zaščite in varstva zasebnosti potrošnikov.

C. **Uveljavljanje varnega pristana**

V okviru programa za uveljavljanje varstva zasebnosti in varnosti je Zvezna komisija za trgovino želela zaščititi tudi potrošnike iz EU, in sicer z vlaganjem tožb zaradi kršitev varnega pristana. Zvezna komisija za trgovino je vložila 39 tožb v zvezi z uveljavljanjem varnega pristana: V 36 zadevah je šlo za domnevne lažne trditve glede certifikacije, v treh zadevah – proti družbam Google, Facebook in Myspace – pa za domnevne kršitve načel zasebnosti varnega pristana ([4]). Te zadeve dokazujejo izvršljivost certificiranja in posledice neizpolnjevanja. Odredbe za pridobivanje soglasij v naslednjih dvajsetih letih od družb Google, Facebook in Myspace zahtevajo, da izvajajo celovite programe za varstvo zasebnosti, ki morajo razumno obravnavati tveganja za varstvo zasebnosti, povezana z razvojem in upravljanjem novih in obstoječih proizvodov in storitev, ter za zaščito zasebnosti in zaupnosti osebnih informacij. Celoviti programi varstva zasebnosti, odrejeni v teh odločbah, morajo opredeliti predvidljiva bistvena tveganja in imeti kontrole za obravnavanje takšnih tveganj. Podjetja morajo Zvezni komisiji za trgovino predložiti tudi stalne neodvisne ocene svojih programov za varstvo zasebnosti. Odločbe tem družbam prepovedujejo tudi lažne navedbe o svojem ravnanju na področju varstva zasebnosti in o svojem sodelovanju v morebitnem programu za varstvo zasebnosti ali varnost. Prepoved bi se nanašala tudi na dejanja in ravnanje podjetij po novem okviru zasebnostnega ščita. Zvezna komisija za trgovino lahko te odločbe uveljavi

([1]) Glej Office of the Privacy Commissioner of Canada, Pritožba v skladu s PIPEDA proti Accusearch, Inc., ki posluje kot Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Urad kanadskega pooblaščenca za varstvo zasebnosti je vložil stališče *amicus curiae* v pritožbi na tožbo Zvezne komisije za trgovino in izvedel lastno preiskavo, v kateri je ugotovil, da je družba Accusearch s svojim ravnanjem kršila tudi kanadsko zakonodajo.

([2]) Glej FTC proti Accusearch, Inc., št. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) Glej v zadevi True Ultimate Standards Everywhere, Inc., št. C-4512 (F.T.C. Mar. 12, 2015) (sklep in odločba), na voljo na https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Glej v zadevi Google, Inc., št. C-4336 (F.T.C. 13. oktober 2011) (sklep in odločba), na voljo na https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; v zadevi Facebook, Inc., št. C-4365 (F.T.C. 27. julij 2012) (sklep in odločba), na voljo na https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; v zadevi Myspace LLC, št. C-4369 (F.T.C. 30. avgust 2012) (sklep in odredba), na voljo na https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

skozi denarne kazni. Družba Google je namreč leta 2012 plačala rekordno denarno kazen v višini 22,5 milijona USD za razrešitev obtožb, da je kršila odlok FTC zoper njo. Posledično pomagajo odloki Zvezne komisije za trgovino ščititi več kot milijardo potrošnikov po vsem svetu, od katerih jih na stotine milijonov prebiva v Evropi.

Zadeve Zvezne komisije za trgovino so osredotočene tudi na lažne, goljufive ali zavajajoče trditve glede sodelovanja v varnem pristanu. Zvezna komisija za trgovino takšne trditve jemlje resno. Na primer, v zadevi Zvezna komisija za trgovino proti Karnani je Zvezna komisija za trgovino leta 2011 vložila tožbo proti spletnemu tržniku v Združenih državah, v kateri je trdila, da je on in njegovo podjetje zavedlo britanske potrošnike, da so verjeli, da ima podjetje sedež v Združenem kraljestvu, tudi z uporabo spletnih pripon.uk in navajanjem britanske valute ter poštnega sistema Združenega kraljestva ([1]). Toda ko so potrošniki prejeli izdelke, so naleteli na nepričakovane uvozne dajatve, garancije, ki niso veljale v Združenem kraljestvu, in stroške, povezane s pridobivanjem povračil. Zvezna komisija za trgovino je v obtožbi navedla tudi, da so obtoženi zavajali potrošnike o svojem sodelovanju v programu varnega pristana. Vsi prizadeti potrošniki so namreč bili v Združenem kraljestvu.

Mnoge naše druge zadeve v zvezi z uveljavljanjem varnega pristana so vključevale organizacije, ki so pristopile k programu varnega pristana, vendar niso obnovile svoje certifikacije, obenem pa so se še naprej predstavljale kot aktualne članice. Kakor je obravnavano spodaj, se Zvezna komisija za trgovino zavezuje tudi k obravnavi lažnih trditev o sodelovanju v okviru zasebnostnega ščita. Ta strateška dejavnost pregona bo dopolnila okrepljene ukrepe Ministrstva za trgovino pri preverjanju izpolnjevanja zahtev programa za certifikacijo in ponovno certifikacijo, njegovo spremljanje učinkovitega izpolnjevanja, vključno z uporabo vprašalnikov za sodelujoče v okviru, in okrepljenimi prizadevanji za odkrivanje lažnih trditev glede članstva v okviru in zlorabe morebitne certifikacijske oznake okvira ([2]).

II. PREDNOSTNA OBRAVNAVA IN PREISKAVE PREDLOŽITEV

Zvezna komisija za trgovino se tako kot v programu varnega pristana zavezuje, da bo dala prednost zadevam, ki jih države članice EU predložijo v okviru zasebnostnega ščita. Prav tako bomo dali prednost zadevam neizpolnjevanja samourejevalnih smernic, ki se nanašajo na okvir zasebnostnega ščita in jih predložijo organizacije s samourejevalnim sistemom za varstvo zasebnosti in druge neodvisne službe za reševanje sporov.

Za lažjo predložitev zadev držav članic EU po tem okviru Zvezna komisija za trgovino pripravlja poenoten postopek za predložitev in daje državam članicam EU navodila glede vrste informacij, ki bi najbolj pomagale Zvezni komisiji za trgovino v njeni preiskavi predložene zadeve. V okviru teh prizadevanj bo Zvezna komisija za trgovino v agenciji imenovala osebo za stike, ki bo sprejemala predložitve držav članic EU. Zelo pripravno je, če organ, ki preloži zadevo, že opravi predhodno preiskavo domnevne kršitve in lahko sodeluje z Zvezno komisijo za trgovino v preiskavi.

Ob prejemu predložitve države članice EU ali organizacije s samourejevalnim sistemom lahko Zvezna komisija za trgovino sprejme vrsto različnih ukrepov za obravnavo sproženih vprašanj. Na primer, pregledamo lahko politike zasebnosti podjetja, pridobimo dodatne informacije neposredno od podjetja ali tretjih strank, ga nadalje spremljamo skupaj s subjektom, ki je predložil zadevo, ocenimo, ali obstaja vzorec kršitev ali precejšnje število prizadetih potrošnikov, določimo, ali predložena zadeva odpira vprašanja na področju delovanja Ministrstva za trgovino, ocenimo, ali bi bilo izobraževanje potrošnikov in podjetij koristno, in po potrebi sprožimo izvršilni postopek.

Zvezna komisija za trgovino se prav tako zavezuje izmenjevati informacije o predloženih zadevah z organi pregona, ki predložijo zadevo, vključno s statusom predloženih zadev, v skladu z omejitvami in zakoni, ki urejajo zaupnost. Če je glede na število in vrsto prejetih predložitev izvedljivo, bodo zagotovljene informacije vključevale oceno predloženih zadev, vključno z opisom pomembnih vprašanj in morebitnih ukrepov, sprejetih za obravnavo kršitev zakona v okviru pristojnosti Zvezne komisije za trgovino. Zvezna komisija za trgovino bo organu, ki predloži zadevo, zagotovila tudi povratne informacije o vrstah predložitev, ki jih prejme, da bi povečala učinkovitost prizadevanj za obravnavo

([1]) Glej FTC proti Karnani, št. 2:09-cv-05276 (C.D. Cal. 20. maj 2011) (pravnomočni sklep), na voljo na https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; glej tudi Lesley Fair, FTC Business Center Blog, Around the World in Shady Ways, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9. junij 2011).

([2]) Pismo vršilca dolžnosti namestnika ministra za mednarodno trgovino Kena Hyatta, Uprava za mednarodno trgovino, Věri Jourovi, komisarki za pravosodje, potrošnike in enakost spolov.

nezakonitega ravnanja. Če organ pregona, ki predloži zadevo, zahteva informacije o statusu posamezne predložene zadeve za namene izvajanja lastnega izvršilnega postopka, bo Zvezna komisija za trgovino odgovorila, pri tem pa upoštevala število predloženih zadev v obravnavi, zaupnost in druge zakonske zahteve.

Zvezna komisija za trgovino bo prav tako tesno sodelovala z organi EU za zaščito podatkov, da bi zagotovila pomoč pri uveljavljanju. V ustreznih primerih bi to lahko vključevalo izmenjavo informacij in pomoč pri preiskovanju v skladu z ameriškim zakonom o spletni varnosti (U.S. SAFE WEB Act), ki Zvezni komisiji za trgovino dovoljuje, da tujim organom kazenskega pregona nudi pomoč, kadar tuji organ uveljavlja zakone, ki prepovedujejo ravnanje, ki je po vsebini precej podobno ravnanju, prepovedanemu z zakoni, ki jih izvaja Zvezna komisija za trgovino ([1]). V okviru te pomoči lahko Zvezna komisija za trgovino izmenjuje informacije, pridobljene v zvezi z lastno preiskavo, izda prisilni postopek v imenu organa EU za zaščito podatkov, ki izvaja lastno preiskavo, in poišče ustna pričevanja prič ali obtoženih v zvezi z izvršilnim postopkom organa za zaščito podatkov v skladu z zahtevami ameriškega zakona o spletni varnosti (U.S. SAFE WEB Act). Zvezna komisija za trgovino redno uporablja to pooblastilo za pomoč drugim organom po svetu v zadevah glede zaščite zasebnosti in potrošnikov ([2]).

Poleg prednostne obravnave zadev, ki jih države članice EU in organizacije s samourejevalnim sistemom za varstvo zasebnosti predložijo v okviru zasebnostnega ščita ([3]), se Zvezna komisija za trgovino zavezuje preiskati morebitne kršitve okvira na lastno pobudo, kjer je primerno, z različnimi orodji.

Zvezna komisija za trgovino že več kot desetletje ohranja trden program preiskovanja zadev glede zasebnosti in varnosti, v katere so vpletene trgovske organizacije. V okviru teh preiskav je Zvezna komisija za trgovino redno pregledovala, ali se zadevni subjekti predstavljajo v okviru varnega pristana. Če se je subjekt tako predstavljal in je preiskava razkrila očitne kršitve načel zasebnosti varnega pristana, je Zvezna komisija za trgovino v uvedbo pregona vključila obtožbe kršitev varnega pristana. S tem dejavnim pristopom bomo nadaljevali tudi v novem okviru. Pomembno je poudariti, da Zvezna komisija za trgovino opravi mnogo več preiskav zadev, kot se jih konča z javno uvedbo pregona. Mnogo preiskav Zvezne komisije za trgovino je zaključenih, ker osebje ne ugotovi očitne kršitve zakonodaje. Ker so preiskave Zvezne komisije za trgovino nejavne in zaupne, zaključek preiskave pogosto ni objavljen.

Uvedba pregona Zvezne komisije za trgovino v skoraj 40 zadevah, ki se nanašajo na program varnega pristana, priča o zavezanosti agencije k dejavnemu uveljavljanju čezmejnih programov za varstvo zasebnosti. Zvezna komisija za trgovino bo iskala morebitne kršitve okvira v sklopu preiskav v zvezi z zasebnostjo in varnostjo, ki jih redno izvajamo.

III. OBRAVNAVANJE LAŽNIH ALI GOLJUFIVIH TRDITEV GLEDE ČLANSTVA V ZASEBNOSTNEM ŠČITU

Kakor je navedeno zgoraj, bo Zvezna komisija za trgovino ukrepala proti subjektom, ki lažno navajajo svoje sodelovanje v okviru. Zvezna komisija za trgovino bo prednostno obravnavala predložitve Ministrstva za trgovino v zvezi z organizacijami, za katere je ugotovilo, da se neustrezno predstavljajo kot aktualni člani okvira ali brez dovoljenja uporabljajo certifikacijsko oznako okvira.

Poleg tega opozarjamo, da v kolikor politika zasebnosti organizacije obljublja, da ta izpolnjuje načela zasebnostnega ščita, in se organizacija ne uspe registrirati pri Ministrstvu za trgovino, to samo po sebi ne oprosti organizacije od uveljavljanja zavez po tem okviru s strani Zvezne komisije za trgovino.

([1]) Pri ugotavljanju, ali uveljaviti svoje pooblastilo po ameriškem zakonu o spletni varnosti (U.S. SAFE WEB Act), Zvezna komisija za trgovino med drugim upošteva: „(A) ali se je organ, ki predloži zahtevo, strinjal, da zagotovi ali da bo zagotovil vzajemno pomoč komisiji; (B) ali bi izpolnitev zahteve posegla v javni interes Združenih držav; in (C) ali se preiskovalni ali izvršilni postopek organa, ki predloži zadevo, nanaša na dejanja ali ravnanje, ki povzroči ali je verjetno, da bo povzročilo, škodo precejšnjemu številu oseb.“ Člen 46(j) (3) naslova 15 zakonodajne zbirke ZDA. To pooblastilo ne velja za uveljavljanje zakonov o konkurenci.

([2]) V davčnih letih 2012–2015 je, na primer, Zvezna komisija za trgovino uporabila svoje pooblastilo v skladu z zakonom ZDA o spletni varnosti (U.S. SAFE WEB Act) za izmenjavo informacij pri odgovarjanju na skoraj 60 zahtev tujih organov in izdala skoraj 60 civilnih preiskovalnih zahtevkov (ki so enakovredni sodnim pozivom) za pomoč v 25 tujih preiskavah.

([3]) Čeprav Zvezna komisija za trgovino ne razrešuje ali izvaja mediacije pri posameznih pritožbah potrošnikov, pa potrjuje, da bo prednostno obravnavala zadeve v zvezi z zasebnostnim ščitom, ki jih predložijo organi za zaščito podatkov EU. Poleg tega Zvezna komisija za trgovino uporablja pritožbe v svoji podatkovni zbirki Consumer Sentinel, dostop do katere imajo mnogi drugi organi kazenskega pregona, da bi odkrila gibanja ter določila prednostne naloge pri pregonu in morebitne preiskovalne cilje. Posamezniki iz EU lahko za predložitev pritožbe Zvezni komisiji za trgovino uporabijo enak pritožbeni sistem, kakor je na voljo državljanom ZDA, in sicer na www.ftc.gov/complaint. Za posamezne pritožbe v okviru zasebnostnega ščita pa je morda najpriročnejše, da posamezniki iz EU predložijo pritožbe organu za zaščito podatkov v svoji državi članici ali drugemu organu za reševanje sporov.

IV. SPREMLJANJE ODLOKOV

Zvezna komisija za trgovino potrjuje tudi zavezo, da bo spremljala izvršilnih odlokov in tako zagotovila skladnost z okvirom zasebnostnega ščita.

Skladnost z okvirom bomo zahtevali skozi vrsto ustreznih prepovednih določb v prihodnjih odlokih FTC v zvezi z okvirom. To vključuje prepoved lažnih navedb v zvezi z okvirom in drugimi programi za varstvo zasebnosti, kadar so te podlaga za ukrep Zvezne komisije za trgovino.

Zadeve Zvezne komisije za trgovino, ki uveljavljajo prvotni program varnega pristana, so poučne. V 36 zadevah v zvezi z lažnimi ali goljufivimi navedbami certifikacije v varnem pristanu vsaka odločba tožencu prepoveduje lažno navajanje svojega sodelovanja v varnem pristanu ali katerem koli drugem programu za varstvo zasebnosti in varnost, ter od podjetja zahteva, da Zvezni komisiji za trgovino zagotovi poročila o skladnosti. V zadevah v zvezi s kršitvami načel zasebnosti varnega pristana je bilo določeno, da morajo podjetja izvajati celovite programe za varstvo zasebnosti in pridobiti neodvisne ocene tretjih strank v zvezi s temi programi vsako drugo leto v naslednjih dvajsetih letih, ki jih morajo predložiti Zvezni komisiji za trgovino.

Kršitve upravnih odlokov FTC lahko privedejo do denarnih kazni v višini do 16 000 ameriških dolarjev za posamezno kršitev ali 16 000 ameriških dolarjev na dan za nenehno kršenje ([1]),ki lahko v primeru ravnanja, ko je prizadeto veliko potrošnikov, znaša tudi več milijonov ameriških dolarjev. Vsak odlok za pridobivanje soglasij vsebuje tudi določbe v zvezi s poročanjem in skladnostjo. Subjekti, na katere se nanaša odlok, morajo hraniti dokumente, ki dokazujejo njihovo izpolnjevanje načel, določeno število let. Odloke je treba poslati tudi zaposlenim, ki so odgovorni za zagotavljanje izpolnjevanja odloka.

Zvezna komisija za trgovino sistematično spremlja izpolnjevanje odlokov v okviru varnega pristana kot pri vseh svojih odlokih. Zvezna komisija za trgovino resno jemlje uveljavljanje svojih odlokov v zvezi z varstvom zasebnosti in podatkov ter po potrebi vlaga tožbe za njihovo uveljavitev. Na primer, kakor je omenjeno zgoraj, je družba Google plačala denarno kazen v višini 22,5 milijona USD za razrešitev obtožb, da je kršila odlok FTC zoper njo. Pomembno je, da bodo odloki FTC še naprej ščitili vse potrošnike po svetu, ki sodelujejo s podjetjem, ne le tiste potrošnike, ki so vložili pritožbe.

Nazadnje, Zvezna komisija za trgovino bo še naprej vodila spletni seznam podjetij, za katera veljajo odloki v zvezi z uveljavljanjem programa varnega pristana in novega okvira zasebnostnega ščita ([2]). Poleg tega načela zasebnostnega ščita zdaj od podjetij, za katera velja odlok FTC ali sodna odločba zaradi neizpolnjevanja načel, da javno objavijo vse pomembne dele poročila o skladnosti ali oceni, povezanega z okvirom, ki ga predložijo Zvezni komisiji za trgovino, v obsegu, v katerem je to v skladu z zakoni in pravili o zaupnosti.

V. SODELOVANJE Z ORGANI ZA ZAŠČITO PODATKOV EU IN PRI UVELJAVLJANJU

Zvezna komisija za trgovino priznava pomembno vlogo, ki jo igrajo organi za zaščito podatkov EU glede skladnosti z okvirom, in spodbuja okrepljeno posvetovanje in sodelovanje pri uveljavljanju. Poleg morebitnih posvetov z organi za zaščito podatkov v zvezi s posameznimi zadevami, ki jih predložijo ti organi, se Zvezna komisija za trgovino zavezuje k sodelovanju na rednih sestankih z imenovanimi predstavniki delovne skupine iz člena 29, kjer bodo na splošno obravnavani načini za izboljšanje sodelovanja pri uveljavljanju glede na okvir. FTC bo skupaj s predstavniki Ministrstva za trgovino, Evropske komisije in delovne skupine iz člena 29 sodelovala tudi v letnem pregledu okvira, kjer bo obravnavala njegovo izvajanje.

Zvezna komisija za trgovino spodbuja tudi razvoj orodij, ki bodo okrepila sodelovanje pri uveljavljanju z organi za zaščito podatkov EU in drugimi organi za uveljavljanje varstva zasebnosti po svetu. Zvezna komisija za trgovino je skupaj s partnerji za uveljavljanje v Evropski uniji in po svetu lani uvedla sistem opozarjanja v okviru mreže za globalno uveljavljanje zasebnosti (Global Privacy Enforcement Network ali GPEN) za izmenjavo informacij o preiskavah in spodbujanje usklajenega uveljavljanja. Ta pripomoček GPEN za opozarjanje je lahko posebej uporaben v okviru zasebnostnega ščita. Zvezna komisija za trgovino in organi za zaščito podatkov EU bi ga lahko uporabili za usklajevanje v zvezi z okvirom in drugimi preiskavami varstva zasebnosti, tudi kot izhodišče za izmenjavo informacij za namene

([1]) Člen 45(m) naslova 15 zakonodajne zbirke ZDA. 16 C.F.R. člen 1.98.
([2]) Glej FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

zagotavljanja usklajene in učinkovitejše zaščite zasebnosti za potrošnike. Veselimo se nadaljnjega dela s sodelujočimi organi EU pri širšem vzpostavljanju sistema za opozarjanje GPEN in razvoju drugih orodij za izboljšanje sodelovanja v zadevah uveljavljanja zasebnosti, vključno s tistimi po okviru.

Zvezna komisija za trgovino z veseljem potrjuje svojo zavezo k uveljavljanju novega okvira zasebnostnega ščita. Prav tako se veselimo nadaljnjega sodelovanja s sodelavci iz EU pri zaščiti zasebnosti potrošnikov na obeh straneh Atlantika.

S spoštovanjem.

Edith Ramirez

Predsednica

Dodatek A

Okvir zasebnostnega ščita EU-ZDA v kontekstu: Pregled ureditve ZDA na področju zasebnosti in varnosti

Zaščitni ukrepi, ki jih nudi Okvir zasebnostnega ščita EU-ZDA (v nadaljevanju: Okvir), so umeščeni v kontekst širšega varstva zasebnosti, ki ga zagotavlja pravni sistem ZDA kot celota. Prvič, Zvezna komisija za trgovino že več kot desetletje izvaja trden program za zasebnost in varnost komercialnih praks v ZDA, ki varuje potrošnike po vsem svetu. Drugič, ureditev na področju varstva zasebnosti in varnosti v ZDA se je od leta 2000, ko je bil sprejet prvotni program varnega pristana med ZDA in EU, občutno razvila. Od takrat so bili sprejeti številni zvezni in državni zakoni o zasebnosti in varnosti, znatno pa se je povečalo tudi število javnih in zasebnih pravd zaradi izvrševanja pravice do zasebnosti. Varstvo posameznikov iz EU, ki ga nudi novi Okvir, dopolnjuje širok nabor pravnih ukrepov ZDA za varstvo zasebnosti in varnosti potrošnikov, ki se uporablja za prakse na področju komercialnih podatkov.

I. SPLOŠNI PROGRAM ZVEZNE KOMISIJE ZA TRGOVINO ZA IZVRŠEVANJE PRAVIC V ZVEZI Z ZASEBNOSTJO IN VARNOSTJO

Zvezna komisija za trgovino (Federal trade commission, v nadaljnjem besedilu: FTC) je vodilna agencija ZDA za varstvo potrošnikov, ki se osredotoča na zasebnost v okviru komercialnega sektorja. FTC je pooblaščena za pregon nepoštenih in goljufivih dejanj ali ravnanj, ki kršijo zasebnost potrošnikov, ter za uveljavljanje bolj ciljnih zakonov, ki varujejo določene informacije v zvezi s finančnimi in zdravstvenimi zadevami, informacije o otrocih ter informacije, ki se uporabljajo za sprejemanje nekaterih odločitev o primernosti v zvezi s potrošniki.

FTC ima izjemne izkušnje na področju uveljavljanja zasebnosti potrošnikov. Z izvršilnimi ukrepi FTC so se odpravljale nezakonite prakse v nespletnih in spletnih okoljih. FTC je na primer sprejela izvršilne ukrepe proti znanim podjetjem, kot so Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC in Snapchat ter tudi proti manj znanim podjetjem. FTC je vložila tožbe proti podjetjem, ki so domnevno pošiljala neželeno pošto potrošnikom, namestila vohunsko ali drugo zlonamerno programsko opremo na računalnike, goljufivo sledila potrošnikom po spletu, kršila zasebnost otrok, nezakonito zbirala informacije na mobilnih napravah potrošnikov in niso zavarovala z internetom povezanih naprav, ki so se uporabljale za shranjevanje osebnih informacij. Na tej podlagi izdane odredbe so praviloma nalagale stalno spremljanje s strani FTC za obdobje dvajsetih let in prepoved nadaljnjih kršitev zakonov, za kršitev teh odredb pa so podjetjem nalagale znatne denarne kazni ([1]). Opozoriti je treba, da odredbe FTC ne varujejo zgolj posameznikov, ki so se pritožili glede težave, temveč varujejo vse potrošnike, v prihodnje poslujejo s temi podjetji. V čezmejnem kontekstu je FTC pristojna za varstvo potrošnikov po vsem svetu pred praksami, ki se izvajajo v Združenih državah ([2]).

Do zdaj je FTC vložila več kot 130 tožb zaradi neželene elektronske pošte in vohunske programske opreme, več kot 120 tožb zaradi „prepovedi klicanja“ v okviru trženja po telefonu, več kot 100 tožb na podlagi zakona o pravičnem poročanju o kreditni sposobnosti, skoraj 60 tožb s področja varovanja podatkov, več kot 50 tožb s področja splošne zasebnosti, skoraj 30 tožb zaradi kršitve zakona Gramm-Leach-Bliley in več kot 20 tožb za izvrševanje zakona o varstvu zasebnosti otrok na spletu (Children's Online Privacy Protection Act, v nadaljnjem besedilu: COPPA) ([3]). Poleg teh primerov je FTC izdala in objavljala opozorila pisma ([4]).

([1]) Vsak subjekt, ki ne ravna v skladu z odredbo FTC, se lahko kaznuje z denarno kaznijo do 16 000 USD za posamezno kršitev ali 16 000 USD za vsak dan kršitve pri nadaljevalnih kršitvah. Glej člen 45(l) naslova 15 Zakonodajne zbirke ZDA in člen 1.98(c) zbirke zveznih predpisov št. 16.

([2]) Kongres je izrecno potrdil pooblastilo FTC za vlaganje pravnih sredstev, vključno z odškodninskimi zahtevki, zoper kakršna koli ravnanja, ki vključujejo zunanjo trgovino in ki (1) povzročajo ali je verjetno, da bodo povzročile, razumno predvidljivo škodo v Združenih državah ali (2) vključujejo bistveno ravnanje v Združenih državah. Glej člen 45(a)(4) naslova 15 Zakonodajne zbirke ZDA.

([3]) V nekaterih primerih se v tožbah komisije s področja zasebnosti in varstva podatkov zatrjuje, da je družba izvajala tako goljufive kot nepoštene prakse; ti primeri včasih vključujejo tudi domnevne kršitve več zakonov, kot so zakon o pravičnem poročanju o kreditni sposobnosti, zakon Gramm-Leach-Bliley in COPPA.

([4]) Glej na primer sporočilo za javnost Zvezne komisije za trgovino z naslovom FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (FTC opozarja družbo BabyBus, ki je izdelovalka aplikacij za otroke, na morebitne kršitve COPPA) (22. december 2014), na voljo na https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; sporočilo za javnost Zvezne komisije za trgovino z naslovom FTC Warns Data Broker Operations of Possible Privacy Violations (FTC opozarja posrednike podatkov o morebitnih kršitvah zasebnosti) (7. maj 2013), na voljo na https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations ter sporočilo za javnost Zvezne komisije za trgovino z naslovom FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (FTC opozarja posrednike podatkov, ki posredujejo zgodovino najemov najemnikov, da zanje morda velja zakon o pravičnem poročanju o kreditni sposobnosti) (3. april 2013), na voljo na https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

FTC je v svoji zgodovini strogega uveljavljanja zasebnosti tudi redno iskala morebitne kršitve programa varnega pristana. Od sprejetja programa varnega pristana je FTC začela številne preiskave glede izvajanja varnega pristana na lastno pobudo in vložila 39 tožb proti ameriškim družbam zaradi kršitev varnega pristana. FTC bo še naprej izvajala proaktiven pristop s tem, da si bo izvrševanje novega okvira zadala za prednostno nalogo.

II. ZVEZNI IN DRŽAVNI ZAŠČITNI UKREPI ZA ZASEBNOST POTROŠNIKOV

Pregled uveljavljanja varnega pristana, ki je dodan kot Priloga k odločbi Evropske komisije o ustreznosti varnega pristana, povzema številne zvezne in državne zakone o zasebnosti, ki so veljali v času sprejetja programa o varnem pristanu leta 2000 ([1]). V tem času so komercialno zbiranje in uporabo osebnih podatkov urejali številni zvezni zakoni razen člena 5 zakona o FTC, vključno z: zakonom o politiki kabelskih komunikacij (Cable Communications Policy Act), zakonom o varstvu zasebnosti voznikov (Driver's Privacy Protection Act), zakonom o zasebnosti elektronskih komunikacij (Electronic Communications Privacy Act), zakonom o elektronskem prenosu sredstev (Electronic Funds Transfer Act), zakonom o pravičnem poročanju o kreditni sposobnosti, zakonom Gramm-Leach-Bliley, zakonom o pravici do finančne zasebnosti, zakonom o varstvu telefonskih potrošnikov (Telephone Consumer Protection Act) in zakonom o varstvu zasebnosti videoposnetkov. Mnoge države so imele tudi analogno zakonodajo na teh področjih.

Od leta 2000 je prišlo do številnih sprememb na zvezni in državni ravni, ki zagotavljajo dodatno varstvo zasebnosti potrošnikov ([2]). Na zvezni ravni je na primer FTC leta 2013 spremenila predpis COPPA, da bi zagotovila številne dodatne zaščitne ukrepe za varstvo osebnih podatkov otrok. FTC je objavila tudi dve pravili za izvajanje zakona Gramm-Leach-Bliley – pravilo o zasebnosti in pravilo o zaščitnih ukrepih –, ki od finančnih institucij ([3]) zahtevata, da razkrivajo svoje prakse glede izmenjave informacij in uvedejo celovit program za varnost informacij, da bi zavarovale informacije o potrošnikih ([4]). Podobno tudi zakon o pravičnih in natančnih kreditnih transakcijah (Fair and Accurate Credit Transactions Act, v nadaljnjem besedilu: FACTA), sprejet leta 2003, dopolnjuje dolgoletno zakonodajo ZDA s področja posojil in določa zahteve za zakritje, izmenjavo in odstranitev nekaterih občutljivih finančnih podatkov. FTC je uvedla številna pravila na podlagi FACTA, ki se med drugim nanašajo na pravico potrošnikov do brezplačnega letnega poročila o kreditni sposobnosti; zahteve za varno odstranitev informacij iz poročil o potrošniških kreditih; pravico potrošnikov do neprejemanja določenih ponudb za posojila in zavarovanja; pravico potrošnikov, da se ne odločijo za uporabo podatkov, ki jih zagotavlja povezana družba zaradi trženja svojih proizvodov in storitev ter na zahtevo za finančne institucije in upnike, naj uvedejo programe za odkrivanje in preprečevanje kraje identitete ([5]). Poleg tega so bili leta 2013 spremenjeni predpisi, ki so bili razglašeni na podlagi zakona o prenosljivosti zdravstvenega zavarovanja in odgovornostih pri njem (Health Insurance Portability and Accountability Act), s čimer so bili dodani dodatni zaščitni ukrepi za varstvo zasebnosti osebnih informacij o zdravstvenem stanju ([6]). Začela so veljati tudi pravila, ki varujejo potrošnike pred neželenimi klici v okviru trženja po telefonu, avtomatskimi klici in neželeno elektronsko pošto. Kongres je prav tako sprejel zakone, ki od nekaterih družb, ki zbirajo informacije o zdravstvenem stanju, zahtevajo, da v primeru kršitve o tem obvestijo potrošnike ([7]).

Tudi države so bila zelo dejavne pri sprejemanju predpisov v zvezi z zasebnostjo in varnostjo. Od leta 2000 so sedeminštirideset držav, District of Columbia, Guam, Portoriko in Deviški otoki sprejeli predpise, v skladu s katerimi morajo

([1]) Glej poročilo Ministrstva ZDA za trgovino z naslovom Safe Harbor Enforcement Overview (pregled izvrševanja varnega pristana), https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) Za celovitejši pregled pravnega varstva v Združenih državah glej tudi Daniel J. Solove in Paul Schwartz, Information Privacy Law (Pravo zasebnosti informacij) (5. izdaja iz leta 2015).

([3]) Finančne institucije so v zakonu Gramm-Leach-Bliley opredeljena zelo široko in vključujejo vsa podjetja, ki so „znatno vključena" v ponujanje finančnih produktov ali storitev. Ta na primer vključujejo podjetja za vnovčevanje čekov, dajalce kratkoročnih posojil z dospelostjo ob naslednji plači, hipotekarne posrednike, nebančne posojilodajalce, cenilce osebnega premoženja ali nepremičnin in poklicne pripravljavce davčnih napovedi.

([4]) V skladu z zakonom o varstvu potrošnikov na področju finančnih storitev iz leta 2010 (Consumer Financial Protection Act, v nadaljnjem besedilu: CFPA), naslov X zbirke aktov Kongresa s področja javnega prava št. 111 do 203, 124, zakon št. 1955 (21. julij 2010) (znan tudi kot Dodd-Frank Wall Street Reform and Consumer Protection Act), je bila večina pooblastil FTC za sprejemanje pravil v skladu z zakonom Gramm-Leach-Bliley prenesena na organ za varstvo potrošnikov na finančnem področju (Consumer Financial Protection Bureau, v nadaljnjem besedilu: CFPB). FTC je ohranila izvršilna pooblastila v okviru zakona Gramm-Leach- Bliley ter zakonodajna pooblastila v zvezi s pravilom o zaščitnih ukrepih in omejena zakonodajna pooblastila v okviru pravila o zasebnosti v zvezi s trgovci z avtomobili.

([5]) V skladu s CFPA FTC deli svojo izvršilno vlogo glede zakona o poštenem kreditnem poročanju s CFPB, zakonodajna pooblastila pa so bila v veliki meri prenesena na CFPB (z izjemo pravil o opozorilih in odstranjevanju).

([6]) Glej zbirko zveznih predpisov št. 45, točke 160, 162 in 164.

([7]) Glej npr. zakon o oživljanju gospodarstva in ponovnih naložbah v ZDA (American Recovery & Reinvestment Act) iz leta 2009, zbirka aktov Kongresa s področja javnega prava št. 111-5, 123 zakon št. 115 (2009) in ustrezne predpise, zbirka zveznih predpisov št. 45, členi 164.404 do 164.414; zbirka zveznih predpisov št. 16, točka 318.

podjetja obvestiti posameznike o kršitvah varnosti osebnih podatkov ([1]). Najmanj dvaintrideset držav in Portoriko imajo zakone o odstranitvi podatkov, ki določajo zahteve za uničenje ali odstranitev osebnih informacij ([2]). Več držav je sprejelo tudi splošne zakone o varstvu podatkov. Poleg tega je Kalifornija sprejela več različnih zakonov o zasebnosti, tudi zakon, ki od podjetij zahteva, da oblikujejo politike varovanja zasebnosti in razkrivajo svoje prakse glede funkcij „ne sledi“ ([3]), zakon o „osvetljevanju“, ki zahteva večjo preglednost pri posrednikih podatkov ([4]), ter zakon, ki uvaja „gumb za izbris“, ki mladoletnikom omogoča, da zahtevajo izbris nekaterih informacij na družbenih medijih ([5]). Zvezna vlada in državne vlade so z uporabo teh zakonov in drugih pooblastil naložile znatne kazni podjetjem, ki niso dovolj zaščitila zasebnosti in varnosti osebnih podatkov potrošnikov ([6]).

Zasebne tožbe so privedle tudi do ugodnih sodb in poravnav, ki zagotavljajo dodatno varstvo zasebnosti in varnosti podatkov za potrošnike. Leta 2015 je na primer družba Target privolila v plačilo 10 milijonov USD v okviru poravnave s strankami, ki so trdile, da so bile njihove osebne finančne informacije ogrožene zaradi vsesplošnih kršitev varnosti osebnih podatkov. Leta 2013 je družba AOL pristala na plačilo poravnave v višini 5 milijonov USD, da bi rešila skupinsko tožbo zaradi domnevno nezadostne odprave prepoznavnosti v zvezi z objavo poizvedb stotisočev članov AOL. Poleg tega je Zvezno sodišče odobrilo plačilo 9 milijonov USD družbe Netflix zaradi domnevnega vodenje evidenc o zgodovini najemov v nasprotju z zakonom o varstvu zasebnosti videoposnetkov (Video Privacy Protection Act) iz leta 1988. Na zveznih sodiščih v Kaliforniji sta bili sklenjeni ločeni poravnavi z družbo Facebook, ena v višini 20 milijonov USD in druga v višini 9,5 milijona USD, zaradi zbiranja, uporabe in izmenjave osebnih podatkov uporabnikov, ki jih je izvajala ta družba. Leta 2008 pa je državno sodišče Kalifornije odobrilo poravnavo v višini 20 milijonov USD z družbo LensCrafters zaradi nezakonitega razkritja zdravstvenih podatkov njenih strank.

Na kratko, ta povzetek dokazuje, da Združene države zagotavljajo občutno pravno varstvo zasebnosti in varnosti potrošnikov. Novi okvir zasebnostnega ščita, ki zagotavlja pomembne zaščitne ukrepe za posameznike iz EU, bo vključen v ta širši okvir, v katerem bo varstvo zasebnosti in varnosti potrošnikov še naprej pomembna prednostna naloga.

([1]) Glej npr. Nacionalna konferenca državnih zakonodajalcev (National Conference of State Legislatures, v nadaljnjem besedilu: NCSL), State Security Breach Notification Laws (Državni zakoni o obveščanju o kršitvah varnosti) (4. januar 2016), na voljo na: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, Data Disposal Laws (Zakoni o odstranjevanju podatkov) (12. januar 2016), na voljo na: http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Gospodarski in poklicni zakonik Kalifornije, členi 22575 do 22579.

([4]) Civilni zakonik Kalifornije, členi 1798.80 do 1798.84.

([5]) Gospodarski in poklicni zakonik Kalifornije, členi 22580 do 22582.

([6]) Glej Jay Cline, U.S. Takes the Gold in Doling Out Privacy Fines (ZDA prve pri nalaganju glob v zvezi z zasebnostjo), Computerworld (17. februar 2014), na voljo na: http://www.computerworld.com/s/article/9246393/JayClineU.S.takesthegoldindolingoutprivacyfines?taxonomyId=17&pageNumber=1.

PRILOGA V

Pismo Ministra za prevoz ZDA Anthonyja Foxxa

19. februar 2016

Komisarka Věra Jourová
Evropska komisija
Rue de la Loi/Wetstraat 200
1049 Bruselj
Belgija

V odgovor na: Okvir zasebnostnega ščita EU-ZDA

Spoštovana komisarka Jourová,

Ministrstvo za promet ZDA (v nadaljevanju: Ministrstvo) se zahvaljuje za priložnost, da opiše svojo vlogo pri uveljavljanja okvira zasebnostnega ščita EU-ZDA. Ta okvir igra ključno vlogo pri zaščiti osebnih podatkov, pridobljenih med trgovinskim poslovanjem v vedno bolj povezanem svetu. Podjetjem omogoča izvajanje pomembnih operacij v svetovnem gospodarstvu, obenem pa bo zagotovil, da potrošniki iz EU obdržijo pomembno varstvo zasebnosti.

Ministrstvo je prvič javno izrazilo svojo zavezo k uveljavljanju okvira varnega pristana v pismu, poslanem Evropski komisiji pred 15 leti. Ministrstvo se je v tem pismu zavezalo, da bo odločno uveljavljalo načela zasebnosti varnega pristana. Ministrstvo še naprej ohranja to zavezo in jo zapisuje v tem pismu.

Ministrstvo zlasti obnavlja svojo zavezo na spodnjih ključnih področjih: (1) prednostna obravnava preiskav domnevnih kršitev zasebnostnega ščita; (2) ustrezen kazenski pregon proti subjektom, ki lažno ali goljufivo navajajo certifikacijo v okviru zasebnostnega ščita; ter (3) spremljanje in javna objava izvršilnih odlokov v zvezi s kršitvami zasebnostnega ščita. Zagotavljamo informacije o vsaki od teh zavez in za potreben kontekst tudi ustrezno ozadje vloge Ministrstva pri zaščiti zasebnosti potrošnikov in uveljavljanju okvira zasebnostnega ščita.

I. OZADJE

A. **Pooblastilo Ministrstva za promet glede varstva zasebnosti**

Ministrstvo je trdno zavezano k zagotavljanju zasebnosti informacij, ki jih potrošniki dajo letalskim prevoznikom in agencijam za prodajo letalskih vozovnic. Pooblastilo Ministrstva za ukrepanje na tem področju je navedeno v členu 41712 naslova 49 zakonodajne zbirke ZDA, ki prevozniku ali agenciji za prodajo letalskih vozovnic prepoveduje „nepošteno ali goljufivo ravnanje ali nelojalno konkurenco“ pri prodaji zračnega prevoza, ki povzroči ali obstaja verjetnost, da povzroči, škodo potrošnikom. Člen 41712 je oblikovan po členu 5 zakona o FTC (Federal Trade Commission Act) (člen 45 naslova 15 zakonodajne zbirke ZDA). Določbo o nepoštenem ali goljufivem ravnanju razlagamo kot prepoved letalskim prevoznikom in agencijam za prodajo letalskih vozovnic, da: (1) kršijo pogoje svoje politike zasebnosti ali (2) zbirajo ali razkrivajo zasebne informacije na način, ki krši javni red, je nemoralen ali povzroči bistveno škodo potrošnikom, ki je ne nadomesti nobena kompenzacijska ugodnost. Člen 41712 razlagamo tudi kot prepoved za letalske prevoznike in agencija za prodajo letalskih vozovnic, da: (l) kršijo katero koli pravilo, ki ga izda Ministrstvo in ki določa posamezno ravnanje v zvezi varstvom zasebnosti kot nepošteno ali goljufivo; ali (2) kršijo zakon o varstvu zasebnosti otrok na spletu (COPPA) ali pravila Zvezne komisije za trgovino, ki izvajajo COPPA. V skladu z zveznim zakonom ima Ministrstvo izključno pristojnost za urejanje praks letalskih prevoznikov v zvezi z varstvom zasebnosti, v zvezi s praksami agencij za prodajo letalskih vozovnic pa si deli pristojnost z Zvezno komisijo za trgovino.

Ko se prevoznik ali prodajalec zračnega prevoza javno zaveže k načelom zasebnosti iz okvira zasebnostnega ščita, lahko Ministrstvo kot tako uporabi zakonske pristojnosti iz člena 41712 za zagotovitev skladnosti z navedenimi načeli. Ko torej potnik da podatke letalskemu prevozniku ali agenciji za prodajo letalskih vozovnic, ki se je zavezal(-a) k načelom zasebnosti v okviru zasebnostnega ščita, vsako neizpolnjevanje teh načel letalskega prevoznika ali agencije za prodajo letalskih vozovnic pomeni kršitev člena 41712.

B. **Prakse izvrševanja**

Urad za izvrševanje in postopke v letalstvu (Office of Aviation Enforcement and Proceedings ali Aviation Enforcement Office) v okviru Ministrstva opravlja preiskave in pregon po členu 41712 naslova 49 zakonodajne zbirke ZDA. Uveljavlja zakonsko prepoved v členu 41712 proti nepoštenemu in goljufivemu ravnanju, zlasti s pogajanji ter pripravo odlokov o prepovedi in odlokov za oceno denarne kazni. Urad izve za morebitne kršitve predvsem iz pritožb, ki jih prejme od posameznikov, potovalnih agencij, letalskih prevoznikov in organov ameriške in tujih vlad. Potrošniki lahko proti letalskim prevoznikom in agencijam za prodajo letalskih vozovnic vložijo pritožbe v zvezi z varstvom zasebnosti na spletni strani Ministrstva za promet ([1]).

Če v zadevi ni dosežena razumna in ustrezna rešitev, ima Aviation Enforcement Office pristojnost, da uvede izvršilni postopek, ki vključuje predhodno obravnavo pred upravnim sodnikom Ministrstva za promet. Upravni sodni ima pristojnost za izdajo odlokov o prepovedi in denarnih kazni. Posledica kršitev člena 41712 je lahko izdaja odloka o prepovedi ter odredba denarne kazni v višini do 27 500 ameriških dolarjev za vsako kršitev člena 41712.

Ministrstvo nima pristojnosti za dodelitev odškodnine ali zagotovitev denarnega nadomestila posameznim pritožnikom. Vendar pa ima Ministrstvo pristojnost za odobritev poravnav na podlagi preiskav, ki jih je opravil Aviation Enforcement Office in ki neposredno koristijo potrošnikom (npr. gotovina, boni), kot poravnavo za denarne kazni, ki jih je sicer treba plačati vladi ZDA. To se je zgodilo že v preteklosti in se lahko zgodi tudi v okviru načel zasebnostnega ščita, kadar to omogočajo okoliščine. Ob ponavljajočih se kršitvah člena 41712, ki jih zagreši letalski prevoznik, bi se pojavilo vprašanje o pripravljenosti letalskega prevoznika, da ravna v skladu z načeli, kar se lahko v izjemno hudih primerih konča z ugotovitvijo, da letalski prevoznik ni več sposoben opravljati dejavnost, in torej z izgubo pooblastila za opravljanje gospodarske dejavnosti.

Do danes je Ministrstvo prejelo razmeroma malo število pritožb v zvezi z domnevnimi kršitvami zasebnosti agencij za prodajo letalskih vozovnic in letalskih prevoznikov. Ko je pritožba vložena, je preiskana glede na načela, določena zgoraj.

C. **Pravno varstvo Ministrstva za promet v korist potrošnikom iz EU**

V skladu s členom 41712 se prepoved nepoštenega ali goljufivega ravnanja v letalskem prevozu ali prodaji letalskega prevoza nanaša na ameriške in tuje letalske prevoznike ter agencije za prodajo letalskih vozovnic. Ministrstvo za promet pogosto ukrepa proti ameriškim in tujim letalskim prevoznikom v zvezi z ravnanjem, ki vpliva tako na tuje kot tudi ameriške potrošnike, na podlagi tega, da se je tako ravnanje letalskega prevoznika zgodilo v toku zagotavljanja prevoza v in iz ZDA. Ministrstvo za promet bo še naprej uporabljalo vsa pravna sredstva, ki so na voljo za zaščito tujih in ameriških potrošnikov pred nepoštenim ali goljufivim ravnanjem reguliranih subjektov v letalskem prevozu.

V zvezi z letalskimi prevozniki Ministrstvo za promet uveljavlja tudi druge ciljne zakone, katerih varstvo zajema potrošnike zunaj ZDA, kot je zakon COPPA. Zakon COPPA med drugim od upravljavcev spletnih strani in storitev, namenjenih otrokom, ali strani za splošno občinstvo, ki zavestno zbirajo osebne informacije od otrok, starih do 13 let, zahteva, da obvestijo starše in pridobijo preverljivo soglasje staršev. Ameriške spletne strani in storitve, za katere velja zakon COPPA in ki zbirajo osebne informacije tujih otrok, so dolžne upoštevati zakon COPPA. Tuje spletne strani in storitve morajo prav tako upoštevati zakon COPPA, če so usmerjene v otroke v Združenih državah ali če zavestno zbirajo osebne informacije otrok v Združenih državah. Če ameriški ali tuji letalski prevozniki, ki poslujejo v Združenih državah, kršijo zakon COPPA, je Ministrstvo za promet pristojno za uvedbo pregona.

II. UVELJAVLJANJE ZASEBNOSTNEGA ŠČITA

Če se letalski prevoznik ali agencija za prodajo letalskih vozovnic odloči sodelovati v okviru zasebnostnega ščita in Ministrstvo prejme pritožbo, da je tak letalski prevoznik ali agencija za prodajo letalskih vozovnic domnevno kršil okvir, Ministrstvo sprejme naslednje ukrepe za odločno uveljavljanje okvira.

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

A. **Prednostna obravnava preiskave domnevnih kršitev**

Aviation Enforcement Office v okviru Ministrstva bo preiskal vsako pritožbo glede domnevnih kršitev zasebnostnega ščita (vključno s pritožbami, prejetimi od organov za zaščito podatkov EU) in uvedel pregon, kjer obstajajo dokazi o kršitvi. Poleg tega bo Aviation Enforcement Office sodeloval z Zvezno komisijo za trgovino in Ministrstvom za trgovino ter prednostno obravnaval obtožbe, da regulirani subjekti ne izpolnjujejo zavez v zvezi z varstvom zasebnosti, ki so jih sprejeli v okviru zasebnostnega ščita.

Ob prejemu obtožbe glede kršitve okvira zasebnostnega ščita lahko Aviation Enforcement Office v okviru Ministrstva sprejme različne ukrepe v sklopu svoje preiskave. Na primer, pregleda lahko politike o zasebnosti agencije za prodajo letalskih vozovnic ali letalskega prevoznika, pridobi nadaljnje informacije od agencije za prodajo letalskih vozovnic, letalskega prevoznika ali tretjih strank, ter s subjektom, ki je predložil zadevo, le-to nadalje spremlja in oceni, ali obstaja vzorec kršitev ali precejšnje število prizadetih potrošnikov. Poleg tega bi določilo, ali ima lahko zadeva posledice na področju, ki ga ureja Ministrstvo za trgovino in Zvezna komisija za trgovino, in ocenilo, ali bi bilo izobraževanje potrošnikov in podjetij koristno, ter po potrebi uvedlo pregon.

Če Ministrstvo izve za morebitne kršitve zasebnostnega ščita agencij za prodajo letalskih vozovnic, bo zadevo uskladilo z Zvezno komisijo za trgovino. O izidu morebitnega pregona v okviru zasebnostnega ščita bomo obvestili Zvezno komisijo za trgovino in Ministrstvo za trgovino.

B. **Obravnavanje lažnih ali goljufivih trditev glede članstva**

Ministrstvo ostaja zavezano k preiskovanju kršitev zasebnostnega ščita, vključno z lažnimi ali goljufivimi trditvami članstva v programu zasebnostnega ščita. Prednostno bomo obravnavali zadeve, ki jih predloži Ministrstvo za trgovino v zvezi z organizacijami, za katere je ugotovilo, da se neustrezno predstavljajo kot aktualni člani zasebnostnega ščita ali brez dovoljenja uporabljajo certifikacijsko oznako okvira zasebnostnega ščita.

Poleg tega opozarjamo, da v kolikor politika zasebnosti organizacije obljublja, da izpolnjuje bistvena načela zasebnostnega ščita, in se organizaciji ne uspe registrirati pri Ministrstvu za trgovino, to samo po sebi ne oprosti organizacije od uveljavljanja teh zavez s strani Ministrstva za promet.

C. **Spremljanje in javna objava izvršilnih odlokov v zvezi s kršitvami zasebnostnega ščita**

Aviation Enforcement Office v okviru Ministrstva se še naprej zavezuje, da bo spremljalo izvršilne odloke, kakor so potrebni za zagotavljanje skladnosti s programom zasebnostnega ščita. Zlasti, če urad izda odlok, ki letalskemu prevozniku ali agenciji za prodajo letalskih vozovnic prepoveduje nadaljnje kršitve zasebnostnega ščita in člena 41712, bo spremljal subjektovo izpolnjevanje določbe o prepovedi v odloku. Poleg tega bo urad zagotovil, da bodo odloki, ki izhajajo iz zadev zasebnostnega ščita, na voljo na njegovi spletni strani.

Veselimo se nadaljnjega dela z našimi zveznimi partnerji in deležniki iz EU v zadevah zasebnostnega ščita.

Upam, da vam bodo ta pojasnila v pomoč. Če boste imeli še kakšno vprašanje ali če boste potrebovali nadaljnja pojasnila, mi, prosim, brez oklevanja sporočite.

S spoštovanjem

Anthony R. Foxx

Minister za promet

PRILOGA VI

Pismo glavnega pravnika Roberta Litta
Urad direktorja nacionalne obveščevalne službe

22. februar 2016

Justin S. Antonipillai
Svetovalec
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Namestnik pomočnika ministra
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Spoštovana g. Antonipillai in g. Dean,

v preteklih dveh letih in pol so Združene države v okviru pogajanj v zvezi z zasebnostnim ščitom EU-ZDA zagotovile precej informacij o delovanju ameriške obveščevalne skupnosti pri zbiranju informacij v okviru SIGINT. Te vključujejo informacije o veljavnem pravnem okviru, večplastni nadzor teh dejavnosti, široko preglednost teh dejavnosti in celovito varstvo zasebnosti in državljanskih svoboščin, da bi Evropski komisiji pomagali doseči sklep o ustreznosti tega varstva glede na izjeme načel zasebnostnega ščita v zvezi z nacionalno varnostjo. Ta dokument povzema podane informacije.

I. PPD-28 IN IZVAJANJE OBVEŠČEVALNE DEJAVNOSTI SIGINT

Ameriška obveščevalna skupnost zbira tuje obveščevalne podatke na skrbno nadzorovan način strogo v skladu z zakonodajo ZDA in več plastmi nadzora, pri čemer je poudarek na pomembnih prednostnih nalogah v zvezi s tujimi obveščevalnimi podatkih in nacionalno varnostjo. Zbiranje obveščevalnih podatkov v okviru obveščevalnih dejavnosti SIGINT v ZDA ureja več zakonov in politik, vključno z Ustavo ZDA, zakonom o nadzoru tujih obveščevalnih podatkov (Foreign Intelligence Surveillance Act; člen 1801 in naslednji naslova 50 Zakonodajne zbirke ZDA), odredbo št. 12333 in njenimi izvedbenimi postopki, predsedniškimi smernicami ter številnimi postopki in smernicami, ki jih odobrita sodišče FISA in državni tožilec in ki vzpostavljajo dodatna pravila, ki omejujejo zbiranje, hranjenje, uporabo in širjenje tujih obveščevalnih podatkov ([1]).

a. **Pregled PPD-28**

Januarja 2014 je predsednik Obama v svojem govoru povzel različne reforme ameriških obveščevalnih dejavnost SIGINT in izdal predsedniško politično direktivo 28 (Presidential Policy Directive 28 ali PPD-28) v zvezi s temi dejavnostmi ([2]). Predsednik je poudaril, da obveščevalne dejavnosti SIGINT, ki jih izvajajo ZDA, pomagajo varovati ne le našo državo, temveč tudi naše svobode ter varnost in svobode drugih držav, vključno z državami članicami EU, ki se zanašajo na informacije ameriških obveščevalnih agencij, da bi zaščitili svoje državljane.

PPD-28 določa niz načel in zahtev, ki veljajo za vse ameriške obveščevalne dejavnosti SIGINT ter za vse ljudi ne glede na njihovo narodnost ali kraj. Zlasti določa nekatere zahteve za postopke za obravnavo zbiranja, hranjenja in širjenja osebnih informacij o nedržavljanih ZDA, pridobljenih v skladu s SIGINT. Te zahteve so podrobneje določene spodaj, toda če jih povzamemo:

— PPD znova ponavlja, da Združene države zbirajo obveščevalne podatke s SIGINT le v okviru zakona, odredbe ali druge predsedniške direktive.

([1]) Nadaljnje informacije v zvezi s tujimi obveščevalnimi dejavnostmi ZDA so objavljene na spletu in javno dostopne prek obveščevalne skupnosti v evidenci Record (www.icontherecord.tumblr.com), tj. javni spletni strani Urada direktorja nacionalne obveščevalne službe, ki je namenjena večanju prepoznavnosti obveščevalnih dejavnosti vlade v javnosti.
([2]) Na voljo na https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— PPD vzpostavlja postopke, ki zagotavljajo, da se SIGINT izvaja le za zakonite in pooblaščene potrebe nacionalne varnosti.

— PPD zahteva tudi, da so zasebnost in državljanske svoboščine bistveni vprašanji pri načrtovanju zbiranja obveščevalnih podatkov v okviru SIGINT. Združene države zlasti ne zbirajo obveščevalnih podatkov za zatiranje ali obremenjevanje kritik ali nestrinjanja; da bi prikrajšale osebe na podlagi njihove narodnosti, rase, spola, spolne usmerjenosti ali vere; ali da bi ameriškim podjetjem in poslovnim sektorjem omogočile konkurenčno poslovno prednost.

— PPD predpisuje, da mora biti zbiranje obveščevalnih podatkov v okviru SIGINT prilagojeno tako, da je izvedljivo in da se lahko množilno zbrani obveščevalni podatki v okviru SIGINT uporabijo zgolj za posebej navedene namene.

— PPD določa, da mora obveščevalna skupnost sprejeti postopke, „ki so ustrezni oblikovani za zmanjševanje širjenja in hranjenja osebnih informacij, zbranih v okviru SIGINT," in zlasti širi določene elemente varstva, kakor so zagotovljeni za osebne informacije državljanov ZDA, na osebne informacije nedržavljanov ZDA.

— Postopki agencije za izvajanje PPD-28 so sprejeti in objavljeni.

Veljavnost postopkov in varstva, določenega v tem dokumentu za zasebnostni ščit, je jasna. Ko so podatki preneseni korporacijam v Združenih državah v skladu z zasebnostnim ščitom ali s kakršnimi koli sredstvi, lahko ameriške obveščevalne agencije zahtevajo te podatke od teh korporacij le, če je zahteva v skladu z zakonom o nadzoru tujih obveščevalnih podatkov ali z eno od zakonskih določb sodnega poziva v zvezi z nacionalno varnostjo, ki so obravnavane spodaj ([1]). Poleg tega, ne da bi potrdil ali zanikal poročila medijev o tem, da obveščevalna skupnost ZDA zbira podatke po čezatlantskih kabelskih vezah med prenosom v Združene države, če bi obveščevalna skupnost ZDA zbirala podatke po čezatlantskih kabelskih vezah, bi to naredila v skladu z omejitvami in zaščitnimi ukrepi, določenimi v tem dokumentu, vključno z zahtevami PPD-28.

b. **Omejitve zbiranja**

PPD-28 določa vrsto pomembnih splošnih načel, ki urejajo zbiranje obveščevalnih podatkov v okviru SIGINT:

— Zbiranje obveščevalnih podatkov v okviru SIGINT mora dovoljevati zakon ali predsedniško pooblastilo ter mora biti izvedeno v skladu z Ustavo in zakonom.

— Zasebnost in državljanske svoboščine morajo biti osrednji pomisleki pri načrtovanju obveščevalnih dejavnosti SIGINT.

— Obveščevalni podatki SIGINT se bodo zbirali le, kadar obstaja veljavna potreba za tuje obveščevalne podatke ali protiobveščevalno dejavnost.

— Združene države ne bodo zbirale obveščevalnih podatkov v okviru SIGINT za namene zatiranja ali obremenjevanja kritik ali nestrinjanja.

— Združene države ne bodo zbirale obveščevalnih podatkov v okviru SIGINT za prikrajšanje ljudi na podlagi njihove narodnosti, rase, spola, spolne usmerjenosti ali vere.

— Združene države ne bodo zbirale obveščevalnih podatkov v okviru SIGINT, da bi podjetjem in poslovnim sektorjem iz ZDA omogočile konkurenčno poslovno prednost.

— Ameriška obveščevalna dejavnost SIGINT mora biti *vedno* tako prilagojena, kot je izvedljiva, ob upoštevanju razpoložljivosti drugih virov informacij. To med drugim pomeni, da se, kadar koli je izvedljivo, obveščevalne dejavnosti SIGINT izvajajo usmerjeno namesto množično.

Zahteva, da je obveščevalna dejavnost SIGINT „tako prilagojena, kot je izvedljiva", se nanaša na način, na katerega se zbirajo obveščevalni podatki v okviru SIGINT, kot tudi na to, kaj se dejansko zbira. Na primer, pri določanju, ali zbirati

([1]) Organi kazenskega pregona ali nadzorni organi lahko zahtevajo informacije od korporacij za preiskovalne namene v Združenih državah v skladu z drugimi kazenskimi, civilnimi in regulativnimi pooblastili zunaj okvira tega dokumenta, ki je omejen na pooblastila v okviru nacionalne varnosti.

obveščevalne podatke v okviru SIGINT, mora obveščevalna skupnost upoštevati razpoložljivost drugih virov informacij, vključno z diplomatskimi ali javnimi viri, ter, kjer je ustrezno in izvedljivo, dati prednost zbiranju z drugimi sredstvi. Poleg tega bi morale politike članov obveščevalne skupnosti, kadar je izvedljivo, zahtevati, da je zbiranje osredotočeno na posebne tuje obveščevalne cilje ali teme z uporabo diskriminant (npr. posebni instrumenti, izbirni izrazi in identifikatorji).

Pomembno je, da se informacije, zagotovljene Komisiji, obravnavajo kot celota. Odločitve o tem, kaj je „izvedljivo“ ali „uresničljivo“, niso prepuščene presoji posameznikov, temveč zanje veljajo politike, ki so jih agencije izdale po PPD-28 in ki so javno dostopne, ter drugi procesi, opisani v navedenem dokumentu ([1]). Kakor pravi PPD-28, je množično zbiranje obveščevalnih podatkov v okviru SIGINT zbiranje podatkov, ki „se zaradi tehničnih ali operativnih pomislekov pridobivajo brez uporabe diskriminant (npr. posebni identifikatorji, izbirni izrazi itd.)“. V tem pogledu PPD-28 priznava, da morajo člani obveščevalne skupnosti zbirati velike količine obveščevalnih podatkov v okviru SIGINT v določenih okoliščinah, da bi odkrili nove ali nastajajoče grožnje in pridobili druge bistvene informacije v zvezi z nacionalno varnostjo, ki so pogosto skrite v velikem in kompleksnem sistemu sodobnih globalnih komunikacij. Prav tako priznava pomisleke glede zasebnosti in državljanskih svoboščin, sprožene ob množičnem zbiranju obveščevalnih podatkov v okviru SIGINT. PPD-28 torej predpisuje, da obveščevalna skupnost prednostno razvrsti alternativne možnosti, ki bi omogočile izvajanje usmerjene obveščevalne dejavnosti SIGINT namesto množičnega zbiranja obveščevalnih podatkov v okviru SIGINT. Temu ustrezno bi morali, kadar je izvedljivo, člani obveščevalne skupnosti izvajati usmerjeno zbiranje v okviru SIGINT, namesto da množično zbirajo obveščevalne podatke v okviru SIGINT ([2]). Ta načela zagotavljajo, da izjema za množično zbiranje ne spodkopa splošnega pravila.

Koncept „razumnosti“ pa je temeljno načelo zakonodaje ZDA. Pomeni, da članom obveščevalne skupnosti ne bo treba sprejeti nobenega teoretično možnega ukrepa, temveč bodo morali uskladiti svoja prizadevanja za zaščito zakonitih interesov v zvezi z varstvom zasebnosti in državljanskih svoboščin s praktičnimi potrebami obveščevalnih dejavnosti SIGINT. Tudi tukaj so politike agencij dostopne in lahko dajo zagotovilo, da izraz „razumno oblikovan za zmanjševanje širjenja in hranjenja osebnih informacij“ ne spodkopa splošnega pravila.

PPD-28 prav tako določa, da je mogoče množično zbrane obveščevalne podatke v okviru SIGINT uporabiti le za šest posebnih namenov: zaznavanje in preprečevanje določenih dejavnosti tujih sil; boj proti terorizmu; preprečevanje širjenja orožja; kibernetska varnost; odkrivanje in preprečevanje groženj za ZDA ali zavezniške oborožene sile in boj proti nadnacionalnim grožnjam za kazniva dejanja, vključno z izmikanjem sankcijam. Predsednikov svetovalec za nacionalno varnost bo v posvetovanju z direktorjem nacionalne obveščevalne službe vsako leto pregledal te dovoljene uporabe množično zbranih obveščevalnih podatkov v okviru SIGINT in določil, ali jih je treba spremeniti. Direktor nacionalne obveščevalne službe bo javno objavil ta seznam, kolikor je to izvedljivo v skladu z nacionalno varnostjo. To omogoča pomembno in pregledno omejitev uporabe množičnega zbiranja obveščevalnih podatkov v okviru SIGINT.

Poleg tega so člani obveščevalne skupnosti, ki izvajajo PPD-28, okrepili analitične prakse in standarde za poizvedovanje neocenjenih obveščevalnih podatkov v okviru SIGINT ([3]). Analitiki morajo oblikovati svoje poizvedbe ali druge iskalne izraze in tehnike tako, da zagotovijo njihovo ustreznost pri odkrivanju obveščevalnih podatkov, ki se nanašajo na veljavno nalogo v zvezi s tujimi obveščevalnimi podatki ali kazenskim pregonom. V ta namen morajo člani obveščevalne skupnosti osredotočiti poizvedbe o osebah na kategorije obveščevalnih podatkov SIGINT glede na zahtevo o tujih obveščevalnih podatkih ali kazenskem pregonu, da bi preprečili uporabo osebnih informacij, ki se ne nanašajo na zahteve glede tujih obveščevalnih podatkov ali kazenskega pregona.

Pomembno je poudariti, da se vsaka dejavnost množičnega zbiranja podatkov v zvezi s komunikacijo po internetu, ki jo izvaja ameriška obveščevalna skupnost z dejavnostjo SIGINT, izvaja na majhnem deležu interneta. Poleg tega uporaba ciljnih poizvedb, kakor je opisano zgoraj, zagotavlja, da so v pregled analitiku predstavljeni samo tisti deli, ki naj bi imeli potencialno obveščevalno vrednost. Te omejitve so namenjene zaščiti zasebnosti in državljanskih svoboščin vseh oseb ne glede na njihovo narodnost in kraj bivanja.

([1]) Na voljo na www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Ti postopki izvajajo usmerjene in prilagojene koncepte, obravnavane v tem pismu, na način, ki je značilen za posameznega člana obveščevalne skupnosti.

([2]) Če navedem en primer, postopki Agencije ZDA za nacionalno varnost (NSA) za izvajanje PPD-28 navajajo, da „kadar koli je izvedljivo, se zbiranje izvaja z uporabo enega ali več izbirnih izrazov, da bi zbiranje usmerili na posebnih tuje obveščevalne cilje (npr. poseben znani mednarodni terorist ali teroristična skupina) ali posebne tuje obveščevalne teme (npr. širjenje orožja za množično uničevanje s strani tuje sile ali njenih agentov)“.

([3]) Na voljo na http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Združene države so izpopolnile postopke in tako zagotovile, da se obveščevalne dejavnosti SIGINT izvajajo le za ustrezne potrebe nacionalne varnosti. Vsako leto predsednik določi najpomembnejše prednostne naloge države pri zbiranju tujih obveščevalnih podatkov po obsežnem uradnem medagencijskem postopku. Direktor nacionalne obveščevalne službe je dolžan prenesti te prednostne naloge v obveščevalni dejavnosti v nacionalni okvir prednostnih nalog v obveščevalni dejavnosti ali NIPF (National Intelligence Priorities Framework). PPD-28 je okrepil in izboljšal medagencijski postopek, da bi zagotovil pregled vseh prednostnih nalog obveščevalne skupnosti in njihovo odobritev s strani načrtovalcev politik na visoki ravni. Direktiva o obveščevalni skupnosti (Intelligence Community Directive ali ICD 204) zagotavlja nadaljnja navodila glede NIPF in je bila posodobljena januarja 2015, da bi vključila zahtevo PPD-28 ([1]). Čeprav je NIPF tajen, se informacije v zvezi s posameznimi prednostnimi nalogami Združenih držav v zvezi s tujimi obveščevalnimi podatki odražajo vsako leto v netajni oceni nevarnosti svetu (*Worldwide Threat Assessment*) direktorja nacionalne obveščevalne službe, ki je prav tako na voljo na spletni strani Urada direktorja nacionalne obveščevalne službe.

Prednostne naloge v NIPF so na dokaj visoki ravni posplošenosti. Vsebujejo teme, kot so spremljanje jedrskih zmogljivosti in zmogljivosti balističnih izstrelkov posameznih tujih nasprotnikov ter učinke korupcije narkokartelov in zlorabe človekovih pravic v posameznih državah. Te se ne nanašajo samo na SIGINT, temveč na vse obveščevalne dejavnosti. Organizacija, ki je odgovorna za prenos prednostnih nalog v okviru NIPF v dejansko zbiranje obveščevalnih podatkov v okviru SIGINT, je nacionalni odbor za SIGINT (National Signals Intelligence Committee) ali SIGCOM. Ta deluje pod okriljem direktorja Agencije ZDA za nacionalno varnost (NSA), ki je imenovan v odredbi št. 12333 kot „funkcionalni vodja SIGINT“, odgovoren za nadzor in usklajevanje SIGINT po vsej obveščevalni skupnosti pod nadzorom Ministra za obrambo in direktorja nacionalne obveščevalne službe. SIGCOM ima predstavnike vseh članov obveščevalne skupnosti in bo, ker Združene države v celoti izvajajo PPD-28, polno predstavljal tudi druga Ministrstva in agencije s političnim interesom v SIGINT.

Vsa ameriška Ministrstva in agencije, ki so uporabniki tujih obveščevalnih podatkov, predložijo svoje zahteve za zbiranje, odboru SIGCOM. SIGCOM pregleda te zahteve, zagotovi, da so skladne z NIPF, in jim dodeli prednostno raven na podlagi meril, kot so:

— Ali lahko SIGINT zagotovi koristne informacije v tem primeru ali obstajajo boljši ali stroškovno učinkovitejši viri informacij za obravnavo zahteve, kot so slikovni material ali informacije iz prosto dostopnih virov?

— Kako kritična je potreba po teh informacijah? Če ima visoko prednostno raven v NIPF, bo najpogosteje imela visoko prednostno raven v SIGINT.

— Kakšno vrsto SIGINT je mogoče uporabiti?

— Ali je zbiranje tako prilagojeno, kot je izvedljivo? Ali so potrebne časovne, geografske ali druge omejitve?

Postopek zahtev v zvezi z ameriško dejavnostjo SIGINT zahteva tudi izrecno obravnavo drugih dejavnikov, in sicer:

— Ali je cilj zbiranja ali metodologija, uporabljena za zbiranje, še posebno občutljiva? Če da, jo bodo morali pregledati višji načrtovalci politik.

— Ali bo zbiranje predstavljalo neupravičeno tveganje za zasebnost in državljanske svoboščine ne glede na narodnost?

— Ali so potrebni dodatni zaščitni ukrepi glede širjenja in hranjenja za zaščito zasebnosti ali interesov nacionalne varnosti?

Nazadnje ob koncu postopka usposobljeni zaposleni v NSA izvedejo prednostne naloge, ki jih je potrdil SIGCOM, ter raziščejo in določijo posamezne izbirne izraze, kot so telefonske številke ali elektronski naslovi, ki naj bi zbirali tuje obveščevalne podatke glede na te prednostne naloge. Vsak izbirnik je treba pregledati in odobriti, preden je vnesen v zbirne sistem NSA. Tudi takrat bo odločitev, ali in kdaj se bo izvedlo dejansko zbiranje, deloma odvisna od dodatnih

([1]) Na voljo na http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

pomislekov, kot je razpoložljivost ustreznih virov zbiranja. Ta postopek zagotavlja, da je ameriško zbiranje obveščevalnih podatkov v okviru SIGINT usmerjeno v veljavne in pomembne potrebe po tujih obveščevalnih podatkih. In seveda, kadar se zbiranje izvaja v skladu z zakonom o nadzoru tujih obveščevalnih podatkov, morajo NSA in druge agencije upoštevati dodatne omejitve, ki jih odobri sodišče za nadzor tujih obveščevalnih podatkov (Foreign Intelligence Surveillance Court). Skratka, ne NSA ne nobena druga ameriška obveščevalna služba se ne odloči sama, kaj bo zbirala.

Na splošno ta postopek zagotavlja, da prednostne naloge ameriške obveščevalne dejavnosti določijo višji načrtovalci politik, ki so v najboljšem položaju za opredelitev ameriških zahtev glede tujih obveščevalnih podatkov, ti načrtovalci politik pa ne upoštevajo le potencialne vrednosti zbiranja obveščevalnih podatkov, temveč tudi tveganja, povezana s takim zbiranjem, vključno s tveganjem za zasebnost, nacionalne gospodarske interese in tuje odnose.

V zvezi s podatki, prenesenimi v Združene države v skladu z zasebnostnim ščitom, čeprav Združene države ne morejo potrditi ali zanikati posameznih obveščevalnih metod ali operacij, zahteve PPD-28 veljajo za vse operacije SIGINT, ki jih izvajajo Združene države, ne glede na vrsto ali vir podatkov, ki se zbira. Poleg tega omejitve in zaščitni ukrepi, ki veljajo za zbiranje obveščevalnih podatkov v okviru SIGINT, veljajo za obveščevalne podatke, zbrane za kateri koli pooblaščen namen, vključno za potrebe zunanjih zadev in nacionalne varnosti.

Postopki, navedeni zgoraj, so dokaz jasne zavezanosti k preprečevanju samovoljnega in neselektivnega zbiranja obveščevalnih podatkov v okviru SIGINT ter k izvajanju načela razumnosti na najvišjih ravneh naše vlade. PPD-28 in izvedbeni postopki agencije pojasnjujejo nove in obstoječe omejitve ter bolj podrobno opisujejo namen, za katerega Združene države zbirajo in uporabljajo obveščevalne podatke v okviru SIGINT. Ti morajo zagotavljati, da se in se bodo obveščevalne dejavnost SIGINT še naprej izvajale le za spodbujanje zakonitih ciljev z zvezi s tujimi obveščevalnimi podatki.

c. **Omejitve v zvezi s hranjenjem in širjenjem**

Člen 4 PPD-28 določa, da mora imeti vsak član obveščevalne skupnosti izrecne omejitve glede hranjenja in širjenja osebnih informacij, zbranih v okviru SIGINT o nedržavljanih ZDA, ki so primerljive z omejitvami za državljane ZDA. Ta pravila so vključena v postopke za vsako agencijo v obveščevalni skupnosti, ki so bili objavljeni februarja 2015 in so javno dostopni. Za izpolnjevanje pogojev glede hranjenja ali širjenja kot tujih obveščevalnih podatkov se morajo osebne informacije nanašati na zahtevo o dovoljenih obveščevalnih podatkih, kakor je določena v postopku NIPF, opisanem zgoraj; mora obstajati utemeljen sum, da so dokaz kaznivega dejanja, ali morajo izpolnjevati enega od preostalih standardov za hranjenje informacij o državljanih ZDA, kakor so določeni v odredbi št. 12333, člen 2.3.

Informacij, ki niso tako določene, ni dovoljeno hraniti več kot pet let, razen če direktor nacionalne obveščevalne službe določi, da je nadaljnje hranjenje v interesu nacionalne varnosti Združenih držav. Zato morajo člani obveščevalne skupnosti zbrisati informacije o nedržavljanih ZDA, zbrane v okviru SIGINT, pet let po zbiranju, razen če so, na primer, informacije določene kot pomembne glede na zahtevo o dovoljenih tujih obveščevalnih podatkih ali če direktor nacionalne obveščevalne službe po obravnavi stališč uradnika za zaščito državljanskih svoboščin v Uradu direktorja nacionalne obveščevalne službe in uradnikov na področju varstva zasebnosti in državljanskih svoboščin v agenciji določi, da je nadaljnja hramba v interesu nacionalne varnosti.

Poleg tega vse politike agencije, ki izvajajo PPD-28, zdaj izrecno zahtevajo, da informacij o osebi ni dovoljeno širiti zgolj zato, ker posameznik ni državljan ZDA, Urad direktorja nacionalne obveščevalne službe pa je izdal direktivo vsem članom obveščevalne skupnosti ([1]), ki odraža to zahtevo. Od zaposlenih v obveščevalni skupnosti se še posebno zahteva, da upoštevajo interese zasebnosti nedržavljanov ZDA, kadar pripravljajo in širijo obveščevalna poročila. Zlasti se SIGINT o vsakdanjih dejavnostih tujca ne šteje za tuje obveščevalne podatke, ki jih je mogoče širiti ali hraniti trajno na osnovi samo tega dejstva, razen če se kako drugače nanaša na zahtevo o dovoljenih tujih obveščevalnih podatkih. To priznava pomembno omejitev in se odziva na pomisleke Evropske komisije o širini definicije tujih obveščevalnih podatkov, kakor je navedena v odredbi št. 12333.

([1]) Intelligence Community Directive (ICD) 203, na voljo na http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Skladnost in nadzor**

Ameriški sistem nadzora nad tujimi obveščevalnimi podatki zagotavlja strog in večplastni nadzor za zagotavljanje skladnosti z veljavnimi zakoni in postopki, tudi tistimi, ki se nanašajo na zbiranje, hranjenje in širjenje informacij o nedržavljanih ZDA, pridobljenih v okviru SIGINT, kakor je opredeljeno v PPD-28. Ti zajemajo:

— Obveščevalna skupnost zaposluje na stotine ljudi za nadzor. Samo v NSA je več kot 300 ljudi zadolženih za preverjanje skladnosti, pa tudi drugi člani imajo urade za nadzor. Poleg tega Ministrstvo za pravosodje zagotavlja temeljit nadzor obveščevalnih dejavnosti, nadzor pa izvaja tudi Ministrstvo za obrambo.

— Vsak član obveščevalne skupnosti ima svoj urad generalnega inšpektorja, ki je med drugim odgovoren za nadzor tujih obveščevalnih dejavnosti. Generalni inšpektorji so zakonsko neodvisni; imajo široka pooblastila za izvajanje preiskav, revizij in pregledov programov, vključno z goljufijami in zlorabo ali kršitvijo zakona; in lahko priporočajo popravne ukrepe. Medtem ko so priporočila generalnega inšpektorja nezavezujoča, pa so njegova poročila pogosto objavljena in v vsakem primeru predložena Kongresu; to zajema tudi poročila o nadaljnjem spremljanju, če popravni ukrepi, priporočeni v prejšnjih poročilih, še niso zaključeni. Kongres je torej obveščen o morebitni neskladnosti in lahko izvaja pritisk, tudi s proračunskimi sredstvi, da bi dosegel popravne ukrepe. Številna poročila generalnih inšpektorjev o programih obveščevalnih dejavnosti so javno objavljena ([1]).

— Urad za državljanske svoboščine in zasebnost v okviru Urada direktorja nacionalne obveščevalne službe je dolžan zagotoviti, da obveščevalna skupnost deluje na način, ki spodbuja nacionalno varnost, obenem pa ščiti državljanske svoboščine in pravice do zasebnosti ([2]). Drugi člani obveščevalne skupnosti imajo svoje uradnike, zadolžene za varstvo zasebnosti.

— Odbor za nadzor zasebnosti in državljanskih svoboščin (PCLOB), zakonsko ustanovljeno neodvisno telo, je zadolženo za analizo in pregled programov in politik za boj proti terorizmu, vključno z uporabo SIGINT, da bi zagotovil ustrezno zaščito zasebnosti in državljanskih svoboščin. Izdal je več javnih poročil glede obveščevalnih dejavnosti.

— Kakor je podrobneje obravnavano spodaj, je sodišče za nadzor tujih obveščevalnih podatkov, sestavljeno iz neodvisnih zveznih sodnikov, odgovorno za nadzor nad in skladnost vseh dejavnosti zbiranja obveščevalnih podatkov v okviru SIGINT, ki so izvedene v skladu z zakonom o nadzoru tujih obveščevalnih podatkov.

— Nazadnje ima ameriški kongres, bolj točno odbori spodnjega doma in senata za obveščevalno dejavnost in pravosodje, pomembne nadzorne naloge v zvezi z vsemi dejavnostmi Združenih držav za pridobivanje tujih obveščevalnih podatkov, vključno s SIGINT.

Poleg teh uradnih nadzornih mehanizmov ima obveščevalna skupnost vzpostavljene številne mehanizme, s katerimi zagotavlja, da obveščevalna skupnost izpolnjuje omejitve glede zbiranja, opisane zgoraj. Na primer,

— uradniki v kabinetu so dolžni vsako leto potrditi svoje zahteve v zvezi s SIGINT.

— NSA preverja cilje SIGINT skozi celoten proces zbiranja, da bi ugotovila, ali dejansko zagotavljajo dragocene tuje obveščevalne podatke, ki ustrezajo prednostnim nalogam, ter ustavila zbiranje podatkov o ciljih, ki ne. Dodatni postopki zagotavljajo, da so izbirni izrazi redno pregledani.

([1]) Glej, na primer, poročilo generalnega inšpektorja na Ministrstvu za pravosodje ZDA „Pregled dejavnosti Zveznega preiskovalnega urada v okviru člena 702 zakona o nadzoru tujih obveščevalnih podatkov iz leta 2008“ (september 2012), na voljo na https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) Glej www.dni.gov/clpo.

— Na podlagi priporočila neodvisne skupine za pregledovanje, ki jo je imenoval predsednik Obama, je direktor nacionalne obveščevalne službe vzpostavil novi mehanizem za spremljanje in širjenje obveščevalnih podatkov SIGINT, ki so posebej občutljivi zaradi narave cilja ali sredstev zbiranja, da bi zagotovil njegovo skladnost z določili načrtovalcev politik.

— Urad direktorja nacionalne obveščevalne službe vsako leto pregleda dodelitev sredstev obveščevalne skupnosti glede na prednostne naloge NIPF in obveščevalno nalogo kot celoto. Ta pregled vključuje ocene vrednosti vseh vrst zbiranja obveščevalnih podatkov, vključno s SIGINT, ter se ozira nazaj, in sicer na to, kako uspešna je bila obveščevalna skupnost pri doseganju svojih ciljev, in naprej na to, kakšne bodo prihodnje potrebe obveščevalne skupnosti. To omogoča, da se viri SIGINT uporabijo za večino pomembnih nacionalnih prednostnih nalog.

Kakor prikazuje ta celovit pregled, obveščevalna skupnost ne odloča sama o tem, katerim pogovorom bo prisluškovala, skušala zbrati vse ali delovala brez nadzora. Njene dejavnosti so osredotočene na prednostne naloge, ki jih določijo načrtovalci politik, skozi proces, ki vključuje vhodne podatke od vlade in ga nadzorujejo NSA, Urad direktorja nacionalne obveščevalne službe, Ministrstvo za pravosodje in Ministrstvo za obrambo.

PPD-28 vsebuje tudi številne druge določbe, ki zagotavljajo zaščito za osebne informacije, zbrane v okviru SIGINT, ne glede na narodnost. Denimo, PPD-28 zagotavlja varnost podatkov, dostop in kakovostne postopke za zaščito osebnih informacij, zbranih v okviru SIGINT, ter obvezno usposabljanje, s katerim je zagotovljeno, da zaposleni razumejo dolžnost zaščite osebnih informacij ne glede na narodnost. PPD zagotavlja tudi dodatne mehanizme za nadzor in skladnost. Ti vsebujejo redne revizije in preglede s strani ustreznih uradnikov za nadzor in skladnost praks za zaščito osebnih informacij v SIGINT. Pregledi morajo zajeti tudi izpolnjevanje postopkov za zaščito takšnih informacij s strani agencij.

Poleg tega PPD-28 določa, da bodo pomembne zadeve glede skladnosti v zvezi z nedržavljani ZDA obravnavale višje ravni vlade. Če se pojavi pomembna zadeva glede skladnosti v zvezi z osebnimi informacijami katere koli osebe, ki so zbrane na podlagi obveščevalnih dejavnosti SIGINT, je treba poleg morebitnih obstoječih zahtev glede poročanja o zadevi nemudoma poročati direktorju nacionalne obveščevalne službe. Če zadeva vključuje osebne informacije nedržavljana ZDA, bo direktor nacionalne obveščevalne službe v posvetovanju z zunanjim ministrom in vodjo ustreznega člana obveščevalne skupnosti določil, ali je treba ukrepati in obvestiti ustrezno tujo vlado, skladno z zaščito virov, načinov in ameriškega osebja. Poleg tega je, kakor predpisuje PPD-28, zunanji minister imenoval višjo uradnico, in sicer namestnico ministra Catherine Novelli, kot osebo za stike s tujimi vladami, ki želijo sprožiti vprašanja glede ameriških obveščevalnih dejavnosti SIGINT. Ta zaveza k vključitvi visokih ravni ponazarja prizadevanja vlade ZDA v preteklih nekaj letih, da bi vlila zaupanje v številne in prekrivajoče se zaščite zasebnosti, vzpostavljene za informacije o državljanih in nedržavljanih ZDA.

e. **Povzetek**

Procesi Združenih držav za zbiranje, hranjenje in širjenje tujih obveščevalnih podatkov zagotavljajo pomembne elemente varstva zasebnosti za osebne informacije vseh oseb ne glede na narodnost. Ti procesi zlasti zagotavljajo, da se naša obveščevalna skupnost osredotoči na svojo nacionalno-varnostno nalogo, kakor jo dovoljuje veljavna zakonodaja, odredbe in predsedniške direktive; varuje informacije pred nepooblaščenim dostopom, uporabo in razkritjem; in izvaja svoje dejavnosti pod več plastmi pregleda in nadzora, vključno z kongresnimi odbori za nadzor. PPD-28 in njeni izvedbeni postopki predstavljajo naša prizadevanja, da razširimo določena načela glede zmanjšanja količin podatkov in druge pomembne elemente varstva podatkov na osebne informacije vseh oseb ne glede na narodnost. Za osebne informacije, zbrane z ameriško obveščevalno dejavnostjo SIGINT, veljajo načela in zahteve zakonodaje ZDA in predsedniških navodil, vključno z varstvom, določenim v PPD-28. Ta načela in zahteve zagotavljajo, da so osebe obravnavane z dostojanstvom in spoštovanjem ne glede na njihovo narodnost ali kraj bivanja, ter priznavajo, da imajo vse osebe zakonite interese zasebnosti pri ravnanju z njihovimi osebnimi informacijami.

II. ZAKON O NADZORU TUJIH OBVEŠČEVALNIH PODATKOV – ČLEN 702

Zbiranje po členu 702 zakona o nadzoru tujih obveščevalnih podatkov ([1]) ni „množično in neselektivno“, temveč je ozko usmerjeno v zbiranje tujih obveščevalnih podatkov od posamezno določenih zakonitih ciljev; je jasno dovoljeno s izrecnim zakonskim pooblastilom; in je predmet neodvisnega sodnega nadzora in temeljitega pregleda in nadzora v okviru izvršilne veje in kongresa. Zbiranje po členu 702 se šteje za obveščevalno dejavnost pri zaznavanju signalov (SIGINT) v skladu z zahtevami PPD-28 ([2]).

Zbiranje v skladu s členom 702 je eno najdragocenejših virov obveščevalnih podatkov, ki ščiti Združene države in naše evropske partnerje. Obsežne informacije o delovanju in nadzoru člena 702 so javno dostopne. Številnim zadevam, vloženim na sodišče, sodnim odločbam in poročilom o nadzoru v zvezi s programom je bila preklicana stopnja tajnosti in so bili objavljeni na spletni strani Urada direktorja nacionalne obveščevalne službe za javna razkritja, tj. www.icontherecord.tumblr.com. Poleg tega je Odbor za nadzor zasebnosti in državljanskih svoboščin temeljito analiziral člen 702 v poročilu, ki je na voljo na https://www.pclob.gov/library/702-Report.pdf ([3]).

Člen 702 je bil sprejet v okviru zakona o spremembi zakona o nadzoru tujih obveščevalnih podatkov (FISA Amendments Act) iz leta 2008 ([4]) po obsežni javni razpravi v kongresu. Dovoljuje pridobivanje tujih obveščevalnih podatkov z usmerjanjem na nedržavljane ZDA zunaj Združenih držav in s prisilno pomočjo ameriških ponudnikov storitev elektronskih komunikacij. Člen 702 državnega tožilca in direktorja nacionalne obveščevalne službe – dva uradnika v kabinetu, ki ju imenuje predsednik in potrdi senat – pooblašča, da vloži letne certifikacije sodišču FISA ([5]). Te certifikacije opredeljujejo posebne kategorije tujih obveščevalnih podatkov, ki se bodo zbirale, kot so obveščevalni podatki v zvezi z bojem proti terorizmu ali orožjem za množično uničevanje, ki morajo soditi v kategorije tujih obveščevalnih podatkov, kakor jih opredeljuje zakon o nadzoru tujih obveščevalnih podatkov ([6]). Kakor je opozoril Odbor za nadzor zasebnosti in državljanskih svoboščin, „[t]e omejitve *ne* dovoljujejo neomejenega zbiranja informacij o tujcih“ ([7]).

Certifikacije so potrebne tudi za vključitev postopkov „izbire cilje“ in „zmanjševanja količine podatkov“, ki jih mora pregledati in odobriti sodišče FISA ([8]). Postopki izbire cilje so zasnovani tako, da zagotavljajo zbiranje samo, kakor ga dovoljuje zakon in ki je v okviru certifikacij; postopki zmanjševanja so zasnovani tako, da omejujejo pridobivanje, širjenje in hranjenje informacij o državljanih ZDA, obenem pa vsebujejo določbe, ki zagotavljajo precejšnjo zaščito informacij tudi o nedržavljanih ZDA, kakor so opisane spodaj. Poleg tega je, kakor je opisano zgoraj, predsednik v PPD-28 predpisal, da mora obveščevalna skupnost zagotoviti dodatno varstvo osebnih informacij o nedržavljanih ZDA, to varstvo pa se nanaša na informacije, zbrane v okviru člena 702.

Ko sodišče odobri postopke izbire cilja in zmanjševanja količine podatkov, zbiranje po členu 702 ni več množično ali neselektivno, temveč „je v celoti sestavljeno iz usmerjanja na posamezne osebe, o katerih je bila sprejeta individualizirana ugotovitev,“ kakor pravi Odbor za nadzor zasebnosti in državljanskih svoboščin ([9]). Zbiranje je usmerjeno z uporabo posameznih izbirnikov, kot so elektronski naslovi ali telefonske številke, za katere so ameriški obveščevalci ugotovili, da

([1]) Člen 1881a naslova 50 zakonodajne zbirke ZDA.

([2]) Združene države lahko pridobijo tudi sodne odločbe v skladu z drugimi določbami zakona o nadzoru tujih obveščevalnih podatkov za pridobivanje podatkov, vključno s podatki, prenesenimi v skladu z zasebnostnim ščitom. *Glej* člen 1801 *et seq* naslova 50 zakonodajne zbirke ZDA. Naslova I in III zakona o nadzoru tujih obveščevalnih podatkov, ki ustrezno dovoljuje elektronski nadzor in fizične preiskave, zahtevata sodno odločbo (razen v izrednih razmerah) in vedno zahtevata utemeljeni sum za prepričanje, da je cilj tuja sila ali agent tuje sile. Naslov IV zakona o nadzoru tujih obveščevalnih podatkov dovoljuje uporabo snemalnikov klicev ter naprav za pasti in sledenje v skladu s sodno odločbo (razen v izrednih razmerah) v dovoljenih dejavnostih za pridobivanje tujih obveščevalnih podatkov, protiobveščevalnih dejavnostih ali preiskavah v boju proti terorizmu. Naslov V zakona o nadzoru tujih obveščevalnih podatkov Zveznemu preiskovalnemu uradu dovoljuje, da pridobiva poslovne evidence, ki so potrebne za dovoljene preiskave tujih obveščevalnih podatkov, protiobveščevalne dejavnosti ali preiskave v boju proti terorizmu. Kakor je navedeno spodaj, ameriški zakon o svobodi (USA FREEDOM Act) posebej prepoveduje uporabo odločb za snemalnike klicev ali poslovne evidence v okviru zakona o nadzoru tujih obveščevalnih podatkov za množično zbiranje ter predpisuje zahtevo po „posebnem izbirnem izrazu“, ki zagotavlja, da se ta pooblastila uporabijo usmerjeno.

([3]) Odbor za nadzor zasebnosti in državljanskih svoboščin, „Poročilo o programu nadzora, ki se izvaja v skladu s členom 702 zakona o nadzoru tujih obveščevalnih podatkov“ (2. julij 2014) („poročilo PCLOB“).

([4]) Glej Pub. L. No. 110-261, 122 Stat. 2436 (2008).

([5]) Glej člen 1881a(a) in (b) naslova 50 zakonodajne zbirke ZDA.

([6]) Glej *id.* člen 1801(e).

([7]) Glej poročilo PCLOB na 99.

([8]) Glej člen 1881a(d) in (e) naslova 50 zakonodajne zbirke ZDA.

([9]) Glej poročilo PCLOB na strani 111.

se verjetno uporabljajo za sporočanje tujih obveščevalnih podatkov vrste, ki jo zajema certifikacija, predložena sodišču ([1]). Podlago za izbiro cilja je treba dokumentirati, dokumentacijo za vsak izbirnik pa naknadno pregleda Ministrstvo za pravosodje ([2]). Vlada ZDA je objavila informacije, ki kažejo, da je bilo leta 2014 okoli 90 000 posameznikov izbranih za cilj v okviru člena 702, kar je neznaten delež več kot 3 milijard uporabnikov interneta po vsem svetu ([3]).

Za informacije, zbrane v okviru člena 702, mora sodišče odobriti postopke zmanjševanja, ki zagotavljajo varstvo nedržavljanom in državljanom ZDA in ki so bili javno objavljeni ([4]). Na primer, komunikacija, pridobljena v okviru člena 702 o državljanu ali nedržavljanu ZDA, je shranjena v podatkovnih zbirkah s strogim nadzorom dostopa. Te lahko pregledujejo le obveščevalci, usposobljeni v postopkih zmanjševanja za zaščito zasebnosti in posebej potrjeni za ta dostop, da bi izvajali svoja pooblaščene funkcije ([5]). Uporaba podatkov je omejena na odkrivanje tujih obveščevalnih podatkov ali dokazov kaznivega dejanja ([6]). V skladu s PPD-28 je te informacije mogoče širiti le, če obstaja veljavna potreba po tujih obveščevalnih podatkih ali kazenskem pregonom; samo dejstvo, da ena stranka komunikacije ni državljan ZDA, ne zadostuje ([7]). Postopki zmanjševanja in PPD-28 pa prav tako postavljajo omejitve glede dolžine hranjenja podatkov, pridobljenih v skladu s členom 702 ([8]).

Nadzor člena 702 je temeljit in ga izvajajo tri veje naše vlade. Agencije, ki izvajajo zakon, imajo več ravni notranje revizije, vključno z neodvisnimi generalnimi inšpektorji, in tehnološki nadzor nad dostopom do podatkov. Ministrstvo za pravosodje in Urad direktorja nacionalne obveščevalne službe natančno in temeljito pregledujeta uporabo člena 702, da bi preverila izpolnjevanje zakonskih pravil; agencije imajo tudi neodvisno obveznost, da poročajo o morebitnih primerih neizpolnjevanja. Ti primeri se preiščejo, vsi primeri neizpolnjevanja pa se sporočijo sodišču za nadzor tujih obveščevalnih podatkov, predsednikovemu odboru za nadzor obveščevalnih podatkov in kongresu ter ustrezno odpravijo ([9]). Do danes ni bilo nobenih primerov namernih poskusov kršenja zakona ali izogibanja zakonskim zahtevam ([10]).

Sodišče FISA igra pomembno vlogo v izvajanju člena 702. Sestavljajo ga neodvisni zvezni sodniki, katerih mandat na sodišču FISA traja sedem let, vendar pa imajo tako kot vsi zvezni sodniki stalni mandat sodnika. Kakor je poudarjeno zgoraj, mora sodišče pregledati, ali so letne certifikacije ter postopki izbire cilja in zmanjševanja skladni z zakonom. Obenem je vlada dolžna takoj obvestiti sodišče o zadevah v zvezi z izpolnjevanjem načel ([11]) in več mnenjem sodišča je bila preklicana stopnja tajnosti ter so bila objavljena, kar kaže na izjemno stopnjo sodnega pregleda in neodvisnosti, ki jo izvaja med pregledom teh primerov.

Natančne procese sodišča je opisal bivši predsedujoči sodnik v pismu kongresu, ki je bilo javno objavljeno ([12]). Zaradi ameriškega zakona o svobodi (USA FREEDOM Act), ki je opisan spodaj, je sodišče zdaj izrecno pooblaščeno za imenovanje zunanjega odvetnika kot neodvisnega zagovornika v imenu zasebnosti v zadevah, ki predstavljajo nova ali pomembna pravna vprašanja ([13]). Ta stopnja vključenosti neodvisnega sodstva v tuje obveščevalne dejavnosti, usmerjene v osebe, ki niso državljani te države in se ne nahajajo v njej, je neobičajna, če ne celo brez primere, ter pomaga zagotoviti, da zbiranje v okviru člena 702 poteka znotraj ustreznih pravnih omejitev.

([1]) *Id.*

([2]) *Id.* na strani 8; Člen 1881a(l) naslova 50 zakonodajne zbirke ZDA; glej tudi Poročilo direktorja NSA za državljanske svoboščine in zasebnost, „Izvajanje člena 702 zakona o nadzoru tujih obveščevalnih podatkov s strani NSA“ (v nadaljnjem besedilu „poročilo NSA“) na strani 4, na voljo na http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Poročilo o preglednosti direktorja nacionalne obveščevalne službe za leto 2014, na voljo na http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Postopki zmanjševanja, ki so na voljo na: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf („postopki zmanjševanja NSA“); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) Glej poročilo NSA na strani 4.

([6]) Glej, na primer, postopke zmanjševanja NSA na strani 6.

([7]) Postopki PPD-28 za obveščevalne agencije so na voljo na http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Glej postopke zmanjševanja NSA; PPD-28, člen 4.

([9]) Glej člen 1881(l) naslova 50 zakonodajne zbirke ZDA; glej tudi poročilo PCLOB na straneh 66–76.

([10]) Glej polletno oceno izpolnjevanja postopkov in smernic v zadevah iz člena 702 zakona o nadzoru tujih obveščevalnih podatkov, ki sta ga predložila državni tožilec in direktor nacionalne obveščevalne službe na straneh 2–3, na voljo na http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Pravilo 13 poslovnika sodišča za nadzor tujih obveščevalnih podatkov, na voljo na http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) 29. julij 2013, Pismo Reggieja B. Waltona Patricku J. Leahyju, *na voljo na* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) Glej člen 401 USA FREEDOM Act, P.L. 114-23.

Kongres izvaja nadzor z zakonsko predpisanimi poročili za odbore za obveščevalne dejavnosti in sodstvo ter pogostimi informativnimi sestanki in obravnavami. Ti vključujejo polletno poročilo državnega tožilca, ki opisuje uporabo člena 702 in morebitne primere skladnosti ([1]); ločeno polletno oceno državnega tožilca in direktorja nacionalne obveščevalne službe, ki opisuje izpolnjevanje postopkov izbire cilja in zmanjševanja podatkov, vključno z izpolnjevanjem postopkov, katerih namen je zagotoviti, da se zbiranje izvaja za veljavno potrebo po tujih obveščevalnih podatkih ([2]); in letno poročilo vodij članov obveščevalne dejavnosti, ki vključuje certifikacijo, da se z zbiranjem v okviru člena 702 še naprej pridobivajo tuji obveščevalni podatki ([3]).

Skratka, zbiranje po členu 702 dovoljuje zakon; je predmet več plasti pregleda, sodnega nadzora in nadzora; in se, kakor je navedlo sodišče FISA v nedavnem mnenju, kateremu je bila preklicana stopnja zaupnosti, „ne izvaja množično ali neselektivno“, temveč „z ... diskretnimi odločitvami o izbiri cilja za posamezne [komunikacijske] zmogljivosti.“ ([4])

III. AMERIŠKI ZAKON O SVOBODI (USA FREEDOM Act)

Ameriški zakon o svobodi (USA FREEDOM Act), vpisan v zakonodajo junija 2015, je pomembno spremenil ameriške organe nadzora in nacionalne varnosti ter povečal javno preglednost uporabe teh pooblastil in sklepov sodišča FISA, kakor so določeni spodaj ([5]). Zakon zagotavlja, da imajo naši strokovnjaki v obveščevalni dejavnosti in kazenskem pregonu pooblastila, ki jih potrebujejo za zaščito naroda, obenem pa nadalje zagotavlja, da je pri izvajanju teh pooblastil zasebnost posameznikov ustrezno zaščitena. Krepi varstvo zasebnosti in državljanskih svoboščin ter povečuje preglednost.

Zakon prepoveduje množično zbiranje katerih koli evidenc o državljanih in nedržavljanih ZDA v skladu z različnimi določbami zakona o nadzoru tujih obveščevalnih podatkov ali z uporabo sodnih pozivov v zvezi z nacionalno varnostjo (National Security Letters) ([6]). Ta prepoved posebej vključuje telefonske metapodatke v zvezi s klici med osebami v ZDA in osebami zunaj ZDA ter bi tako vključevala tudi zbiranje informacij zasebnostnega ščita v skladu s temi pooblastili. Zakon od vlade zahteva, da utemelji vsako prošnjo za evidence v okviru teh pooblastil na „posebnem izbirnem izrazu“ – izrazu, ki posebej določa osebo, račun, naslov ali osebno napravo na način, ki omejuje obseg informacij, iskanih do največje razumno izvedljive mere ([7]). To nadalje zagotavlja, da je zbiranje informacij za obveščevalne potrebe natančno osredotočeno in usmerjeno v cilj.

Zakon je prav tako pomembno spremenil postopke pred sodiščem FISA, ki so povečali preglednost in dali dodatna zagotovila za zaščito zasebnosti. Kakor je poudarjeno zgoraj, je dovolil ustanovitev stalnega odbora varnostno preverjenih odvetnikov s strokovnim znanjem in izkušnjami na področju zasebnosti in državljanskih svoboščin, zbiranja obveščevalnih podatkov, komunikacijske tehnologije ali drugih ustreznih področjih, ki so lahko imenovani, da se pojavijo pred sodiščem kot prijatelji sodišča *amicus curiae* v zadevah, ki vključujejo pomembne ali nove razlage zakona. Ti odvetniki so pooblaščeni, da dajejo pravne argumente, ki izboljšujejo zaščito zasebnosti posameznikov in državljanskih svoboščin, ter bodo imeli dostop do vseh informacij, tudi tajnih, ki jih sodišče določi kot potrebne za izvedbo njihovih dolžnosti ([8]).

Zakon nadgrajuje edinstveno preglednost vlade ZDA v zvezi z obveščevalnimi dejavnostmi, s tem ko od direktorja nacionalne obveščevalne službe zahteva, da v posvetovanju z državnim tožilcem bodisi prekliče stopnjo tajnosti bodisi objavi netajni povzetek vsake odločitve, sklepa ali mnenja, ki ga je izdalo sodišče FISA ali prizivno sodišče za nadzor tujih obveščevalnih podatkov, ki vključuje pomembno sestavo ali razlago katere koli določbe zakona.

([1]) Glej člen 1881f naslova 50 zakonodajne zbirke ZDA člen 1881f.
([2]) Glej *id*. člen 1881a(l)(1).
([3]) Glej *id*. člen 1881a(l)(3). Nekatera od teh poročil so tajna.
([4]) Mem. Mnenje in sklep na strani 26 (FISC 2014), na voljo na http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) Glej USA FREEDOM Act of 2015, Pub. L. No. 114-23, člen 401, 129 Stat. 268.
([6]) Glej *id*. členi 103, 201 in 501. Sodne pozive v zvezi z nacionalno varnostjo dovoljuje vrsta zakonov in omogočajo Zveznemu preiskovalnemu uradu, da pridobiva informacije v poročilih o kreditni sposobnosti, finančne podatke ter elektronske podatke o naročnikih in transakcijah od določenih vrst podjetij samo za potrebe zaščite pred mednarodnim terorizmom ali tajnimi obveščevalnimi dejavnostmi. Glej člen 3414 naslova 12 zakonodajne zbirke ZDA; člena 1681u in 1681v naslova 15 zakonodajne zbirke ZDA in člen 2709 naslova 18 zakonodajne zbirke ZDA. Sodne pozive v zvezi z nacionalno varnostjo praviloma uporablja Zvezni preiskovalni urad za zbiranje nevsebinskih informacij v začetnih fazah preiskav v boju proti terorizmu in protiobveščevalni dejavnosti – kot je identiteta naročnika računa, ki morda komunicira z agenti teroristične skupine, kot je Islamska država. Prejemniki sodnega poziva v zvezi z nacionalno varnostjo ga imajo pravico izpodbijati na sodišču. Glej člen 3511 naslova 18 zakonodajne zbirke ZDA.
([7]) Glej *id*.
([8]) Glej *id*. člen 401.

Poleg tega zakon omogoča obsežna razkritja o zbiranju v okviru zakona o nadzoru tujih obveščevalnih podatkov in zahtev sodnih pozivov v zvezi z nacionalno varnostjo. Združene države morajo vsako leto kongresu in javnosti razkriti število odredb v okviru zakona o nadzoru tujih obveščevalnih podatkov ter zahtevane in prejete certifikacije; ocene števila državljanov in nedržavljanov ZDA, ki so bili izbrani kot cilj in postali predmet nadzora; in število imenovanih prijateljev sodišča *amici curiae*, med drugimi informacijami ([1]). Zakon od vlade zahteva tudi dodatno javno poročanje glede števila zahtev v sodnih pozivih v zvezi z nacionalno varnostjo o državljanih in nedržavljanih ZDA ([2]).

V zvezi s preglednostjo podjetij daje zakon podjetjem vrsto možnosti za javno sporočanje skupnega števila sklepov in direktiv zakona o nadzoru tujih obveščevalnih podatkov ali sodnih pozivov v zvezi z nacionalno varnostjo, ki jih prejmejo od vlade, ter število uporabniških računov, ki so izbrani za cilj v teh sklepih ([3]). Več podjetij je že opravilo takšna razkritja, ki so pokazala omejeno število strank, katerih podatki so se iskali.

Ta poročila o preglednosti podjetij kažejo, da se zahtevki ameriške obveščevalne službe nanašajo le na neznaten delež podatkov. Denimo, nedavno poročilo nekega velikega podjetja kaže, da je prejelo zahtevke v zvez z nacionalno varnostjo (v skladu z zakonom o nadzoru tujih obveščevalnih podatkov ali sodnimi pozivi v zvezi z nacionalno varnostjo) za manj kot 20 000 svojih računov v času, ki je imelo vsaj 400 milijonov naročnikov. Z drugimi besedami, vsi zahtevki Združenih držav v zvezi z nacionalno varnostjo, o katerih je poročalo to podjetje, se je nanašalo na manj kot 0,005 % njegovih naročnikov. Tudi če bi se eden od teh zahtevkov nanašal na podatke v okviru varnega pristana, čemur ni tako, je očitno, da so zahteve usmerjene in ustreznega obsega ter niso množične in neselektivne.

Medtem ko so zakoni, ki dovoljujejo sodne pozive v zvezi z nacionalno varnostjo, že omejili okoliščine, v katerih je mogoče prejemniku takšnega sodnega poziva prepovedati njegovo razkritje, je zakon nadalje zagotovil, da je treba takšne zahteve po nerazkrivanju redno pregledovati; zahteval, da so prejemniki sodnih pozivov v zvezi z nacionalno varnostjo obveščeni, kadar dejstva ne podpirajo več zahteve po nerazkrivanju; in kodificiral postopke za prejemnike, s katerimi lahko izpodbijajo zahteve po nerazkrivanju ([4]).

Če povzamem, pomembne spremembe ameriškega zakona o svobodi v zvezi ameriškimi obveščevalnimi organi jasno pričajo o obsežnih prizadevanjih Združenih držav, da postavijo zaščito osebnih informacij, zasebnost, državljanske svoboščine in preglednosti v ospredje vseh obveščevalnih praks.

IV. PREGLEDNOST

Poleg preglednosti, ki jo predpisuje ameriški zakon o svobodi, ameriška obveščevalna skupnost javnosti zagotavlja veliko dodatnih informacij in tako postavlja trden zgled v zvezi s preglednostjo v svojih obveščevalnih dejavnostih. Obveščevalna skupnost je objavila mnoge svoje politike, postopke, sklepe sodišča za nadzor tujih obveščevalnih podatkov in drugo gradivo, kateremu je bila preklicana stopnja zaupnosti, s čimer zagotavlja izjemno stopnjo preglednosti. Poleg tega je obveščevalna skupnost precej povečala razkrivanje statističnih podatkov o vladni uporabi organov, ki zbirajo podatke v zvezi z nacionalno varnostjo. Obveščevalna skupnost je 22. aprila 2015 izdala svoje drugo letno poročilo, v katerem je predstavila statistične podatke v zvezi s tem, kako pogosto vlada uporablja ta pomembna pooblastila. Urad direktorja nacionalne obveščevalne službe je na svoji spletni strani in spletni strani *IC On the Record* prav tako objavil niz konkretnih načel preglednosti ([5]) in izvedbeni načrt, ki prenaša ta načela v konkretne merljive pobude ([6]). Direktor nacionalne obveščevalne službe je oktobra 2015 vsaki obveščevalni agenciji odredil, da imenuje uradnika za preglednost obveščevalne dejavnosti v okviru svojega vodstva za spodbujanje preglednosti in vodenje pobud v zvezi s preglednostjo ([7]). Uradnik za preglednost bo tesno sodeloval z uradnikom za nadzor zasebnosti in državljanskih svoboščin vsake obveščevalne agencije in tako zagotovil, da preglednost, zasebnost in državljanske svoboščine ostanejo najpomembnejše prednostne naloge.

([1]) Glej *id.* člen 602.
([2]) Glej *id.*
([3]) Glej *id.* člen 603.
([4]) Glej *id.* členi 502(f)–503.
([5]) Na voljo na http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) Na voljo na http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) Glej *id.*

Kot primer teh prizadevanj je glavni uradnik za nadzor zasebnosti in državljanskih svoboščin pri NSA v preteklih nekaj letih objavil več poročil, katerim je bila preklicana stopnja zaupnosti, vključno s poročili o dejavnostih v okviru člena 702, odredbe št. 12333 in ameriškega zakona o svobodi (USA FREEDOM Act [1]). Poleg tega, obveščevalna skupnost tesno sodeluje z Odborom za nadzor zasebnosti in državljanskih svoboščin, kongresom in ameriško skupnostjo, ki zagovarja zasebnost, da bi zagotovila še večjo preglednost v zvezi z ameriškimi obveščevalnimi dejavnostmi, kjer je to izvedljivo in skladno z zaščito občutljivih virov in metod za pridobivanje obveščevalnih podatkov. Ameriške obveščevalne dejavnosti so kot celota tako ali pa bolj pregledne kot tiste katerega koli drugega naroda na svetu in so pregledne, kolikor je to mogoče v skladu s potrebo po zaščiti občutljivih virov in metod.

Če povzamemo obsežno preglednost ameriških obveščevalnih dejavnosti:

— Obveščevalna skupnost je na spletu objavila na tisoče strani mnenj sodišča in postopkov agencij, v katerih so povzeti posamezni postopki in zahteve naših obveščevalnih dejavnosti. Prav tako smo objavili poročila o izpolnjevanju veljavnih omejitev s strani obveščevalnih agencij.

— Višji obveščevalni delavci redno govorijo v javnosti o vlogi in dejavnosti svoje organizacije, pri čemer vključujejo opise ureditev in zaščitnih ukrepov v zvezi s skladnostjo, ki urejajo njihovo delo.

— Obveščevalna skupnost je objavila številne dodatne dokumente o obveščevalnih dejavnostih v skladu z zakonom o dostopu do informacij javnega značaja.

— Predsednik je izdal PPD-28, v kateri je javno določil dodatne omejitve za naše obveščevalne dejavnosti, Urad direktorja nacionalne obveščevalne službe pa je izdal dve javni poročili o izvajanju teh omejitev.

— Zakon zdaj od obveščevalne skupnosti zahteva, da objavi pomembna pravna mnenja, ki jih izda sodišče FISA, ali povzetke teh mnenj.

— Vlada mora vsako leto poročati o obsegu uporabe določenih pooblastil v zvezi z nacionalno varnostjo, to pa je dovoljeno tudi podjetjem.

— Odbor za nadzor zasebnosti in državljanskih svoboščin je izdal več podrobnih javnih poročil glede obveščevalnih dejavnosti in bo to delal še naprej.

— Obveščevalna skupnost zagotavlja obsežne tajne informacije kongresnim odborom za nadzor.

— Direktor nacionalne obveščevalne službe je izdal načela preglednosti, s katerimi je uredil dejavnosti obveščevalne skupnosti.

Ta obsežna preglednost bo šla še naprej. Vse javno objavljene informacije bodo seveda na voljo Ministrstvu za trgovino in Evropski komisiji. Letni pregled med Ministrstvom za trgovino in Evropsko komisijo glede izvajanja zasebnostnega ščita bo dal Evropski komisiji priložnost, da obravnava vsa vprašanja, sprožena ob morebitnih novo objavljenih informacijah, in druge zadeve v zvezi z zasebnostnim ščitom in njegovim delovanjem, in razumemo, da lahko Ministrstvo po lastni presoji povabi predstavnike drugih agencij, vključno z obveščevalno skupnostjo, da sodelujejo v tem pregledu. Ta je seveda na voljo poleg mehanizma, zagotovljenega v PPD-28, s katerim lahko države članice EU sprožijo vprašanja v zvezi z nadzorom pri imenovanem uradniku na zunanjem Ministrstvu.

V. PRAVNO VARSTVO

Zakonodaja ZDA zagotavlja več možnosti pravnega varstva za posameznike, ki so predmet nezakonitega elektronskega nadzora za potrebe nacionalne varnosti. V skladu z zakonom o nadzoru tujih obveščevalnih podatkov pravica do zahtevanja nadomestila na sodišču ZDA ni omejena na državljane ZDA. Posameznik, ki lahko dokaže procesno

[1] Na voljo na: https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

upravičenje za tožbo, ima pravna sredstva za izpodbijanje nezakonitega elektronskega nadzora v okviru zakona o nadzoru tujih obveščevalnih podatkov. Na primer, zakon o nadzoru tujih obveščevalnih podatkov omogoča osebam, ki so predmet nezakonitega elektronskega nadzora, da v svojem imenu tožijo ameriške vladne uradnike za denarno odškodnino, vključno z dodatno odškodnino in odvetniškimi stroški. *Glej* člen 1810 naslova 50 zakonodajne zbirke ZDA. Posamezniki, ki lahko dokažejo procesno upravičenost za tožbo, imajo tudi civilno podlago za zahtevek proti Združenim državam za denarno odškodnino, vključno s stroški sodnih postopkov, kadar so bile informacije o njih, pridobljene v elektronskem nadzoru v okviru zakona o nadzoru tujih obveščevalnih podatkov, nezakonito in namerno uporabljene ali razkrite. *Glej* člen 2712 naslova 18 zakonodajne zbirke ZDA. Če namerava vlada uporabiti ali razkriti morebitne informacije, ki so bile pridobljene ali izhajajo iz elektronskega nadzora katerega koli oškodovanca v okviru zakona o nadzoru tujih obveščevalnih podatkov, proti tej osebi v sodnem ali upravnem postopku v Združenih državah, mora zagotoviti predhodno obvestilo o svoji nameri sodišču in tej osebi, ki lahko nato izpodbija zakonitost nadzora in zahteva zadržanje informacij. *Glej* člen 1806 naslova 50 zakonodajne zbirke ZDA. Nazadnje zakon o nadzoru tujih obveščevalnih podatkov zagotavlja tudi kazenske sankcije za posameznike, ki se namerno ukvarjajo z nezakonitim elektronskim nadzorom pod pretvezo zakona ali ki namerno uporabljajo ali razkrivajo informacije, pridobljene z nezakonitim nadzorom. *Glej* člen 1809 naslova 50 zakonodajne zbirke ZDA.

Državljani EU imajo tudi druge možnosti, da se zakonsko pritožijo proti ameriškim vladnim uradnikom zaradi nezakonite vladne uporabe ali dostopa do podatkov, tudi proti vladnim uradnikom, ki kršijo zakon v toku nezakonitega dostopa do ali uporabe informacij za navidezne potrebe nacionalne varnosti. Zakon o računalniških goljufijah in zlorabah (Computer Fraud and Abuse Act) prepoveduje nameren nepooblaščen dostop (ali dostop, ki presega pooblastila) za pridobivanje informacij od finančne ustanove, računalniškega sistema vlade ZDA ali z računalniškim dostopom prek interneta ter grožnje za poškodovanje zaščitenih računalnikov za potrebe izsiljevanja ali goljufije. *Glej* člen 1030 naslova 18 zakonodajne zbirke ZDA. Vsaka oseba katere koli narodnosti, ki utrpi škodo ali izgubo zaradi kršenja tega zakona, lahko toži kršitelja (vključno z vladnim uradnikom) za nadomestilo za škodo ter prepoved ali drugo pravično nadomestilo v skladu s členom 1030(g) ne glede na to, ali je bil izveden kazenski pregon, pod pogojem, da ravnanje vsebuje vsaj eno od več okoliščin, določenih v zakonu. Zakon o zasebnosti elektronskih komunikacij (Electronic Communications Privacy Act ali ECPA) ureja vladni dostop do shranjenih evidenc elektronskih komunikacij in poslov ter informacij o naročnikih, ki jih hranijo tretji ponudniki komunikacijskih storitev. *Glej* člene 2701 do 2712 naslova 18 zakonodajne zbirke ZDA. Zakon o zasebnosti elektronskih komunikacij omogoča oškodovancu, da toži vladne uradnike za namerni nezakoniti dostop do shranjenih podatkov. Zakon o zasebnosti elektronskih komunikacij velja za vse osebe ne glede na državljanstvo, oškodovanci pa lahko prejmejo odškodnino in odvetniške stroške. Zakon o pravici do finančne zasebnosti (Right to Financial Privacy Act ali RFPA) omejuje dostop ameriške vlade do bančnih in borznoposredniških evidenc posameznih strank. *Glej* člene 3401 do 3422 naslova 12 zakonodajne zbirke ZDA. V skladu z zakonom o pravici do finančne zasebnosti lahko stranka banke ali borznoposredniške hiše toži vlado ZDA za zakonsko, dejansko in dodatno odškodnino zaradi nepravilno pridobljenega dostopa do evidenc stranke, ugotovitev, da je takšen nepravilen dostop bil nameren, pa avtomatično sproži preiskavo o morebitnih disciplinskih ukrepih proti ustreznim vladnim uslužbencem. *Glej* člen 3417 naslova 12 zakonodajne zbirke ZDA.

Nazadnje zakon o dostopu do informacij javnega značaja (Freedom of Information Act ali FOIA) vsem osebam zagotavlja sredstva, da zahtevajo dostop do obstoječih evidenc zveznih agencij o kateri koli temi v skladu z določenimi kategorijami izjem. *Glej* člen 552(b) naslova 5 zakonodajne zbirke ZDA. Te vključujejo omejitve dostopa do tajnih informacij v zvezi z nacionalno varnostjo, osebnih informacij drugih posameznikov in informacij v zvezi s kazenskimi preiskavami ter so primerljive z omejitvami, ki jih narodi odredijo s svojimi zakoni o dostopu do informacij. Te omejitve veljajo enako za Američane in Neameričane. Na spore v zvezi z objavo zahtevanih evidenc v skladu z zakonom o dostopu do informacij javnega značaja se je mogoče pritožiti upravno in nato na zveznem sodišču. Sodišče mora na novo ugotoviti, ali so bile evidence ustrezno zadržane (člen 552(a)(4)(B) naslova 5 zakonodajne zbirke ZDA), in lahko vladi odredi, da zagotovi dostop do evidenc. V nekaterih zadevah so sodišča ovrgla trditve vlade, da je treba zadevne informacije pridržati kot tajne ([1]). Čeprav ni na voljo nobenih denarnih odškodnin, lahko sodišča prisodijo odvetniške stroške.

VI. SKLEP

Združene države priznavajo, da morajo naše dejavnosti SIGINT in druge obveščevalne dejavnosti upoštevati, da je treba vse osebe obravnavati z dostojanstvom in spoštovanjem ne glede na njihovo narodnost ali kraj bivanja ter da imajo vse osebe zakonite interese zasebnosti pri ravnanju z njihovimi osebnimi informacijami. Združene države uporabljajo dejavnosti SIGINT samo, da bi ugodile interesom nacionalne varnosti in zunanjepolitičnih interesov ter za zaščito svojih državljanov in državljanov svojih zaveznikov in partnerjev pred oškodovanjem. Skratka, obveščevalna skupnost ne izvaja neselektivnega nadzora kogarkoli, vključno z navadnimi evropskimi državljani. Zbiranje obveščevalnih podatkov v

([1]) Glej, na primer, New York Times proti Department of Justice, 756 F.3d 100 (2d Cir. 2014); American Civil Liberties Union proti CIA, 710 F.3d 422 (D.C. Cir. 2014).

okviru SIGINT se izvaja samo z ustreznimi pooblastili in na način, ki je strogo v skladu s temi omejitvami; šele po obravnavi razpoložljivosti alternativnih virov, vključno z diplomatskimi in javnimi viri; in na način, ki daje prednost ustreznim in izvedljivim alternativam. Kadar koli je izvedljivo, se SIGINT izvaja le z zbiranjem, ki je osredotočeno na posebne cilje ali teme tujih obveščevalnih podatkov z uporabo diskriminant.

V tem pogledu je bila politika ZDA potrjena v PPD-28. V tem okviru ameriške obveščevalne agencije nimajo zakonskega pooblastila, virov, tehničnih zmožnosti ali želje, da prestrezajo vso svetovno komunikacijo. Te agencije ne berejo elektronskih sporočil vseh v Združenih državah ali vseh na svetu. Skladno s PPD-28, Združene države zagotavljajo trdno varstvo osebnih informacij nedržavljanov ZDA, ki se zbirajo z obveščevalno dejavnostjo SIGINT. Če je izvedljivo v skladu z nacionalno varnostjo, to vključuje politike in postopke za zmanjševanje hranjenja in širjenja osebnih informacij v zvezi z nedržavljani ZDA, ki so primerljivi z varstvom, kot ga uživajo državljani ZDA. Poleg tega je, kakor obravnavano zgoraj, celostna ureditev nadzora usmerjenega pooblastila po členu 702 zakona o nadzoru tujih obveščevalnih podatkov brez primere. Nazadnje pomembne spremembe zakona o ameriški obveščevalni dejavnosti, kakor so določene v ameriškem zakonu o svobodi (USA FREEDOM Act), in pobude, ki jih vodi Urad direktorja nacionalne obveščevalne službe za spodbujanje preglednosti v obveščevalni skupnosti, močno izboljšujejo varstvo zasebnosti in državljanskih svoboščin vseh posameznikov ne glede na njihovo narodnost.

S spoštovanjem.

Robert S. Litt

21. junij 2016

Justin S. Antonipillai
Svetovalec
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Namestnik pomočnika ministra
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Spoštovana g. Antonipillai in g. Dean,

pišem vama z namenom predložiti dodatne informacije o tem, kako so Združene države izvajajo množično zbiranje podatkov SIGINT. Kot je pojasnjeno v opombi 5 k predsedniški politični direktivi št. 28 (v nadaljevanju: PPD-28), se „množično“ zbiranje nanaša na pridobitev relativno velikega obsega obveščevalnih informacij ali podatkov SIGINT v okoliščinah, v katerih obveščevalna skupnost ne more uporabiti identifikatorja, povezanega z določeno ciljno osebo (kot je e-poštni naslov ali telefonska številka ciljne osebe), da bi osredotočila zbiranje. Vendar to ne pomeni, da je tovrstno zbiranje se „masovno“ ali „neselektivno“. PPD-28 namreč tudi zahteva, da so „obveščevalne dejavnosti SIGINT kolikor je le izvedljivo prilagojene.“ Na podlagi teh pooblastil obveščevalna skupnost sprejema ukrepe za zagotovitev, da bodo, tudi če ne moremo uporabiti posebnih identifikatorjev za ciljno zbiranje, podatki, ki se zbirajo, verjetno vsebovali tuje obveščevalne podatke, ki bodo ustrezali zahtevam, ki so jih oblikovalci politik ZDA navedli na podlagi postopka, pojasnjenega v mojem prejšnjem dopisu, ter zmanjšuje količino neupoštevnih informacij, ki se zbirajo.

Obveščevalna skupnost ima lahko na primer nalogo pridobiti obveščevalne podatke SIGINT o dejavnostih teroristične skupine, ki deluje v regiji države Bližnjega vzhoda in za katero se domneva, da načrtuje napade na zahodnoevropske države, vendar pa ne pozna imen, telefonskih številk, elektronskih naslovov ali drugi posebni identifikatorji posameznikov, povezanih s to teroristično skupino. Lahko se odloči, da bo na to skupino ciljala z zbiranjem in komunikacij, poslanih v to regijo in iz nje, da bi opravila nadaljnji pregled in analizo z namenom prepoznavanja tistih sporočil, ki se nanašajo na to skupino. Pri tem si bo obveščevalna skupnost prizadevala, da bi čim bolj zožila zbiranje podatkov. To se šteje za „množično“ zbiranje, ker je uporaba diskriminant ni izvedljiva, vendar tako zbiranje ni niti „masovno“ niti „neselektivno“, temveč je kolikor je le mogoče natančno osredotočeno.

Tako Združene države tudi takrat, ko izbiranje ciljev z uporabo posebnih izbirnikov ni mogoče, ne zbirajo vseh sporočil iz vseh komunikacijskih sredstev povsod po svetu, temveč uporabljajo filtre in druga tehnična orodja za osredotočanje zbiranja na tista sredstva, ki verjetno vsebujejo sporočila s tujo obveščevalno vrednostjo. Pri tem obveščevalne dejavnosti SIGINT, ki jih izvajajo Združene države, zajamejo le majhen del sporočil, ki potekajo po internetu.

Poleg tega, kot je navedeno v mojem prejšnjem dopisu, ker „množično“ zbiranje pomeni večje tveganje za zbiranje neupoštevnih komunikacij, PPD-28 omejuje uporabo obveščevalnih podatkov SIGINT, ki bi jih obveščevalna skupnost zbrala množično, na šest določenih namenov. PPD-28 in politike agencije za izvajanje PPD-28 omejujejo tudi shranjevanje in širjenje osebnih informacij, pridobljenih na podlagi obveščevalnih podatkov SIGINT, ne glede na to, ali so bile informacije zbrane množično ali s ciljno usmerjenim zbiranjem, in ne glede na posameznikovo državljanstvo.

Tako „množično“ zbiranje, ki ga izvaja obveščevalna skupnost, ni „masovno“ ali „neselektivno“, temveč vključuje uporabo metod in orodij za filtriranje zbiranja, da bi se osredotočilo na zbiranje materiala, ki bo ustrezal zahtevam, ki so jih oblikovalci politik navedli glede tujih obveščevalnih podatkov, pri čemer čim bolj zmanjšuje zbiranje neupoštevnih

informacij ter določa stroga pravila za varstvo neupoštevnih informacij, ki bi se lahko zbrale. Politike in postopki, opisani v tem pismu, se uporabljajo za množično zbiranje vseh obveščevalnih podatkov SIGINT, vključno z vsem množičnim zbiranjem komunikacij v Evropo in iz nje, ne da bi se pri tem potrdil ali zanikal obstoj takega zbiranja.

Prosili ste me tudi za več informacij o odboru za nadzor zasebnosti in državljanskih svoboščin (Privacy and Civil Liberties Oversight Board, v nadaljnjem besedilu: PCLOB) in generalnih inšpektorjih ter o pooblastilih teh organov. PCLOB je neodvisna agencija izvršilne veje oblasti. Člane dvostrankarskega petčlanskega odbora imenuje predsednik, potrdi pa jih Senat ([1]). Mandat posameznega člana odbora traja šest let. Člani odbora in osebje pridobijo ustrezna varnostna potrdila, da lahko v celoti izvršujejo svoje zakonsko določene dolžnosti in odgovornosti ([2]).

Naloga PCLOB je zagotavljati, da se prizadevanja zvezne vlade za preprečevanje terorizma uravnotežijo s potrebo po varstvu zasebnosti in državljanskih svoboščin. Odbor ima dve temeljni nalogi – nadzor in svetovanje. PCLOB sam oblikuje svoj program in določa, katere dejavnosti nadzora ali svetovanja želi izvajati.

PCLOB v svoji *nadzorni* vlogi pregleduje in analizira ukrepe, ki jih izvršilna veja oblasti sprejme za zaščito države pred terorizmom, pri čemer zagotavlja, da je potreba po takih ukrepih uravnotežena s potrebo po varstvu zasebnosti in državljanskih svoboščin ([3]). Najnovejši zaključen nadzorni pregled PCLOB se je osredotočal na nadzorne programe, ki se izvajajo na podlagi člena 702 FISA ([4]). Trenutno odbor izvaja pregled obveščevalnih dejavnosti, ki se izvajajo na podlagi odredbe št. 12333 ([5]).

PCLOB v svoji *svetovalni* vlogi zagotavlja, da se vprašanja svoboščin ustrezno upoštevajo pri oblikovanju in izvajanju zakonov, drugih predpisov in politik, povezanih s prizadevanji za varovanje države pred terorizmom ([6]).

Da bi lahko opravljal svoje naloge, je odbor z zakonom pooblaščen za dostopanje do vseh ustreznih evidenc, poročil, revizij, pregledov, dokumentov, okrožnic, priporočil in vsega drugega zadevnega gradiva Agencije, vključno z zaupnimi informacijami v skladu z zakonom ([7]). Poleg tega lahko odbor opravi razgovore in sprejema izjave ali javna pričevanja katerega koli uradnika ali delavca vseh organov izvršilne veje oblasti ([8]). Odbor lahko tudi pisno zahteva, naj generalni državni tožilec v njegovem imenu izda sodne pozive, ki osebam zunaj izvršilne veje oblasti nalagajo, naj predložijo ustrezne informacije ([9]).

Nazadnje, za PCLOB veljajo zakonsko določene zahteve glede javne preglednosti. To vključuje obveščanje javnosti o dejavnostih odbora z organizacijo javnih obravnav in dajanjem njegovih poročil na voljo javnosti, in sicer v največjem mogočem obsegu, ki je skladen z varovanjem tajnih podatkov ([10]). Poleg tega mora PCLOB v primeru, da agencija izvršilne veje oblasti ne upošteva njegovega mnenja, o tem poročati.

Generalni inšpektorji v okviru obveščevalne skupnosti izvajajo revizije, inšpekcijske preglede in preglede programov in dejavnosti obveščevalne skupnosti, da bi opredelili in odpravili sistemska tveganja, ranljivosti in pomanjkljivosti. Poleg tega generalni inšpektorji preučujejo pritožbe ali informacije o domnevnih kršitvah zakonov, pravil ali drugih predpisov

([1]) Člen 2000ee(a) in (h) naslova 42 Zakonodajne zbirke ZDA.
([2]) Člen 2000ee(k) naslova 42 Zakonodajne zbirke ZDA.
([3]) Člen 2000ee(d)(2) naslova 42 Zakonodajne zbirke ZDA.
([4]) Glej, na splošno, https://www.pclob.gov/library.html#oversightreports.
([5]) Glej, na splošno, https://www.pclob.gov/events/2015/may13.html.
([6]) Člen 2000ee(d)(1) naslova 42 Zakonodajne zbirke ZDA; glej tudi PCLOB Advisory Function Policy and Procedure, Policy 2015-004 (Politika in postopek za svetovalno funkcijo PCLOB, politika št. 2015-004), na voljo na: https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) Člen 2000ee(g)(1)(A) naslova 42 Zakonodajne zbirke ZDA.
([8]) Člen 2000ee(g)(1)(B) naslova 42 Zakonodajne zbirke ZDA.
([9]) Člen 2000ee(g)(1)(D) naslova 42 Zakonodajne zbirke ZDA.
([10]) Člen 2000eee(f) naslova 42 Zakonodajne zbirke ZDA.

ali domnevnih slabem upravljanju, velikem zapravljanju sredstev, zlorabi pooblastil, ali znatni in posebni nevarnosti za javno zdravje in varnost v programih in dejavnostih obveščevalne skupnosti. Neodvisnost generalnih inšpektorjev je ključen element objektivnosti in integritete vsakega poročila, ugotovitve in priporočila, ki jih generalni inšpektor izda. Med najbolj odločilnimi elementi za ohranjanje neodvisnosti generalnih inšpektorjev so postopek za njihovo imenovanje in razrešitev, ločena operativna in proračunska pooblastila ter pooblastila glede osebja in zahteve za dvojno poročanje vodjem agencij izvršilne veje oblasti ter Kongresu.

Kongres je ustanovila neodvisen urad generalnega inšpektorja v vseh agencijah izvršilne veje oblasti, vključno z vsemi organi obveščevalne skupnosti ([1]). Po sprejetju zakona o obveščevalnih pooblastilih za davčno leto 2015 skoraj vse generalne inšpektorje, ki nadzirajo organe obveščevalne skupnosti, imenuje predsednik, potrdi pa Senat. Gre za generalne inšpektorje, ki nadzirajo ministrstvo za pravosodje, Osrednjo obveščevalno agencijo (CIA), agencijo za nacionalno varnost in obveščevalno skupnost ([2]). Poleg tega so ti generalni inšpektorji uradniki s stalno funkcijo, ki so nestrankarski, razreši pa jih lahko le predsednik. Medtem ko ZDA ustava določa, da je predsednik pristojen za razrešitev generalnega inšpektorja, pa se ta pristojnost redko uporablja, zahteva pa tudi, da predsednik razrešitev generalnega inšpektorja pisno obrazloži Kongresu 30 dni preden jo izvede ([3]). Ta postopek imenovanja generalnega inšpektorja zagotavlja, da uradniki izvršilne veje oblasti ne vplivajo neupravičeno na izbiro, imenovanje ali razrešitev generalnega inšpektorja.

Drugič, generalni inšpektorji imajo znatna zakonsko določena pooblastila za opravljanje revizij, preiskav in pregledov programov in dejavnosti izvršilne veje oblasti. Poleg nadzornih preiskav in pregledov, ki jih zahteva zakon, imajo generalni inšpektorji široko diskrecijo pri izvajanju nadzora nad programi in dejavnostmi po lastni izbiri ([4]). Zakon zagotavlja, da imajo generalni inšpektorji pri izvrševanju te pristojnosti na voljo neodvisna sredstva za opravljanje svojih nalog, vključno s pooblastilom za zaposlovanje lastnega osebja in ločeno navajanje proračunskih zahtev Kongresu ([5]). Zakon zagotavlja, da imajo generalni inšpektorji dostop do informacij, ki jih potrebujejo za izvajanje svojih nalog. To vključuje pooblastila za neposredno dostopanje do vseh evidenc in informacij agencij, v katerih so podrobno opisani programi in dejavnosti agencije, ne glede na zaupnost, pooblastila za pridobitev sodnega naloga za predložitev informacij in dokumentov ter pooblastila za opravljanje zapriseg ([6]). V določenih primerih lahko vodja agencije izvršilne veje oblasti prepove dejavnost generalnega inšpektorja, če bi, na primer, revizija ali preiskava, ki jo opravlja generalni inšpektor, bistveno škodovala interesom nacionalne varnosti Združenih držav. Tudi izvajanje tega pooblastila pa je zelo neobičajno in zahteva, da vodja agencije Kongres v 30 dneh obvestiti o razlogih za njegovo uveljavljanje ([7]). Direktor nacionalne obveščevalne agencije ni denimo nikoli uveljavljal tega omejitvenega pooblastila pri nobeni dejavnosti generalnega inšpektorja.

Tretjič, generalni inšpektorji morajo tako vodje agencij izvršilne veje oblasti kot Kongres v celoti in ažurno obveščati prek poročil o goljufijah in drugih resnih težavah, zlorabah ter pomanjkljivostih v zvezi s programi in dejavnostmi agencij izvršilne veje oblasti ([8]). Z dvojnim poročanjem se krepi neodvisnost generalnega inšpektorja, saj zagotavlja preglednost nadzornega procesa generalnega inšpektorja ter vodjam agencij omogoča izvajanje priporočil generalnega inšpektorja še preden bi Kongres lahko sprejel zakonodajne ukrepe. Generalni inšpektorji so na primer zakonsko zavezane k pripravi polletnih poročil, ki opisujejo take težave in popravne ukrepe, ki so bili doslej sprejeti ([9]). Agencije izvršilne veje oblasti obravnavajo ugotovitve in priporočila generalnega inšpektorja resno in generalni inšpektorji lahko

([1]) Člena 2 in 4 zakona o generalnem inšpektorju (Inspector General Act) iz leta 1978 s spremembami; Člen 103H(b) in (e) zakona o nacionalni varnosti iz leta 1947 s spremembami (v nadaljnjem besedilu: Zakon o nacionalni varnosti). Člen 17(a) zakona o centralni obveščevalni agenciji (v nadaljnjem besedilu: zakon o CIA).

([2]) Glej Zbirko aktov Kongresa s področja javnega prava, št. 113-293, str. 128, zakon 3990 (2014). Predsednik ne imenuje le generalnih inšpektorjev za obrambno obveščevalno agencijo in za nacionalno agencijo za geoprostorske obveščevalne podatke; vendar sta generalni inšpektor za ministrstvo za obrambo in generalni inšpektor za obveščevalno skupnost sočasno pristojna za ti agenciji.

([3]) Člen 3 Zakona o generalnem inšpektorju iz leta 1978 s spremembami; člen 103H(c) Zakona o nacionalni varnosti in člen 17(b) zakona o CIA.

([4]) Glej člena 4(a) in 6(a)(2) zakona o generalnem inšpektorju iz leta 1947; člen 103H(e) in (g)(2)(a) zakona o nacionalni varnosti ter člen 17 (a) in (c) zakona o CIA.

([5]) Členi 3(d), 6(a)(7) in 6(f) zakona o generalnem inšpektorju; členi 103(d), (i), (j) in (m) zakona o nacionalni varnosti ter člena 17(e)(7) in (f) zakona o CIA.

([6]) Člen 6(a)(1), (3), (4), (5), in (6) zakona o generalnem inšpektorju; Člen 103H(g)(2) zakona o nacionalni varnosti ter člen 17(e)(1), (2), (4) in (5) zakona o CIA.

([7]) Glej, na primer, člena 8(b) in 8E(a) zakona o generalnem inšpektorju; člen 103H(f) zakona o nacionalni varnosti ter člen 17(b) Zakona o CIA.

([8]) Člen 4(a)(5) zakona o generalnem inšpektorju; člen 103H(a)(b)(3) in (4) zakona o nacionalni varnosti ter člen 17(a)(2) in (4) zakona o CIA.

([9]) Členi 2(3), 4(a) in 5 Zakona o generalnem inšpektorju; člen 103H(k) Zakona o nacionalni varnosti ter člen 17(d) Zakona o CIA. Generalni inšpektor Ministrstva za pravosodje daje svoja javno objavljena poročila na voljo na spletni strani http://oig.justice.gov/reports/all.htm. Podobno daje generalni inšpektor za obveščevalno skupnost svoja polletna poročila javnosti na voljo na spletni strani https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

pogosto vključijo sprejemanje in izvajanje svojih priporočil v navedena in druga poročila, ki se predložijo Kongresu, v nekaterih primerih pa tudi dajo na voljo javnosti ([1]). Poleg te strukture dvojnega poročanja imajo generalni inšpektorji tudi nalogo, da prijavitelje nepravilnosti iz izvršilne veje oblasti usmerijo k ustreznim nadzornim odborom Kongresa, da bi razkrili domnevne goljufije, zapravljanje ali zlorabe pri programih in dejavnostih izvršilne veje oblasti. Identiteta oseb, ki se tako javijo, je zavarovana pred razkritjem izvršilni veji oblasti, s čimer se prijavitelji nepravilnosti ščitijo pred morebitnimi ukrepi s področja prepovedi osebja ali varnostnega preverjanja, ki bi bili sprejeti v povračilo za poročanje generalnemu inšpektorju ([2]). Ker prijavitelji nepravilnosti pogosto predstavljajo vire za preiskave generalnih inšpektorjev, se z možnostjo poročanja o njihovih pomislekih Kongresu brez vplivanja izvršilne veje oblasti povečuje učinkovitost nadzora, ki ga izvajajo generalni inšpektorji. Zaradi te neodvisnosti lahko generalni inšpektorji z objektivnostjo in integriteto spodbudijo ekonomičnost, učinkovitost in odgovornost pri agencijah izvršilne veje oblasti.

Nazadnje, Kongres je ustanovil svet generalnih inšpektorjev za integriteto in učinkovitost. Ta svet med drugim razvija standarde generalnih inšpektorjev za revizije, preiskave in preglede; spodbuja usposabljanje; ter je pooblaščen za obravnavanje domnevnih kršitev generalnih inšpektorjev, s čimer se nadzirajo generalni inšpektorji, ki nadzirajo vse ostale ([3]).

Upam, da se vam bodo te informacije zdele koristne.

S spoštovanjem.

Robert S. Litt,

Glavni svetovalec

([1]) Členi 2(3), 4(a) in 5 Zakona o generalnem inšpektorju; člen 103H(k) Zakona o nacionalni varnosti ter člen 17(d) Zakona o CIA. Generalni inšpektor Ministrstva za pravosodje daje svoja javno objavljena poročila na voljo na spletni strani http://oig.justice.gov/reports/all.htm. Podobno daje generalni inšpektor za obveščevalno skupnost svoja polletna poročila javnosti na voljo na spletni strani https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Člen 7 zakona o generalnem inšpektorju; Člen 103H(g)(3) zakona o nacionalni varnosti ter člen 17(e)(3) zakona o CIA.

([3]) Člen 11 zakona o generalnem inšpektorju.

PRILOGA VII

Pismo namestnika pomočnika državnega tožilca in svetovalca za mednarodne zadeve Brucea Swartza, Ministrstvo za pravosodje ZDA

19. februar 2016

Justin S. Antonipillai
Svetovalec
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Namestnik pomočnika ministra
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Spoštovana g. Antonipillai in g. Dean,

to pismo podaja kratek pregled glavnih preiskovalnih sredstev za pridobivanje poslovnih podatkov in drugih podatkov iz evidenc korporacij v Združenih državah za (civilne ali regulativne) potrebe kazenskega pregona ali javnega interesa, vključno z omejitvami dostopa, določenimi v teh pooblastilih ([1]). Ti pravni procesi so nediskriminatorni, saj so uporabljeni za pridobivanje informacij od korporacij v Združenih državah, vključno s podjetji, ki se bodo samocertificirala v okviru zasebnostnega ščita EU-ZDA, ne glede na narodnost posameznika, na katerega se nanašajo podatki. Poleg tega lahko korporacije, ki so jim vročeni sodni postopki v Združenih državah, le-te izpodbijajo na sodišču, kakor je navedeno spodaj ([2]).

V zvezi z zaseganjem podatkov s strani javnih organov je zlasti pomemben četrti amandma Ustave ZDA, ki določa, da „pravica ljudi, da so oni sami, njihove hiše, dokumenti in predmeti varni pred nerazumnimi preiskavami in zasegi, ne sme biti kršena in izdan ne sme biti noben nalog, razen na podlagi utemeljenega suma, podprtega z zaprisego ali izjavo, in ki zlasti opisuje kraj, ki ga je treba preiskati, ter osebe in predmete, ki jih je treba zaseči." Ustava ZDA, IV. amandma. Kakor je navedlo vrhovno sodišče ZDA v zadevi *Berger proti State of New York*, „osnovni namen tega amandmaja, kakor je priznan v številnih odločitvah tega sodišča, je zaščititi zasebnost in varnost posameznikov pred samovoljnimi vdori vladnih uradnikov." 388 U.S. 41, 53 (1967) (*navajam zadevo Camara proti Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). V domačih kazenskih preiskavah četrti amandma od uslužbencev organov kazenskega pregona običajno zahteva, da pridobijo sodni nalog, preden opravijo preiskavo. *Glej Katz proti United States*, 389 U.S. 347, 357 (1967). Kadar zahteva naloga ne velja, je vladna dejavnost podvržena preskusu „razumnosti" v skladu s četrtim amandmajem. Sama Ustava torej zagotavlja, da vlada ZDA nima neomejene ali samovoljne moči, da zaseže zasebne informacije.

Organi kazenskega pregona:

Zvezni tožilci, ki so uradniki Ministrstva za pravosodje, in zvezni preiskovalni agenti, ki zajemajo agente Zveznega preiskovalnega urada (FBI), tj. organa kazenskega pregona znotraj Ministrstva za pravosodje, lahko prisilijo korporacije v Združenih državah, da predložijo dokumente in druge podatke iz evidenc za potrebe kazenske preiskave z več vrstami

([1]) Ta pregled ne opisuje preiskovalnih orodij za nacionalno varnost, ki jih uporabljajo organi kazenskega pregona pri terorističnih in drugih preiskavah v zvezi z nacionalno varnostjo, vključno s sodnimi pozivi v zvezi z nacionalno varnostjo (NSL) za določene informacije v poročilih o kreditni sposobnosti, finančnih podatkih in elektronskih podatkih o naročnikih in poslih, glej člen 3414 naslova 12 zakonodajne zbirke ZDA; člen 1681u naslova 15 zakonodajne zbirke ZDA; člen 1681v naslova 15 zakonodajne zbirke ZDA; člen 2709 naslova 18 zakonodajne zbirke ZDA, in za elektronski nadzor, naloge za preiskavo, poslovne knjige in drugo zbiranje komunikacij v skladu z zakonom o nadzoru tujih obveščevalnih podatkov, glej člen 1801 *et seq* naslova 50 zakonodajne zbirke ZDA.

([2]) Ta dokument obravnava zvezne organe kazenskega pregona in nadzorne organe; kršitve državnih zakonov preiščejo države in se jim sodi na državnih sodiščih. Državni organi kazenskega pregona uporabljajo naloge in pozive, izdane v okviru državnega zakona, na pravzaprav enak način, kot je opisan tukaj, vendar z možnostjo, da za državne sodne postopke velja varstvo, ki ga zagotavljajo ustave držav in ki presega določbe v Ustavi ZDA. Varstvo državnih zakonov mora biti vsaj enakovredno varstvu Ustave ZDA, med drugim tudi četrtemu amandmaju.

obveznih sodnih postopkov, vključno s pozivi velike porote, sodnimi pozivi in nalogi za preiskavo, ter lahko pridobijo druge komunikacije v skladu z zveznimi kazenskimi pooblastili za prisluškovanje telefonskim pogovorom in uporabo snemalnikov klicev.

Pozivi velike porote ali pozivi na obravnavo: Pozivi na obravnavo kaznivega dejanja se uporabljajo v podporo usmerjenim kazenskim preiskavam. Poziv velike porote je uradna zahteva, ki jo izda velika porota (običajno na zahtevo zveznega tožilca) v podporo preiskavi posameznega suma kršitve kazenskega prava, ki jo izvaja velika porota. Velike porote so preiskovalna roka sodišča in jih izbere sodnik. V sodnem pozivu se lahko od osebe zahteva, da priča v postopku ali predloži ali zagotovi poslovne evidence, elektronsko shranjene informacije ali druge oprijemljive predmete. Informacije se morajo nanašati na preiskavo, sodni poziv pa ne more biti nerazumen, ker je preširok ali ker je zatirajoč ali obremenjujoč. Na tej podlagi lahko prejemnik vloži predlog za izpodbijanje sodnega poziva. *Glej* Fed. R. Crim. P. 17. V omejenih okoliščinah je mogoče uporabiti sodne pozive na obravnavo za dokumente, potem ko je velika porota vložila obtožnico v zadevi.

Pooblastilo za izdajo sodnih pozivov: V kazenskih in civilnopravnih preiskavah je mogoče uveljaviti pooblastila za izdajo sodnih pozivov. V okviru kazenskega pregona več zveznih zakonov dovoljuje uporabo sodnih pozivov za predložitev ali zagotovitev poslovnih evidenc, elektronsko shranjenih informacij ali drugih oprijemljivih predmetov v preiskavah goljufij v zdravstvu zlorabe otrok, zaščite tajne službe, zadevah v zvezi z nadzorovanimi snovmi in preiskavah generalnega inšpektorja, v katere so vpletene vladne agencije. Če želi vlada uveljaviti sodni poziv na sodišču, lahko prejemnik sodnega poziva, tako kot prejemnik poziva velike porote, zagovarja stališče, da je poziv nerazumen, ker je preširok ali ker je zatirajoč ali obremenjujoč.

Sodne odločbe za snemalnike klicev ter naprave za pasti in sledenje: V skladu s kazenskimi določbami v zvezi s snemalniki klicev ter napravami za pasti in sledenje lahko organi kazenskega pregona pridobijo sodno odločbo za pridobivanje sprotnih nevsebinskih informacij glede klicanih telefonskih številk, usmerjanja, naslavljanja in signaliziranja o telefonski številki ali elektronski pošti ob potrditvi, da so zagotovljene informacije pomembne za kazensko preiskavo v teku. *Glej* člene 3121-3127 naslova 18 zakonodajne zbirke ZDA. Uporaba ali namestitev takšne naprave zunaj zakona je zvezni zločin.

Zakon o zasebnosti elektronskih komunikacij (Electronic Communications Privacy Act ali ECPA): Vladni dostop do informacij o naročnikih, podatkov o prometu in shranjenih vsebin komunikacij, ki jih hranijo telefonska podjetja ponudnikov internetnih storitev in drugi ponudniki storitev, urejajo dodatna pravila v skladu z naslovom II ECPA, imenovanem tudi zakon o shranjenih komunikacijah (Stored Communications Act ali SCA, členi 2701 do 2712 naslova 18 zakonodajne zbirke ZDA. SCA določa sistem zakonskih pravic do zasebnosti, ki omejujejo dostop organov kazenskega pregona do podatkov, ki so več kot potrebni po ustavnem pravu od strank in naročnikov ponudnikov internetnih storitev. SCA zagotavlja višjo raven varstva zasebnosti glede na vsiljivost zbiranja. Za informacije o registraciji naročnikov, naslove IP in povezane časovne žige ter podatke za obračunavanje morajo organi kazenskega pregona pridobiti sodni poziv. Za večino drugih shranjenih nevsebinskih informacij, kot so glave v elektronskem sporočilu brez vrstice z zadevo, mora organ kazenskega pregona predstaviti sodniku posamezna dejstva, ki dokazujejo, da so zahtevane informacije pomembne in bistvene v tekoči kazenski preiskavi. Za pridobivanje shranjene vsebine elektronskih komunikacij organi kazenskega pregona na splošno pridobijo nalog od sodnika na podlagi utemeljenega suma, da zadevni račun vsebuje dokaze o kaznivem dejanju. SCA zagotavlja tudi civilno odgovornost in kazenske sankcije.

Sodne odločbe za nadzor v skladu z zveznim zakonom o prisluškovanju telefonskim pogovorom: Organi kazenskega pregona lahko dodatno sprotno prestrezajo komunikacije po telefonu, ustno ali elektronsko komunikacijo za potrebe kazenske preiskave v skladu z zveznim zakonom o prisluškovanju telefonskim pogovorom. *Glej* člene 2510-2522 naslova 18 zakonodajne zbirke ZDA. To pooblastilo je na voljo le v skladu s sodno odločbo, v kateri sodnik ugotovi, da

med drugim obstaja utemeljeni sum, da bo prisluškovanje telefonskim pogovorom ali elektronsko prestrezanje privedlo do dokazov zveznega zločina ali do lokacije ubežnika, ki beži pred pregonom. Zakon zagotavlja civilno odgovornost in kazenske sankcije za kršitve določb glede prisluškovanja telefonskim pogovorom.

Nalog za preiskavo – pravilo 41: Organi kazenskega pregona lahko fizično preiščejo prostore v Združenih državah, kadar jim to dovoli sodnik. Organi kazenskega pregona morajo na podlagi „utemeljenega suma“ sodniku dokazati, da je bilo ali bo vsak čas storjeno kaznivo dejanje, predmete, povezane s kaznivim dejanjem, pa da je mogoče odkriti na kraju, navedenem v nalogu. To pooblastilo se pogosto uporabi, kadar je potrebna fizična preiskava prostorov s strani policije zaradi nevarnosti, da bodo uničeni dokazi, če bo korporaciji vročen sodni poziv ali drugi nalog za predložitev. *Glej* Ustava ZDA IV. amandma (podrobneje obravnavan zgoraj), Fed. R. Crim. P. 41. Oseba, na katero se nanaša nalog za preiskavo, lahko poda predlog za razveljavitev naloga zaradi preobsežnosti, nadležnosti ali druge neprimerne pridobitve, oškodovane stranke s procesno upravičenostjo pa lahko zadržijo morebitne dokaze, pridobljene v nezakoniti preiskavi. *Glej Mapp proti Ohio*, 367 U.S. 643 (1961).

Smernice in politike Ministrstva za pravosodje: Poleg teh ustavnih in zakonskih omejitev na podlagi pravil glede vladnega dostopa do podatkov je državni tožilec izdal smernice, ki postavljajo nadaljnje omejitve dostopa do podatkov s strani organov kazenskega pregona in ki vsebujejo tudi elemente varstva zasebnosti in državljanskih svoboščin. Na primer, smernice državnega tožilca za domače operacije Zveznega preiskovalnega urada (FBI) (september 2008) (v nadaljnjem besedilu „smernice AG FBI“), na voljo na http://www.justice.gov/archive/opa/docs/guidelines.pdf, postavljajo omejitve glede uporabe preiskovalnih sredstev pri iskanju informacij v zvezi s preiskavami zveznih zločinov. Te smernice določajo, da mora FBI uporabiti najmanj vsiljive preiskovalne metode, ki so izvedljive, ob upoštevanju vpliva na zasebnost in državljanske svoboščine ter potencialne škode ugledu. Poleg tega opozarjajo, da „je jasno, da mora FBI opraviti preiskave in druge dejavnosti na zakonit in razumen način, ki spoštuje svoboščine in zasebnost ter se izogiba nepotrebnim vdorom v življenja ljudi, ki spoštujejo zakon.“ *Glej* smernice AG FBI na strani 5. FBI izvaja te smernice z navodili FBI za domače preiskave in operacije (FBI Domestic Investigations and Operations Guide ali DIOG), na voljo na https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), celovitim priročnikom, ki vsebuje podrobne omejitve uporabe preiskovalnih orodij ter navodila, ki zagotavljajo, da so državljanske svoboščine in zasebnost zaščitene v vsaki preiskavi. Dodatna pravila in politike, ki predpisujejo omejitve preiskovalnih dejavnosti zveznih tožilcev, so določene v priročniku za ameriške odvetnike (**United States Attorneys' Manual** ali USAM), prav tako na voljo na http://www.justice.gov/usam/united-states-attorneys-manual.

Civilni in regulativni organi (javni interes):

Pomembne omejitve so postavljene tudi za dostop do podatkov, ki jih hranijo korporacije v Združenih državah, v civilne in regulativne namene (tj. javni interes). Agencije s civilno in regulativno odgovornostjo lahko korporacijam izdajo pozive za poslovne evidence, elektronsko shranjene informacije ali druge oprijemljive predmete. Te agencije pri izvajanju sodnih ali civilnih pozivov omejujejo ne le njihovi organizacijski zakoni, temveč tudi neodvisni sodni pregled pozivov pred morebitno sodno izvršitvijo. *Glej, na primer*, Fed. R. Civ. P. 45. Agencije lahko zahtevajo dostop samo do podatkov, ki so pomembni v zadevah v okviru njihovih pooblastil za urejanje. Poleg tega lahko prejemnik sodnega poziva izpodbija izvršitev tega poziva na sodišču tako, da predloži dokaze, da agencija ni delovala v skladu z osnovnimi standardi razumnosti, kakor je obravnavano zgoraj.

Tu so tudi druge pravne podlage za podjetja, s katerimi lahko izpodbijajo zahteve za podatke upravnih organov na podlagi njihove posebne panoge in vrst podatkov, ki jim imajo v lasti. Na primer, finančne ustanove lahko izpodbijajo sodne pozive, v katerih so zahtevane določene vrste informacij, kot kršitve zakona o bančni tajnosti (Bank Secrecy Act) in njegovih izvedbenih predpisov. *Glej* člen 5318 naslova 31 zakonodajne zbirke ZDA, 31 C.F.R. Part X. Druga podjetja se lahko oprejo na zakon o poštenem kreditnem poročanju (Fair Credit Reporting Act, *glej* člen 1681b naslova 15 zakonodajne zbirke ZDA) ali na gostitelja drugih zakonov, značilnih za sektorje. Zloraba pooblastila agencije za poziv lahko privede do odškodninske odgovornosti agencije ali osebne odgovornosti uradnikov agencije. *Glej*, na primer, zakon o pravici do finančne zasebnosti (Right to Financial Privacy Act, členi 3401–3422 naslova 12 zakonodajne zbirke ZDA). Sodišča v Združenih državah tako delujejo kot varuhi pred neprimernimi zakonskimi zahtevami in zagotavljajo neodvisen nadzor nad ukrepi zveznih agencij.

Nazadnje mora kakršno koli zakonsko pooblastilo, da morajo upravni organi fizično zaseči evidence podjetja v Združenih državah v skladu z upravno preiskavo, izpolnjevati zahteve četrtega amandmaja. *Glej See proti City of Seattle*, 387 U.S. 541 (1967).

Sklep

Vse dejavnosti kazenskega pregona in regulativne dejavnosti v Združenih državah morajo biti skladne z veljavno zakonodajo, vključno z Ustavo ZDA, zakoni, pravili in predpisi. Takšne dejavnosti morajo biti skladne tudi z veljavnimi politikami, vključno z morebitnimi smernicami državnega tožilca, ki urejajo zvezne dejavnosti kazenskega pregona. Pravni okvir, opisan zgoraj, omejuje zmožnost ameriških organov kazenskega pregona in nadzora za pridobivanje informacij od korporacij v Združenih državah – ne glede na to, ali so informacije v zvezi z državljani ZDA ali državljani tujih držav – poleg tega pa dovoljuje sodni pregled katere koli vladne zahteve za podatke v skladu s temi pooblastili.

S spoštovanjem.

Bruce C. Swartz

Namestnik pomočnika državnega tožilca in
svetovalec za mednarodne zadeve

IZVEDBENI SKLEP KOMISIJE (EU) 2016/1251

z dne 12. julija 2016

o sprejetju večletnega programa Unije za zbiranje, upravljanje in uporabo podatkov v sektorjih ribištva in akvakulture za obdobje 2017–2019

(notificirano pod dokumentarno številko C(2016) 4329)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe Sveta (ES) št. 199/2008 z dne 25. februarja 2008 o vzpostavitvi okvira Skupnosti za zbiranje, upravljanje in uporabo podatkov v sektorju ribištva in podporo znanstvenemu svetovanju v zvezi s skupno ribiško politiko ([1]) in zlasti člena 3 Uredbe,

ob upoštevanju naslednjega:

(1) V skladu s členom 3 Uredbe (ES) št. 199/2008 se večletni program Unije za zbiranje, upravljanje in uporabo podatkov v sektorju ribištva sprejme za obdobje treh let za zagotovitev enotne uporabe obveznosti zbiranja in upravljanja podatkov.

(2) Sedanji večletni program Unije temelji na večletnem programu za obdobje 2011–2013, ki je bil podaljšan z Izvedbenim sklepom Komisije C(2013)5243 za premostitev obdobja med sprejetjem Uredbe (EU) št. 1380/2013 Evropskega parlamenta in Sveta ([2]) in 31. decembrom 2016. Zato je treba vzpostaviti večletni program Unije za obdobje treh let z začetkom 1. januarja 2017.

(3) V skladu s členom 25 Uredbe (EU) št. 1380/2013 države članice zbirajo biološke, okoljske, tehnične in socialno-ekonomske podatke, ki so potrebni za upravljanje ribištva. Večletni program Unije je nujen, da države članice določijo in načrtujejo svoje dejavnosti zbiranja podatkov v svojih nacionalnih delovnih načrtih. V skladu s členom 21 Uredbe (EU) št. 508/2014 Evropskega parlamenta in Sveta ([3]) je treba te nacionalne delovne načrte predložiti Komisiji do 31. oktobra v letu, ki je predhodno letu, v katerem se bo delovni načrt uporabljal.

(4) Večletni program Unije bi moral opredeliti zahteve za zbiranje podatkov v skladu s členom 1 Uredbe (ES) št. 199/2008. Vsebovati bi moral elemente, potrebne za izvajanje skupne ribiške politike, če jih ne zahtevajo že drugi zakonodajni okviri.

(5) Za uresničitev ciljev prenovljene skupne ribiške politike iz člena 2 Uredbe (EU) št. 1380/2013 je treba posodobiti zahteve Unije glede podatkov za zanesljivo znanstveno svetovanje za obdobje, ki se začne 1. januarja 2017.

(6) Poleg tega nove mednarodne obveznosti in zaveze, uvedene za države članice in Unijo z večstranskimi in dvostranskimi sporazumi na področju ribištva, zahtevajo vključitev nekaterih zahtev glede zbiranja podatkov v večletni program Unije, zlasti tistih, ki izhajajo iz sporazumov o partnerstvu o trajnostnem ribištvu.

([1]) UL L 60, 5.3.2008, str. 1.

([2]) Uredba (EU) št. 1380/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o skupni ribiški politiki in o spremembi uredb Sveta (ES) št. 1954/2003 in (ES) št. 1224/2009 ter razveljavitvi uredb Sveta (ES) št. 2371/2002 in (ES) št. 639/2004 ter Sklepa Sveta 2004/585/ES (UL L 354, 28.12.2013, str. 22).

([3]) Uredba (EU) št. 508/2014 Evropskega parlamenta in Sveta z dne 15. maja 2014 o Evropskem skladu za pomorstvo in ribištvo in razveljavitvi uredb Sveta (ES) št. 2328/2003, (ES) št. 861/2006, (ES) št. 1198/2006 in (ES) št. 791/2007 in Uredbe (EU) št. 1255/2011 Evropskega parlamenta in Sveta (UL L 149, 20.5.2014, str. 1).

(7) Ocena sedanjega okvira za zbiranje, upravljanje in uporabo podatkov v sektorju ribištva in nadaljnja posvetovanja z deležniki so pokazali, da bi se moral večletni program Unije osredotočiti na to, kateri podatki se zahtevajo od držav članic, ne na metode za njihovo zbiranje. Metodološke zahteve se opišejo v delovnih načrtih držav članic, ki jih mora odobriti Komisija, ob tesnem sodelovanju med državami članicami na ravni morskih regij.

(8) V programu Unije za obdobje 2017–2019 bi bilo torej treba upoštevati vse te elemente in cilje Uredbe (EU) št. 1380/2013, zlasti člena 2 in 25 Uredbe, kolikor je mogoče v sedanjem pravnem okviru iz Uredbe (ES) št. 199/2008. Če nove zahteve po podatkih presegajo sedanji zakonodajni okvir, bi morale biti neobvezne. Ko bo začel veljati nov pravni okvir o spremembi Uredbe (ES) št. 199/2008, Komisija lahko spremeni večletni program Unije, če je to potrebno, da se upoštevajo nove zahteve glede zbiranja podatkov.

(9) Komisija je upoštevala priporočila, ki izhajajo iz posvetovanja v okviru regionalnih usklajevalnih sestankov iz člena 5 Uredbe (ES) št. 199/2008 ter Znanstvenega, tehničnega in gospodarskega odbora za ribištvo (STECF). Opravljeno je bilo tudi posvetovanje z drugimi ustreznimi posvetovalnimi znanstvenimi organi, kot je Mednarodni svet za raziskovanje morja (ICES), pa tudi s predstavniki držav članic, zbranimi v posebnih strokovnih skupinah.

(10) Zaradi pravne varnosti bi bilo treba razveljaviti Izvedbeni sklep C(2013)5243.

(11) Ukrepi iz tega sklepa so v skladu z mnenjem Upravljalnega odbora za ribištvo in ribogojstvo –

SPREJELA NASLEDNJI SKLEP:

Člen 1

Večletni program Unije za zbiranje, upravljanje in uporabo podatkov v sektorju ribištva za obdobje 2017–2019 iz člena 3 Uredbe (ES) št. 199/2008 je določen v Prilogi k temu sklepu.

Člen 2

Izvedbeni sklep C(2013)5243 se razveljavi z učinkom od 1. januarja 2017.

Člen 3

Ta sklep je naslovljen na države članice.

V Bruslju, 12. julija 2016

Za Komisijo

Karmenu VELLA

Član Komisije

PRILOGA

POGLAVJE I

Opredelitev pojmov

Za namene te priloge se uporabljajo opredelitve pojmov iz Uredbe Sveta (ES) št. 1224/2009 ([1]), Izvedbene uredbe Komisije (EU) št. 404/2011 ([2]) in Uredbe (EU) št. 1380/2013 Evropskega parlamenta in Sveta ([3]). Poleg teh se uporabljajo tudi naslednje opredelitve pojmov:

(1) **Aktivna plovila**: plovila, ki so v koledarskem letu izvedla kakršne koli ribolovne operacije (en dan ali več). Plovilo, ki med letom ni izvajalo ribolovnih operacij, se šteje za „neaktivno".

(2) **Anadromne vrste**: živi vodni viri z življenjskim ciklom, ki se začne z valitvijo v sladki vodi, selitvijo v morsko vodo, vrnitvijo in konča z drstenjem v sladki vodi.

(3) **Katadromne vrste**: živi vodni viri z življenjskim ciklom, ki se začne z valitvijo v slani vodi, selitvijo v sladko vodo, vrnitvijo in konča z drstenjem v slani vodi.

(4) **Delež ulova**: del celotnega ulova, kot je del iztovorjenega ulova, katerega velikost je nad najmanjšo referenčno velikostjo ohranjanja, del iztovorjenega ulova, katerega velikost je pod najmanjšo referenčno velikostjo ohranjanja, del zavrženega ulova, katerega velikost je pod najmanjšo referenčno velikostjo ohranjanja, zavržki *de minimis* ali zavržki.

(5) **Dnevi na morju**: vsako neprekinjeno obdobje 24 ur (ali del obdobja), v katerem je plovilo prisotno na območju in odsotno iz pristanišča.

(6) **Ribolovni dnevi**: vsak koledarski dan na morju, ko poteka ribolovna operacija, brez poseganja v mednarodne obveznosti Unije in njenih držav članic. Eno ribolovno potovanje lahko prispeva tako k vsoti ribolovnih dni za pasivna orodja kot k vsoti ribolovnih dni za aktivna orodja na navedenem potovanju.

(7) **Ribolovno območje**: skupina geografskih enot/geografske enote, v katerih poteka ribolov. Te enote se določijo na ravni morske regije na podlagi obstoječih območij, ki so jih določile regionalne organizacije za upravljanje ribištva ali znanstveni organi.

(8) **Segment flote**: skupina plovil enakega dolžinskega razreda (LOA, celotna dolžina) in z enakim prevladujočim ribolovnim orodjem med letom.

(9) **Ribolovna dejavnost**: skupina ribolovnih operacij, s katerimi se lovijo podobne vrste (skupek vrst), pri katerih se uporablja podobno orodje ([4]) v istem delu leta in/ali na istem območju in za katere so značilni podobni vzorci izkoriščanja.

(10) **Raziskave na morju**: potovanja, izvedena na raziskovalnem plovilu ali plovilu, namenjenemu znanstvenim raziskavam za spremljanje staleža in ekosistema, ki ga za to nalogo določi organ, pristojen za izvajanje nacionalnega delovnega načrta, pripravljenega v skladu s členom 21 Uredbe (EU) št. 508/2014.

([1]) Uredba Sveta (ES) št. 1224/2009 z dne 20. novembra 2009 o vzpostavitvi nadzornega sistema Skupnosti za zagotavljanje skladnosti s pravili skupne ribiške politike, o spremembi uredb (ES) št. 847/96, (ES) št. 2371/2002, (ES) št. 811/2004, (ES) št. 768/2005, (ES) št. 2115/2005, (ES) št. 2166/2005, (ES) št. 388/2006, (ES) št. 509/2007, (ES) št. 676/2007, (ES) št. 1098/2007, (ES) št. 1300/2008, (ES) št. 1342/2008 in razveljavitvi uredb (EGS) št. 2847/93, (ES) št. 1627/94 in (ES) št. 1966/2006 (UL L 343, 22.12.2009, str. 1).

([2]) Izvedbena uredba Komisije (EU) št. 404/2011 z dne 8. aprila 2011 o določitvi podrobnih pravil za izvajanje Uredbe Sveta (ES) št. 1224/2009 o vzpostavitvi nadzornega sistema Skupnosti za zagotavljanje skladnosti s pravili skupne ribiške politike (UL L 112, 30.4.2011, str. 1).

([3]) Uredba (EU) št. 1380/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o skupni ribiški politiki in o spremembi uredb Sveta (ES) št. 1954/2003 in (ES) št. 1224/2009 ter razveljavitvi uredb Sveta (ES) št. 2371/2002 in (ES) št. 639/2004 ter Sklepa Sveta 2004/585/ES (UL L 354, 28.12.2013, str. 22).

([4]) Kakor je opredeljeno v Prilogi XI k Uredbi (EU) št. 404/2011.

POGLAVJE II

Metode zbiranja podatkov

Metode in kakovost zbiranja podatkov so primerne za predvidene namene, opredeljene v členu 25 Uredbe (EU) št. 1380/2013, in upoštevajo najboljše prakse ter ustrezne metodologije, ki jih priporočajo ustrezni znanstveni organi. V ta namen neodvisni znanstveni organi v ustreznih časovnih presledkih pregledujejo metode in rezultate uporabe teh metod, da se preveri njihova ustreznost za upravljanje skupne ribiške politike.

POGLAVJE III

Zahteve glede podatkov

1. **Sklopi podatkov**

1.1 Države članice v okviru načrtov, izdelanih v skladu s členom 21 Uredbe (EU) št. 508/2014, pripravijo podatke, ki se zbirajo v naslednjih sklopih, kot je opredeljeno v točkah 2 do 7 tega poglavja:

(a) biološke podatke po deležu ulova o staležih, ulovljenih v okviru komercialnega ribolova Unije v vodah Unije in zunaj voda Unije ter v okviru rekreacijskega ribolova v vodah Unije;

(b) podatke za oceno vpliva ribolova Unije na morski ekosistem v vodah Unije in zunaj voda Unije;

(c) podrobne podatke o dejavnosti ribiških plovil Unije v vodah Unije in zunaj voda Unije v skladu z Uredbo (ES) št. 1224/2009;

(d) socialne in ekonomske podatke o ribolovu ([1]);

(e) socialne, ekonomske in okoljske podatke o ribogojstvu.

1.2 Podatki, ki se zbirajo, se določijo v skladu s členi 3, 4 in 5 Uredbe (ES) št. 199/2008 ter ob upoštevanju pragov, določenih v poglavju V te priloge.

1.3 Podatki se zberejo, da se omogočijo veljavne ocene za vrste ribolova, časovna obdobja in območja na podlagi potreb končnih uporabnikov, dogovorjenih na ravni morskih regij. Pogostost zbiranja podatkov se usklajuje na ravni morske regije, razen če je v tej prilogi in ustreznih tabelah določeno drugače.

2. **Biološki podatki o staležih, ujetih v okviru komercialnega ribolova Unije v vodah Unije in zunaj njenih voda ter rekreacijskega ribolova v vodah Unije**

Ti podatki zajemajo naslednje:

(a) Količine ulova po vrstah in biološke podatke iz posameznih osebkov, ki omogočajo oceno:

(i) za komercialni ribolov: količine in frekvence dolžine vseh deležev ulova (vključno z zavržki in neželenim ulovom) za staleže, navedene v tabelah 1A, 1B in 1C, sporočene na ravni agregiranja 6 iz tabele 2. Časovna ločljivost se usklajuje na ravni morskih regij na podlagi potreb končnih uporabnikov;

(ii) za komercialni ribolov: povprečne teže in starostne porazdelitve ulova staležev iz tabel 1A, 1B in 1C. Izbor staležev, iz katerih se zberejo te spremenljivke, in časovna ločljivost se usklajujeta na ravni morskih regij na podlagi potreb končnih uporabnikov;

([1]) Podatki o predelovalni industriji se lahko zbirajo prostovoljno.

(iii) za komercialni ribolov: podatkov o razmerju med spoloma, zrelosti in plodnosti za staleže iz tabel 1A, 1B in 1C za ulove s pogostostjo, potrebno za znanstveno svetovanje. Izbor staležev, iz katerih se zberejo te spremenljivke, in časovna ločljivost se usklajujeta na ravni morskih regij na podlagi potreb končnih uporabnikov;

(iv) za rekreacijski ribolov: letne količine (število in teža ali dolžina) ulova in izpusta za vrste iz tabele 3 in/ali vrste, opredeljene na ravni morskih regij, kadar je to potrebno za namene upravljanja ribištva. Potrebe končnih uporabnikov po podatkih o starosti ali drugih bioloških podatkih, kot so določeni v odstavkih (i) do (iii), se za rekreacijski ribolov ocenijo na ravni morskih regij.

(b) Poleg zbranih podatkov iz točke (a) podatke o anadromnih in katadromnih vrstah iz tabele 1E, ujetih v okviru komercialnega ribolova v sladkovodni fazi njihovega življenjskega cikla, ne glede na to, kako se izvaja ta vrsta ribolova, kot sledi:

(i) spremenljivke, povezane s staleži (za posamezne osebke glede starosti, dolžine, teže, spola, zrelosti in plodnosti, po fazi življenjskega cikla, toda nadalje opredeljene na podlagi vrste in območja), ter

(ii) letne količine ulova po starostnih razredih ali fazi življenjskega cikla.

(c) Poleg tega:

za jegulje informacije (npr. podatke, ocene, povezane trende itd.), zbrane vsako leto v vsaj enem rečnem bazenu na enoto za upravljanje jegulj, o:

(i) številčnosti novih mladih rib

(ii) številčnosti stalnega staleža (rumena jegulja) in

(iii) številu ali teži in razmerju med spoloma srebrnih jegulj, ki se selijo,

in v zvezi z vsemi divjimi lososi: informacije, ki se zbirajo letno – razen če je drugače dogovorjeno na regionalni ravni – o številčnosti srebrne mladice lososa in marogaste mladice lososa ter številu naraščajočega števila osebkov.

Določitev rek, ki se spremljajo za jegulje in atlantske lososе, se opredeli na regionalni ravni. Izbor staležev, iz katerih se zberejo te spremenljivke, se usklajuje na regionalni ravni na podlagi potreb končnih uporabnikov.

3. **Podatki za oceno vpliva ribolova Unije na morske ekosisteme v vodah Unije in zunaj voda Unije**

Navedeni podatki zajemajo naslednje:

(a) Za vse vrste ribolova: podatke o naključnem prilovu vseh ptic, sesalcev in plazilcev ter rib, zaščitenih v skladu z zakonodajo Unije in mednarodnimi sporazumi, vključno z vrstami iz Tabele 1D, tudi o odsotnosti ulova, zbrane med potovanjem znanstvenih opazovalcev na ribolovnih potovanjih ali iz ladijskih dnevnikov ribičev samih.

Kadar se za podatke, zbrane med potovanji opazovalcev, šteje, da ne zagotavljajo zadostnih podatkov o naključnem prilovu za potrebe končnih uporabnikov, države članice izvedejo druge metodologije. Izbor teh metodologij se usklajuje na ravni morskih regij na podlagi potreb končnih uporabnikov.

(b) Podatke za pomoč pri oceni vpliva ribolova na morske habitate v vodah Unije in zunaj voda Unije.

Spremenljivke, ki se uporabljajo za ocenjevanje vpliva ribolova na morske habitate, so spremenljivke, evidentirane v skladu z Uredbo (ES) št. 1224/2009. Podatki se razčlenijo na ravni ribolovne aktivnosti 3 ([1]), razen če se na regionalni ravni zahteva nižja raven agregiranja, zlasti v primeru zaščitenih morskih območij.

([1]) Glej Tabelo 2.

Kadar podatki, evidentirani v skladu z Uredbo (ES) št. 1224/2009, niso pravilne resolucije ali niso dovolj kakovostni ali dovolj obsežni za nameravano znanstveno uporabo, se zbirajo na drugačen način z uporabo ustreznih metod vzorčenja. Podatki, kot so evidentirani v skladu z Uredbo (ES) št. 1224/2009, se dajo na voljo nacionalnim institucijam za izvajanje delovnih načrtov na ustrezni ravni agregiranja.

(c) Podatke za ocenjevanje ravni ribolova in vpliva ribolovnih dejavnosti na morske biološke vire in morske ekosisteme, kot so učinki na nekomercialne vrste, odnose med plenilcem in plenom ter naravno umrljivost vrste rib v vsaki morski regiji.

Ti podatki se najprej ocenijo v okviru pilotnih študij. Države članice na podlagi rezultatov teh pilotnih študij določijo prihodnje zbiranje podatkov za posamezno morsko regijo, usklajeno na ravni morskih regij na podlagi potreb končnih uporabnikov.

4. **Podrobni podatki o dejavnosti ribiških plovil Unije** [1] **v vodah Unije in zunaj voda Unije v skladu z Uredbo (ES) št. 1224/2009**

Podatki za oceno dejavnosti ribiških plovil Unije v vodah Unije in zunaj voda Unije so sestavljeni iz spremenljivk, kot je navedeno v tabeli 4. Podatki, kot so evidentirani, sporočeni in posredovani v skladu z Uredbo (ES) št. 1224/2009, se dajo na voljo nacionalnim institucijam za izvajanje delovnih načrtov v obliki primarnih podatkov. Kadar se ti podatki ne zbirajo v skladu z Uredbo (ES) št. 1224/2009 ali kadar podatki, zbrani na podlagi Uredbe (ES) št. 1224/2009, niso pravilne resolucije ali niso dovolj kakovostni ali dovolj obsežni za nameravano znanstveno uporabo, se zbirajo na drugačen način z uporabo ustreznih metod vzorčenja. Te metode omogočajo oceno spremenljivk iz tabele 4 na najnižji ustrezni geografski ravni po segmentih flote (tabela 5a) in ravni ribolovne dejavnosti 6 (tabela 2).

5. **Socialno-ekonomski podatki o ribištvu, da se omogoči ocena socialno-ekonomske uspešnosti ribiškega sektorja Unije**

Ti podatki zajemajo naslednje:

(a) Ekonomske spremenljivke, kot so navedene v tabeli 5A v skladu z razčlenitvijo sektorja iz tabele 5B in v skladu z nadregijami, kot so opredeljene v tabeli 5C.

Populacija so vsa aktivna in neaktivna plovila, registrirana v registru ribolovne flote Unije, kot je opredeljen v Uredbi Komisije (ES) št. 26/2004 [2] dne 31. decembra v letu poročanja, in plovila, ki niso navedena v registru na navedeni datum, vendar so opravljala ribolov vsaj en dan v letu poročanja.

Za neaktivna plovila se zbirajo samo podatki o vrednosti kapitala in stroških kapitala.

Kadar obstaja tveganje identificiranja fizične in/ali pravne osebe, se lahko za poročanje ekonomskih spremenljivk uporabi združevanje za zagotovitev zaupnosti statističnih podatkov. Združevanje se lahko uporabi, če je potrebno za pripravo statistično zanesljivih načrtov vzorčenja. Takšno združevanje je ves čas dosledno.

Ekonomski podatki se zbirajo na letni osnovi.

(b) Socialne spremenljivke, kot so navedene v tabeli 6.

Socialni podatki se zbirajo vsaka tri leta z začetkom leta 2018.

Podatki o zaposlenosti po stopnji izobrazbe in zaposlenosti po državljanstvu se lahko zbirajo na podlagi pilotnih študij.

---

[1] Vključno s posebnimi zahtevami za regionalne organizacije za upravljanje ribištva, kot so določene v Uredbi (EU) 1343/2011 Evropskega parlamenta in Sveta z dne 13. decembra 2011 o nekaterih določbah za ribolov na območju Sporazuma GFCM (Generalne komisije za ribištvo v Sredozemlju) in spremembi Uredbe Sveta (ES) št. 1967/2006 o ukrepih za upravljanje za trajnostno izkoriščanje ribolovnih virov v Sredozemskem morju (UL L 347, 30.12.2011, str. 44).

[2] Uredba Komisije (ES) št. 26/2004 z dne 30. decembra 2003 o registru ribolovne flote Skupnosti (UL L 5, 9.1.2004, str. 25).

6. **Socialni, ekonomski in okoljski podatki o morskem ribogojstvu in neobvezno o sladkovodnem ribogojstvu, da se omogoči ocena socialne, ekonomske in okoljske učinkovitosti sektorja ribogojstva v Uniji**

Navedeni podatki zajemajo naslednje:

(a) Ekonomske spremenljivke, kot so navedene v tabeli 7, glede na razčlenitev sektorja iz tabele 9.

Populacija so vsa podjetja, katerih primarna dejavnost je opredeljena v skladu z oznakama 03.21 in 03.22 evropske klasifikacije gospodarskih dejavnosti NACE ([1]) in ki delujejo za dobiček.

Ekonomski podatki se zbirajo na letni osnovi.

(b) Socialne spremenljivke, kot so navedene v tabeli 6.

Socialni podatki se zbirajo vsaka tri leta z začetkom leta 2018.

Podatki o zaposlenosti po stopnji izobrazbe in zaposlenosti po državljanstvu se lahko zbirajo na podlagi pilotnih študij.

(c) Okoljske podatke o ribogojstvu, kakor so navedeni v tabeli 8, da se omogoči ocena vidikov okoljske uspešnosti.

Okoljski podatki se lahko zbirajo na podlagi pilotnih študij in se ekstrapolirajo, da se prikažejo skupne vrednosti za ustrezno skupno količino rib, ulovljenih v državi članici.

Okoljski podatki se zbirajo vsaki dve leti.

POGLAVJE IV

Raziskave na morju

1. Izvedejo se vsaj vse raziskave na morju iz tabele 10, razen če je iz pregleda raziskav mogoče sklepati, da raziskava ni več primerna za oceno staležev in upravljanje ribištva. Na podlagi istih meril za znanstveni pregled se v to tabelo lahko dodajo nove raziskave.

2. Države članice v okviru delovnih načrtov, izdelanih v skladu s členom 21 Uredbe (EU) št. 508/2014, opredelijo raziskave na morju, ki se izvajajo, in so odgovorne za te raziskave.

3. Prispevki posameznih držav članic k mednarodnim raziskavam se usklajujejo znotraj iste morske regije.

4. Države članice v okviru svojih nacionalnih delovnih načrtov jamčijo za kontinuiteto s prejšnjimi raziskavami.

POGLAVJE V

Pragi

1. To poglavje se uporablja za ribištvo Unije.

2. Bioloških podatkov ni treba zbirati, če za določen stalež ali vrsto rib velja naslednje:

(a) delež zadevnega celotnega dovoljenega ulova (TAC) države članice predstavlja manj kot 10 % celotnega TAC Unije ali

([1]) Uredba (ES) št. 1893/2006 Evropskega Parlamenta in Sveta z dne 20. decembra 2006 o uvedbi statistične klasifikacije gospodarskih dejavnosti NACE Revizija 2 in o spremembi Uredbe Sveta (EGS) št. 3037/90 kakor tudi nekaterih uredb ES o posebnih statističnih področjih (UL L 393, 30.12.2006, str. 1).

(b) če TAC ni določen, skupno število iztovorov države članice za stalež ali vrsto znaša manj kot 10 % celotnega iztovora EU v zadnjih 3 letih ali

(c) skupni letni iztovor države članice za vrsto je manj kot 200 ton. Za vrste, pri katerih je potrebno posebno upravljanje, se lahko določi nižji prag na ravni morskih regij.

Kadar je vsota ustreznih kvot več držav članic, katerih delež TAC znaša manj kot 10 %, višja od 25 % deleža TAC za določen stalež, se 10-odstotni prag iz točke (a) ne uporablja, države članice pa zagotovijo delitev nalog na regionalni ravni za zagotovitev, da je stalež zajet z vzorčenjem v skladu s potrebami končnih uporabnikov.

Za velike pelagične vrste ter anadromne in katadromne vrste se prag ne uporablja.

3. Brez poseganja v bolj specifične določbe v zvezi z mednarodnimi obveznostmi v okviru regionalnih organizacij za upravljanje ribištva bioloških podatkov ni treba zbirati, če je delež Unije za določen stalež mednarodno lovljenih rib, razen staležev velikih pelagičnih ali izrazito selivskih vrst, manjši od 10 %.

4. Države članice ocene ulova iz obstoječih raziskav v okviru rekreacijskega ribolova, vključno s tistimi, ki so izvedene v skladu z okvirom za zbiranje podatkov, ali iz dodatne pilotne študije predložijo v dveh letih od datuma začetka veljavnosti tega sklepa. Te raziskave omogočijo oceno deleža ulovov v okviru rekreacijskega ribolova glede na komercialni ulov za vse vrste v morski regiji, za katere se zahtevajo ocene rekreacijskega ulova v okviru tega večletnega programa Unije. Nadaljnje načrtovanje in obseg nacionalnih raziskav rekreacijskega ribolova, vključno z morebitnimi pragovi za zbiranje podatkov, se usklajujeta na ravni morskih regij na podlagi potreb končnih uporabnikov.

Prag se ne uporablja za rekreacijski ulov staležev rib, ki so vključeni v načrte za obnovo ali večletne načrte upravljanja, kot so tisti, ki veljajo za ribolov velikih pelagičnih vrst in izrazito selivskih vrst.

5. Socialnih in ekonomskih podatkov o ribogojstvu ni treba zbirati, če skupna proizvodnja države članice predstavlja manj kot 1 % skupne količine in vrednosti proizvodnje Unije. Podatkov o ribogojstvu ni treba zbirati za vrste, ki predstavljajo manj kot 10 % proizvodnje države članice na področju ribogojstva po količini in vrednosti. Poleg tega države članice, katerih skupna proizvodnja znaša manj kot 2,5 % skupne količine in vrednosti proizvodnje Unije na področju ribogojstva, lahko določijo poenostavljeno metodologijo, kot so pilotne študije, za ekstrapolacijo podatkov, potrebnih za vrste, ki predstavljajo več kot 10 % proizvodnje držav članic na področju ribogojstva po količini in vrednosti.

Referenčni podatki so zadnji predloženi podatki držav članic v skladu z Uredbo (ES) št. 762/2008 Evropskega parlamenta in Sveta ([1]) ter ustrezni podatki, ki jih je objavil Eurostat.

6. Okoljskih podatkov o ribogojstvu ni treba zbirati, če skupna proizvodnja države članice na področju ribogojstva predstavlja manj kot 2,5 % skupne količine in vrednosti proizvodnje Unije.

Referenčni podatki so zadnji predloženi podatki držav članic v skladu z Uredbo (ES) št. 762/2008 Evropskega parlamenta in Sveta ter ustrezni podatki, ki jih je objavil Eurostat.

7. Sodelovanje (fizično ali finančno) države članice v raziskavah na morju iz tabele 10 ni obvezno, če je njen delež TAC Unije za ciljne vrste v okviru raziskav pod pragom 3 %. Kadar TAC ni določen, (fizično ali finančno) sodelovanje države članice v raziskavah na morju ni obvezno, če je njen delež pri skupnem iztovoru Unije v zadnjih treh letih za stalež ali vrsto pod pragom 3 %. Pragovi za raziskave več vrst in ekosistemov se lahko določijo na ravni morskih regij.

8. Ne glede na točke 2 do 7 se v isti morski regiji države članice lahko sporazumejo o alternativnih pragih.

([1]) Uredba (ES) št. 762/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o predložitvi statističnih podatkov o ribogojstvu s strani držav članic in razveljavitvi Uredbe Sveta (ES) št. 788/96 (UL L 218, 13.8.2008, str. 1).

BIOLOŠKI PODATKI

Tabela 1A

Staleži v vodah Unije

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES (1), IBSFC (2) ali FAO (3)), kjer se stalež nahaja/ oznaka staleža
Vzhodna Arktika, Norveško morje in Barentsovo morje		
Jegulja	*Anguilla anguilla*	I, II
Morski menek	*Brosme brosme*	I, II
Atlantski sled	*Clupea harengus*	I, II
Trska	*Gadus morhua*	I, II
Kapelan	*Mallotus villosus*	I, II
Vahnja	*Melanogrammus aeglefinus*	I, II
Sinji mol	*Micromesistius poutassou*	I–II
Severna kozica	*Pandalus borealis*	I, II
Saj	*Pollachius virens*	I, II
Grenlandska morska plošča	*Reinhardtius hippoglossoides*	I, II
Atlantski losos	*Salmo salar*	I, II
Skuša	*Scomber scombrus*	II
Veliki rdeči okun	*Sebastes marinus*	I, II
Kljunati okun	*Sebastes mentella*	I, II
Šur	*Trachurus trachurus*	IIa
Skagerrak in Kattegat		
Prava peščenka	*Ammodytidae*	IIIa
Jegulja	*Anguilla anguilla*	IIIa
Sled	*Clupea harengus*	IIIa/22–24, IIIa
Okroglonosi repak	*Centroscymnus coelolepis*	IIIa
Sivi krulec	*Eutrigla gurnardus*	IIIa
Vzhodnoatlantski rdeči krulec	*Aspitrigla cuculus*	IIIa

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES [1], IBSFC [2] ali FAO [3]), kjer se stalež nahaja/ oznaka staleža
Trska	*Gadus morhua*	IIIaN
Trska	*Gadus morhua*	IIIaS
Sivi jezik	*Glyptocephalus cynoglossus*	IIIa
Limanda	*Limanda limanda*	IIIa
Vahnja	*Melanogrammus aeglefinus*	IIIa
Mol	*Merlangius merlangus*	IIIa
Oslič	*Merluccius merluccius*	IIIa
Sinji mol	*Micromesistius poutassou*	IIIa
Škamp	*Nephrops norvegicus*	funkcionalna enota
Severna kozica	*Pandalus borealis*	IIIa
Morska plošča	*Pleuronectes platessa*	IIIa
Saj	*Pollachius virens*	IIIa
Atlantski losos	*Salmo salar*	IIIa
Romb	*Psetta maxima*	IIIa
Skuša	*Scomber scombrus*	IIIa
Gladki romb	*Scophthalmus rhombus*	IIIa
Morski list	*Solea solea*	IIIa
Papalina	*Sprattus sprattus*	IIIa
Norveški molič	*Trisopterus esmarki*	IIIa
Vsi komercialni morski psi, raže in skati [4]	*Selachii, Rajidae*	IIIa
Baltsko morje –		
Jegulja	*Anguilla anguilla*	22–32
Sled	*Clupea harengus*	22–24/25–29, 32/30/31/ Riški zaliv
Ozimica	*Coregonus lavaretus*	IIId
Mala ozimica	*Coregonus albula*	22–32
Trska	*Gadus morhua*	22–24/25–32

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES [1], IBSFC [2] ali FAO [3]), kjer se stalež nahaja/ oznaka staleža
Limanda	*Limanda limanda*	22–32
Navadni ostriž	*Perca fluviatilis*	IIId
Iverka	*Platichthys flesus*	22–32
Morska plošča	*Pleuronectes platessa*	22–32
Romb	*Psetta maxima*	22–32
Atlantski losos	*Salmo salar*	22–31/32
Morska postrv	*Salmo trutta*	22–32
Smuč	*Sander lucioperca*	IIId
Gladki romb	*Scophthalmus rhombus*	22–32
Morski list	*Solea solea*	22
Papalina	*Sprattus sprattus*	22–32
Severno morje in vzhodni Rokavski preliv		
Prava peščenka	*Ammodytidae*	IV
Ostrigarji	*Anarhichas* spp.	IV
Jegulja	*Anguilla anguilla*	IV, VIId
Srebrenke	*Argentina* spp.	IV
Sivi krulec	*Eutrigla gurnardus*	IV
Morski menek	*Brosme brosme*	IV
Sled	*Clupea harengus*	IV, VIId
Navadna peščena kozica	*Crangon crangon*	IV, VIId
Brancin	*Dicentrarchus labrax*	IV, VIId
Sivi krulec	*Eutrigla gurnardus*	IV
Trska	*Gadus morhua*	IV, VIId
Sivi jezik	*Glyptocephalus cynoglossus*	IV
Sinjeusti okun	*Helicolenus dactylopterus*	IV
Štiripegasti krilati romb	*Lepidorhombus boscii*	IV, VIId

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES (1), IBSFC (2) ali FAO (3)), kjer se stalež nahaja/ oznaka staleža
Krilati romb	*Lepidorhombus whiffiagonis*	IV, VIId
Limanda	*Limanda limanda*	IV, VIId
Mala morska spaka	*Lophius budegassa*	IV, VIId
Morska spaka	*Lophius piscatorius*	IV
Čebulastooki repak	*Macrourus berglax*	IV
Vahnja	*Melanogrammus aeglefinus*	IV
Mol	*Merlangius merlangus*	IV, VIId
Oslič	*Merluccius merluccius*	IV, VII
Sinji mol	*Micromesistius poutassou*	IV, VIId
Rdeči jezik	*Microstomus kitt*	IV, VIId
Modri leng	*Molva dypterygia*	IV
Leng	*Molva molva*	IV
Bradač	*Mullus barbatus*	IV, VIId
Progasti bradač	*Mullus surmuletus*	IV, VIId
Škamp	*Nephrops norvegicus*	vse funkcionalne enote
Severna kozica	*Pandalus borealis*	IVa vzhodno/IVa/IV
Grebenasta pokrovača	*Pecten maximus*	VIId
Tabinja belica	*Phycis blennoides*	IV
Tabinja	*Phycis phycis*	IV
Iverka	*Platichthys flesus*	IV
Morska plošča	*Pleuronectes platessa*	IV
Morska plošča	*Pleuronectes platessa*	VIId
Saj	*Pollachius virens*	IV
Romb	*Psetta maxima*	IV, VIId
Grenlandska morska plošča	*Reinhardtius hippoglossoides*	IV

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES [1], IBSFC [2] ali FAO [3]), kjer se stalež nahaja/ oznaka staleža
Atlantski losos	*Salmo salar*	IV, VIId
Skuša	*Scomber scombrus*	IV, VIId
Gladki romb	*Scophthalmus rhombus*	IV, VIId
Kljunati okun	*Sebastes mentella*	IV
Morski list	*Solea solea*	IV
Morski list	*Solea solea*	VIId
Papalina	*Sprattus sprattus*	IV/VIId
Šur	*Trachurus trachurus*	IV, VIId
Rdeči krulec	*Trigla lucerna*	IV
Norveški molič	*Trisopterus esmarki*	IV
Kovač	*Zeus faber*	IV, VIId
Vsi komercialni morski psi, raže in skati [4]	*Selachii, Rajidae*	IV, VIId
Severovzhodni Atlantik in zahodni Rokavski preliv		
Bairdijeva gladkoglavka	*Alepocephalus bairdii*	VI, XII
Prava peščenka	*Ammodytidae*	VIa
Merjaščevka	*Capros aper*	V, VI, VII
Grebenasta pokrovača	*Pecten maximus*	IV, VI, VII
Kraljevska pokrovača	*Aequipecten opercularis*	VII
Morski pajek	*Maja squinado*	V, VI, VII
Jegulja	Anguilla anguilla	vsa območja
Morski meči	*Aphanopus spp.*	vsa območja
Srebrenke	*Argentina* spp.	vsa območja
Grba	*Argyrosomus regius*	vsa območja
Vzhodnoatlantski rdeči krulec	*Aspitrigla cuculus*	vsa območja
Sluzoglavke	*Beryx* spp.	vsa območja, razen X in IXa
Sluzoglavke	*Beryx* spp.	IXa in X

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES [1], IBSFC [2] ali FAO [3]), kjer se stalež nahaja/ oznaka staleža
Velika rakovica	*Cancer pagurus*	vsa območja
Sled	*Clupea harengus*	VIa/VIaN/ VIa S, VIIbc/VIIa/VIIj
Ugor	*Conger conger*	vsa območja, razen X
Ugor	*Conger conger*	X
Okroglonosi repak	*Centroscymnus coelolepis*	vsa območja
Temni morski pes	*Dalatias licha*	vsa območja
Morski bič	*Dasyatis pastinaca*	VII, VIII
Kljunati morski pes	*Deania calcea*	V, VI, VII, IX, X, XII
Brancin	*Dicentrarchus labrax*	vsa območja, razen IX
Brancin	*Dicentrarchus labrax*	IX
Klinasti list	*Dicologlossa cuneata*	VIIIc, IX
Sardon	*Engraulis encrasicolus*	IXa (samo Cadiz)
Sardon	*Engraulis encrasicolus*	VIII
Črni svetilec	*Etmopterus spinax*	VI, VII, VIII
Sivi krulec	*Eutrigla gurnardus*	VIId, e
Trska	*Gadus morhua*	Va/Vb/VIa/VIb/VIIa/VIIe–k
Sivi jezik	*Glyptocephalus cynoglossus*	VI, VII
Sinjeusti okun	*Helicolenus dactylopterus*	vsa območja
Jastog	*Homarus gammarus*	vsa območja
Oranžna sluzoglavka	*Hoplostethus atlanticus*	vsa območja
Morski meč	*Lepidopus caudatus*	IXa
Štiripegasti krilati romb	*Lepidorhombus boscii*	VIIIc, IXa
Krilati romb	*Lepidorhombus whiffiagonis*	VI/VII, VIIIabd/VIIIc, IXa
Limanda	*Limanda limanda*	VIIe/VIIa, f–h
Navadni ligenj	*Loligo vulgaris*	vsa območja, razen VIIIc, Ixa
Navadni ligenj	*Loligo vulgaris*	VIIIc, IXa

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES (1), IBSFC (2) ali FAO (3)), kjer se stalež nahaja/ oznaka staleža
Mala morska spaka	*Lophius budegassa*	IV, VI/VIIb–k, VIIIabd
Mala morska spaka	*Lophius budegassa*	VIIIc, IXa
Morska spaka	*Lophius piscatorius*	IV, VI/VIIb–k, VIIIabd
Morska spaka	*Lophius piscatorius*	VIIIc, IXa
Kapelan	*Mallotus villosus*	XIV
Vahnja	*Melanogrammus aeglefinus*	Va/Vb
Vahnja	*Melanogrammus aeglefinus*	VIa/VIb/VIIa/VIIb–k
Mol	*Merlangius merlangus*	VIII/IX, X
Mol	*Merlangius merlangus*	Vb/VIa/VIb/VIIa/VIIe–k
Oslič	*Merluccius merluccius*	IIIa, IV, VI, VII, VIIIab/VIIIc, IXa
Klinasti list	*Microchirus variegatus*	vsa območja
Sinji mol	*Micromesistius poutassou*	I–IX, XII, XIV
Rdeči jezik	*Microstomus kitt*	vsa območja
Modri leng	*Molva dypterygia*	vsa območja, razen X
Španski leng	*Molva macrophthalma*	X
Leng	*Molva molva*	vsa območja
Progasti bradač	*Mullus surmuletus*	vsa območja
Pegasti morski pes	*Mustelus asterias*	VI, VII, VIII, IX
Navadni morski pes	*Mustelus mustelus*	VI, VII, VIII, IX
Črnopikčasti morski pes	*Mustelus punctulatus*	VI, VII, VIII, IX
Škamp	*Nephrops norvegicus*	VI. funkcionalna enota
Škamp	*Nephrops norvegicus*	VII. Funkcionalna enota
Škamp	*Nephrops norvegicus*	VIII., IX. funkcionalna enota
Hobotnica	*Octopus vulgaris*	vsa območja, razen VIIIc, Ixa
Hobotnica	*Octopus vulgaris*	VIIIc, IXa

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES (1), IBSFC (2) ali FAO (3)), kjer se stalež nahaja/ oznaka staleža
Okati ribon	*Pagellus bogaraveo*	IXa, X
Hladnovodne kozice	*Pandalus* spp.	vsa območja
Dolgoostna rdeča kozica	*Parapenaeus longirostris*	IXa
Tabinja belica	*Phycis blennoides*	vsa območja
Tabinja	*Phycis phycis*	vsa območja
Morska plošča	*Pleuronectes platessa*	VIIa/VIIe/VIIfg
Morska plošča	*Pleuronectes platessa*	VIIbc/VIIh–k/VIII, IX, X
Polak	*Pollachius pollachius*	vsa območja, razen IX, X
Polak	*Pollachius pollachius*	IX, X
Saj	*Pollachius virens*	Va/Vb/IV, IIIa, VI
Saj	*Pollachius virens*	VII, VIII
Orjaška kirnja, brodolomčar	*Polyprion americanus*	X
Romb	*Psetta maxima*	vsa območja
Grenlandska morska plošča	*Reinhardtius hippoglossoides*	V, XIV/VI
Navadni jezik	*Hippoglossus hippoglossus*	V, XIV/VI
Atlantski losos	*Salmo salar*	vsa območja
Sardela	*Sardina pilchardus*	VIIIabd/VIIIc, IXa
Lokarda	*Scomber colias*	VIII, IX, X
Skuša	*Scomber scombrus*	II, IIIa, IV, V, VI, VII, VIII, IX
Gladki romb	*Scophthalmus rhombus*	vsa območja
Veliki rdeči okun	*Sebastes marinus*	podobmočja ICES V, VI, XII, XIV & NAFO SA 2 + (razd. 1F + 3K)
Kljunati okun	*Sebastes mentella*	podobmočja ICES V, VI, XII, XIV & NAFO SA 2 + (razd. 1F + 3K)
Sipa	*Sepia officinalis*	vsa območja
Morski list	*Solea solea*	VIIa/VIIfg
Morski list	*Solea solea*	VIIbc/VIIhjk/IXa/VIIIc

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES [1], IBSFC [2] ali FAO [3]), kjer se stalež nahaja/ oznaka staleža
Morski list	*Solea solea*	VIIe
Morski list	*Solea solea*	VIIIab
Okati riboni (v množini)	*Sparidae*	vsa območja
Sredozemski šur	*Trachurus mediterraneus*	VIII, IX
Pisani šur	*Trachurus picturatus*	VIII, IX, X
Šur	*Trachurus trachurus*	IIa, IVa, Vb, VIa, VIIa–c, e–k, VIIIabde/X
Šur	*Trachurus trachurus*	VIIIc, IXa
Moliči	*Trisopterus* spp.	vsa območja
Kovač	*Zeus faber*	vsa območja
Vsi komercialni morski psi, raže in skati [4]	*Selachii, Rajidae*	IV, VIId
Sredozemsko morje in Črno morje		
Jegulja	*Anguilla anguilla*	vsa območja v Sredozemskem morju
Orjaška rdeča kozica	*Aristeomorpha foliacea*	vsa območja v Sredozemskem morju
Rdeč-modra kozica	*Aristeus antennatus*	vsa območja v Sredozemskem morju
Bukva	*Boops boops*	1.3, 2.1, 2.2, 3.1, 3.2
Delfinka	*Coryphaena equiselis*	vsa območja v Sredozemskem morju
Delfinka	*Coryphaena hippurus*	vsa območja v Sredozemskem morju
Brancin	*Dicentrarchus labrax*	vsa območja v Sredozemskem morju
Kodrasta hobotnica	*Eledone cirrhosa*	1.1, 1.3, 2.1, 2.2, 3.1
Moškatna hobotnica	*Eledone moschata*	1.3, 2.1, 2.2, 3.1
Sardon	*Engraulis encrasicolus*	vsa območja v Sredozemskem morju
Sardon	*Engraulis encrasicolus*	Črno morje GSA 29
Sivi krulec	*Eutrigla gurnardus*	2.2, 3.1
Ligenj	*Illex* spp., *Todarodes* spp.	vsa območja v Sredozemskem morju
Pahljačasta mečarica	*Istiophoridae*	vsa območja v Sredozemskem morju

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES [1], IBSFC [2] ali FAO [3]), kjer se stalež nahaja/ oznaka staleža
Navadni ligenj	*Loligo vulgaris*	vsa območja v Sredozemskem morju
Mala morska spaka	*Lophius budegassa*	1.1, 1.2, 1.3, 2.2, 3.1
Morska spaka	*Lophius piscatorius*	1.1, 1.2, 1.3, 2.2, 3.1
Mol	*Merlangius merlangus*	Črno morje GSA 29
Oslič	*Merluccius merluccius*	vsa območja v Sredozemskem morju
Sinji mol	*Micromesistius poutassou*	1.1, 3.1
Ciplji	*Mugilidae*	1.3, 2.1, 2.2, 3.1
Bradač	*Mullus barbatus*	vsa območja v Sredozemskem morju
Bradač	*Mullus barbatus*	Črno morje GSA 29
Progasti bradač	*Mullus surmuletus*	vsa območja v Sredozemskem morju
Hobotnica	*Octopus vulgaris*	vsa območja v Sredozemskem morju
Škamp	*Nephrops norvegicus*	vsa območja v Sredozemskem morju
Ribon	*Pagellus erythrinus*	vsa območja v Sredozemskem morju
Dolgoostna rdeča kozica	*Parapenaeus longirostris*	vsa območja v Sredozemskem morju
Tigrasta kozica	*Penaeus kerathurus*	3.1
Romb	*Psetta maxima*	Črno morje GSA 29
Sardela	*Sardina pilchardus*	vsa območja v Sredozemskem morju
Skuša	*Scomber* spp.	vsa območja v Sredozemskem morju
Sipa	*Sepia officinalis*	vsa območja v Sredozemskem morju
Morski list	*Solea vulgaris*	1.2, 2.1, 3.1
Orada, zlatobrov	*Sparus aurata*	1.2, 3.1
Girica	*Spicara smaris*	2.1, 3.1, 3.2
Papalina	*Sprattus sprattus*	Črno morje GSA 29
Morska bogomolka	*Squilla mantis*	1.3, 2.1, 2.2
Sredozemski šur	*Trachurus mediterraneus*	vsa območja v Sredozemskem morju

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območje (oznaka območja po ICES (1), IBSFC (2) ali FAO (3)), kjer se stalež nahaja/ oznaka staleža
Sredozemski šur	*Trachurus mediterraneus*	Črno morje GSA 29
Šur	*Trachurus trachurus*	vsa območja v Sredozemskem morju
Šur	*Trachurus trachurus*	Črno morje GSA 29
Rdeči krulec	*Trigla lucerna*	1.3, 2.2, 3.1
Školjka	*Veneridae*	2.1, 2.2
Beli glavač	*Aphia minuta*	GSA 9,10,16 in 19
Gavuni	*Atherina spp*	GSA 9,10,16 in 19
Molič	*Trisopterusminutus*	vse regije
Vsi komercialni morski psi, raže in skati (4)	*Selachii, Rajidae*	vse regije

(1) Mednarodni svet za raziskovanje morja.
(2) Mednarodna komisija za ribištvo v Baltskem morju.
(3) Organizacija Združenih narodov za prehrano in kmetijstvo.
(4) Poročati na ravni vrste.

BIOLOŠKI PODATKI

Tabela 1B

Staleži najbolj oddaljenih regij Unije

Vrsta (domače ime)	Vrsta (znanstveno ime)
Francoska Gvajana	
Južni rdeči hlastač	*Lutjanus purpureus*
Kozice	*Farfantepenaeus subtilis*
„Acoupa weakfish“	*Cynoscion acoupa*
„Smalltooth weakfish“	*Cynoscion steindachneri*
„Green weakfish“	*Cynoscion virescens*
Morski somi	*Ariidae*
„Tripletail“	*Lobotes surinamensis*
„Torroto grunt“	*Genyatremus luteus*
„Snooks“	*Centropomus spp.*

Vrsta (domače ime)	Vrsta (znanstveno ime)
Kirnje	*Serranidae*
Ciplji	*Mugil spp.*
Guadeloupe in Martinique	
Hlastači	*Lutjanidae*
Prašičevke	*Haemulidae*
Kirnje	*Serranidae*
Velika plamenka	*Pterois volitans*
Tunom podobne ribe	*Scombridae*
Sinja jadrovnica	*Makaira nigricans*
Delfinka	*Coryphaena hippurus*
Otok Réunion in Mayotte	
Hlastači	*Lutjanidae*
Kirnje	*Serranidae*
Tunom podobne ribe	*Scombridae*
Mečarica	*Xiphias gladius*
Druge pahljačaste mečarice	*Istiophoridae*
Delfinka	*Coryphaena hippurus*
Okati šur	*Selar crumenophthalmus*
Azori, Madeira in Kanarski otoki	
Lokarda	*Scomber colias*
Velika sardela	*Sardinella maderensis*
Šur	*Trachurus spp.*
Sardela	*Sardina pilchardus*
Morska papiga	*Sparisoma cretense*
Latvice	*Patellidae*

BIOLOŠKI PODATKI

Tabela 1C

Staleži v morskih regijah v okviru regionalnih organizacij za upravljanje ribištva (RFMO) in sporazumov o partnerstvu o trajnostnem ribištvu (SFPA)

IATTC (Medameriška komisija za tropske tune)

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Geografsko območje	Prioriteta	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa mora biti pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Thunnus albacares	rumenoplavuti tun	vzhodni Pacifik	visoka	
Thunnus obesus	veleoki tun	vzhodni Pacifik	visoka	
Katsuwonus pelamis	črtasti tun	vzhodni Pacifik	visoka	
Thunnus alalunga	beli tun	vzhodni Pacifik	visoka	
Thunnus orientalis	pacifiški modroplavuti tun	vzhodni Pacifik	visoka	
Xiphias gladius	mečarica	vzhodni Pacifik	visoka	
Makaira nigricans (ali mazara)	sinja jadrovnica	vzhodni Pacifik	visoka	
Makaira indica	indijska jadrovnica	vzhodni Pacifik	visoka	
Tetrapturus audax	progasta jadrovnica	vzhodni Pacifik	visoka	

ICCAT (Mednarodna komisija za ohranitev tunov v Atlantiku)

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Geografsko območje	Prioriteta	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa mora biti pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Thunnus albacares	rumenoplavuti tun	Atlantski ocean in sosednja morja	visoka	
Thunnus obesus	veleoki tun	Atlantski ocean in sosednja morja	visoka	
Katsuwonus pelamis	črtasti tun	Atlantski ocean in sosednja morja	visoka	
Thunnus alalunga	beli tun	Atlantski ocean in sosednja morja	visoka	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Thunnus thynnus	tun	Atlantski ocean in sosednja morja	visoka	
Xiphias gladius	mečarica	Atlantski ocean in sosednja morja	visoka	
Makaira nigricans (ali mazara)	sinja jadrovnica	Atlantski ocean in sosednja morja	visoka	
Istiophorus albicans	atlantska pahljačasta mečarica	Atlantski ocean in sosednja morja	visoka	
Tetrapturus albidus	bela jadrovnica	Atlantski ocean in sosednja morja	visoka	
Prionace glauca	sinji morski pes	Atlantski ocean in sosednja morja	visoka	
Auxis rochei	trupec	Atlantski ocean in sosednja morja	visoka	
Sarda sarda	palamida	Atlantski ocean in sosednja morja	visoka	
Euthynnus alletteratus	pegasti tun	Atlantski ocean in sosednja morja	srednja	
Thunnus atlanticus	črnoplavuti tun	Atlantski ocean in sosednja morja	srednja	
Orcynopsis unicolor	bela palamida	Atlantski ocean in sosednja morja	srednja	
Scomberomorus brasiliensis	„Serra Spanish mackerel“	Atlantski ocean in sosednja morja	srednja	
Scomberomorus regalis	karibska kraljeva skuša	Atlantski ocean in sosednja morja	srednja	
Auxis thazard	fregatni trupec	Atlantski ocean in sosednja morja	srednja	
Scomberomorus cavalla	kraljevska skuša	Atlantski ocean in sosednja morja	srednja	
Scomberomorus tritor	zahodnoafriška kraljevska skuša	Atlantski ocean in sosednja morja	srednja	
Scomberomorus maculatus	lisasta kraljevska skuša	Atlantski ocean in sosednja morja	srednja	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Acanthocybium solandri	vahu	Atlantski ocean in sosednja morja	srednja	
Coryphaena hippurus	delfinka	Atlantski ocean in sosednja morja	srednja	

NAFO (Organizacija za ribištvo severozahodnega Atlantika)

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Staleži, kot jih je opredelila regionalna organizacija za upravljanje ribištva	Prioriteta	
Gadus morhua	trska	NAFO 2J 3KL	nizka	
Gadus morhua	trska	NAFO 3M	visoka	
Gadus morhua	trska	NAFO 3NO	visoka	
Gadus morhua	trska	NAFO 3Ps	visoka	
Gadus morhua	trska	NAFO SA1	visoka	
Glyptocephalus cynoglossus	sivi jezik	NAFO 3NO	visoka	
Glyptocephalus cynoglossus	sivi jezik	NAFO 2J3KL	nizka	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa mora biti pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Hippoglossoides platessoides	ameriška morska plošča	NAFO 3LNO	visoka	
Hippoglossoides platessoides	ameriška morska plošča	NAFO 3M	visoka	
Limanda ferruginea	rumenorepa limanda	NAFO 3LNO	srednja	
Coryphaenoides rupestris	okroglonosi repak	NAFO SA0 + 1	nizka	
Macrourus berglax	čebulastooki repak	NAFO SA2 + 3	visoka	
Pandalus borealis	severna kozica	NAFO 3LNO	visoka	
Pandalus borealis	severna kozica	NAFO 3M	visoka	
Amblyraja radiata	žarkasta raža	NAFO 3LNOPs	visoka	
Reinhardtius hippoglossoides	grenlandska morska plošča	NAFO 3KLMNO	visoka	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Reinhardtius hippoglossoides	grenlandska morska plošča	NAFO SA1	visoka	
Hippoglossus hippoglossus	navadni jezik	NAFO SA1	nizka	
Sebastes mentella	kljunati okun	NAFO SA1	visoka	
Sebastes spp.	rdeči okuni	NAFO 3LN	visoka	
Sebastes spp.	rdeči okuni	NAFO 3M	visoka	
Sebastes spp.	rdeči okuni	NAFO 3O	visoka	
Urophycis tenuis	bela repata tabinja	NAFO 3NO	visoka	
Mallotus villosus	kapelan	NAFO 3NO	visoka	
Beryx sp.	sluzoglavke	NAFO 6G	visoka	
Illex illecebrosus	severni kratkoplavuti ligenj	podobmočji NAFO 3 + 4	nizka	
Salmo salar	atlantski losos	NAFO S1 + podobmočje ICES XIV, NEAF, NASCO	visoka	

Morsko območje 34 FAO – Odbor za ribištvo za vzhodni srednji Atlantik (CECAF)

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Geografsko območje	Prioriteta	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa je pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Brachydeuterus spp.	prašičevke	34.1.3, 34.3.1, 34.3.3–6	visoka	
Caranx spp.	trnoboki	34.3.1, 34.3.3–6	visoka	
Cynoglossus spp.	pasji jeziki	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Decapterus spp.	šuri	34.3.1, 34.3.3–6	visoka	
Dentex canariensis	kanarski zobatec	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	srednja	
Dentex congoensis	kongoški zobatec	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	srednja	
Dentex macrophthalmus	veleoki zobatec	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Dentex maroccanus	maroški zobatec	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	srednja	
Dentex spp.	zobatci	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Engraulis encrasicolus	sardon	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Epinephelus aeneus	bela kirnja	34.1.3, 34.3.1, 34.3.3–6	visoka	
Ethmalosa fimbriata	bonga	34.3.1, 34.3.3–6	visoka	
Farfantepenaeus notialis	južna rožnata kozica	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Galeoides decadactylus	nitkarica	34.1.3, 34.3.1, 34.3.3–6	visoka	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa je pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Loligo vulgaris	ligenj	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Merluccius polli	benguelski oslič	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Merluccius senegalensis	senegalski oslič	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Merluccius spp.	drugi osliči	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	srednja	
Octopus vulgaris	hobotnica	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Pagellus acarne	divji ribon	34.1.1	visoka	
Pagellus bellottii	rdeči ribon	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Pagellus bogaraveo	okati ribon	34.1.1	srednja	
Pagellus spp.	riboni	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Pagrus caeruleostictus	modropikasti pagar	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Parapenaeus longirostris	dolgoostna rdeča kozica	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Pomadasys incisus	„Bastard grunt“	34.1.1	srednja	
Pomadasys spp.	prašičevke	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Pseudotolithus spp.	„West African croakers“	34.1.1	visoka	
Sardina pilchardus	sardela	34.1.1, 34.1.3	visoka	
Sardinella aurita	velika sardela	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Sardinella maderensis	madeirska velika sardela	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa je pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Scomber japonicus	lokarda	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Scomber spp.	druge skuše	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Sepia hierredda	„Cuttlefish“	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Sepia officinalis	sipa	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Sepia spp.	sipe	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	srednja	
Sparidae	špari	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Sparus spp.	špari	34.1.1	visoka	
Trachurus trachurus	šur	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Trachurus trecae	afriški šur	34.1.1, 34.1.3, 34.3.1, 34.3.3–6	visoka	
Umbrina canariensis	kanarski korbel	34.3.3–6	srednja	

SEAFO (Organizacija za ribištvo jugovzhodnega Atlantika)

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Geografsko območje	Prioriteta	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa je pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Dissostichus eleginoides	patagonska zobata riba	jugovzhodni Atlantik	*visoka*	
Beryx spp.	sluzoglavke	jugovzhodni Atlantik	*visoka*	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Chaceon spp.	rdeče rakovice	jugovzhodni Atlantik	*visoka*	
Pseudopentaceros richardsoni	pelagična oklepnoglavka	jugovzhodni Atlantik	*visoka*	
Helicolenus spp.	okuni	jugovzhodni Atlantik	*visoka*	
Hoplostethus atlanticus	oranžna sluzoglavka	jugovzhodni Atlantik	*visoka*	
Trachurus spp.	šuri	jugovzhodni Atlantik	*visoka*	
Scomber spp	skuše	jugovzhodni Atlantik	*visoka*	
Polyprion americanus	orjaška kirnja, brodolomčar	jugovzhodni Atlantik	*srednja*	
Jasus tristani	tristanski rarog	jugovzhodni Atlantik	*srednja*	
Lepidopus caudatus	morski meč	jugovzhodni Atlantik	*srednja*	
Schedophilus ovalis	„Imperial Blackfish“	jugovzhodni Atlantik	*nizka*	
Schedophilus velaini	„Violet warehou“	jugovzhodni Atlantik	*nizka*	
Allocyttus verrucossus	„Oreo dories“	jugovzhodni Atlantik	*nizka*	
Neocyttus romboidales		jugovzhodni Atlantik		
Allocyttus guineensis		jugovzhodni Atlantik		
Pseudocyttu smaculatus		jugovzhodni Atlantik		
Emmelichthys nitidus	kapska rubinka	jugovzhodni Atlantik	*nizka*	
Ruvettus pretiosus	raskavka	jugovzhodni Atlantik	*nizka*	
Promethichthys prometheus	„Roudi escolar“	jugovzhodni Atlantik	*nizka*	
Macrourus spp.	repaki	jugovzhodni Atlantik	*nizka*	
Antimora rostrata	sinja antimora	jugovzhodni Atlantik	*nizka*	
Epigonus spp.	globokomorski kraljički	jugovzhodni Atlantik	*nizka*	
Merluccius spp.	osliči	jugovzhodni Atlantik	*nizka*	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Notopogon fernandezianus	„Orange bellowfish“	jugovzhodni Atlantik	*nizka*	
Octopodidae in Loliginidae	hobotnice in lignji	jugovzhodni Atlantik	*nizka*	

WCPFC (Komisija za ribištvo zahodnega in srednjega Pacifika)

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Geografsko območje	Prioriteta	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa je pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Thunnus albacares	rumenoplavuti tun	zahodni srednji Pacifik	visoka	
Thunnus obesus	veleoki tun	zahodni srednji Pacifik	visoka	
Katsuwonus pelamis	črtasti tun	zahodni srednji Pacifik	visoka	
Thunnus alalunga	beli tun	zahodni srednji Pacifik	visoka	
Thunnus orientalis	pacifiški modroplavuti tun	zahodni srednji Pacifik	visoka	
Xiphias gladius	mečarica	zahodni srednji Pacifik	visoka	
Makaira nigricans (ali mazara)	sinja jadrovnica	zahodni srednji Pacifik	visoka	
Makaira indica	indijska jadrovnica	zahodni srednji Pacifik	visoka	
Tetrapturus audax	progasta jadrovnica	zahodni srednji Pacifik	visoka	
Acanthocybium solandri	vahu	zahodni srednji Pacifik	srednja	
Coryphaena hippurus	delfinka	zahodni srednji Pacifik	srednja	
Elagatis bipinnulata	mavrični šur	zahodni srednji Pacifik	srednja	
Lepidocybium flavobrunneum	„Escolar“	zahodni srednji Pacifik	srednja	
Lampris regius	svetlica	zahodni srednji Pacifik	srednja	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Mola mola	morski mesec	zahodni srednji Pacifik	srednja	
Istiophorus platypterus	pacifiška pahljačasta mečarica	zahodni srednji Pacifik	srednja	
Tetrapturus angustirostris	kratkokljuna jadrovnica	zahodni srednji Pacifik	srednja	
Ruvettus pretiosus	raskavka	zahodni srednji Pacifik	srednja	
Prionace glauca	sinji morski pes	zahodni srednji Pacifik	visoka	
Carcharhinus longimanus	dolgoplavuti morski pes	zahodni srednji Pacifik	visoka	
Carcharhinus falciformis	svilnati morski pes	zahodni srednji Pacifik	visoka	
Alopias superciliosus	velikooka morska lisica	zahodni srednji Pacifik	visoka	
Alopias vulpinus	morska lisica	zahodni srednji Pacifik	visoka	
Alopias pelagicus	„Pelagic thresher“	zahodni srednji Pacifik	visoka	

OPOMBA: Za WCPF se dodajo naslednje zahteve glede poročanja za plovila s parangali:

(1) Število stranskih vrvic med plovci. Število stranskih vrvic med plovci se poroča za vsak sklop ribolovnih operacij.

(2) Število ujetih rib po posameznem sklopu ribolovnih operacij, za naslednje vrste rib: beli tun (Thunnus alalunga), veleoki tun (Thunnus obesus), črtasti tun (Katsuwonus pelamis), rumenoplavuti tun (Thunnus albacares), progasta jadrovnica (Tetrapturus audax), tihomorska jadrovnica (Makaira mazara), indijska jadrovnica (Makaira indica) in mečarica (Xiphias gladius), sinji morski pes, svilnati morski pes, dolgoplavuti morski pes, maki, morske lisice, atlantski morski pes (južno od 20°S, dokler biološki podatki kažejo, da je primerna ta ali druga geografska meja), kladvenice (vrste Eusphyra blochii, valovitoglava kladvenica, vrste Sphyrna mokarran in vrste Sphyrna zygaena), orjaški kitovec in druge vrste, kot jih je določila Komisija.

Če je bila zabeležena skupna teža ali povprečna teža ulovljenih rib na posamezen sklop ribolovnih operacij, potem se tudi poroča o skupni teži ali povprečni teži ulovljenih rib na posamezen sklop ribolovnih operacij po posameznih vrstah. Če skupna teža ali povprečna teža ulovljenih rib na posamezen sklop ribolovnih operacij ni bila zabeležena, potem se oceni skupna teža ali povprečna teža ulovljenih rib na posamezen sklop ribolovnih operacij po posameznih vrstah ter se poroča o teh ocenah. Skupna teža ali povprečna teža se nanaša na celotno težo in ne na predelano težo.

WECAFC (Komisija za ribištvo v zahodnem srednjem Atlantiku)

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Geografsko območje	Prioriteta	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa je pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Panulirus argus	karibski rarog	zahodni srednji Atlantik	visoka	
Strombus gigas	„Queen Conch“	zahodni srednji Atlantik	visoka	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Morskim psom podobni Selachii, Rajidae	morski psi, raže in skati	zahodni srednji Atlantik	visoka	
Coryphaena hippurus	delfinka	zahodni srednji Atlantik	visoka	
Acanthocybium solandri	vahu	zahodni srednji Atlantik	visoka	
Epinephelus guttatus	„Red Hind“	zahodni srednji Atlantik	visoka	
Lutjanus vivanus	„Silk snapper“	zahodni srednji Atlantik	visoka	
Lutjanus buccanella	„Blackfin snapper“	zahodni srednji Atlantik	visoka	
Lutjanus campechanus	„Red snapper“	zahodni srednji Atlantik	visoka	
Penaeus subtilis	južna rjava kozica	Francoska Gvajana (izključna ekonomska cona – IEC)	visoka	

IOTC (Komisija za tune v Indijskem oceanu)

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Geografsko območje	Prioriteta	
Thunnus albacares	rumenoplavuti tun	zahodni in vzhodni Indijski ocean	visoka	
Thunnus obesus	veleoki tun	zahodni in vzhodni Indijski ocean	visoka	
Katsuwonus pelamis	črtasti tun	zahodni in vzhodni Indijski ocean	visoka	
Thunnus alalunga	beli tun	zahodni in vzhodni Indijski ocean	visoka	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa je pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Xiphias gladius	mečarica	zahodni in vzhodni Indijski ocean	visoka	
Makaira nigricans (ali mazara)	sinja jadrovnica	zahodni in vzhodni Indijski ocean	visoka	
Makaira indica	indijska jadrovnica	zahodni in vzhodni Indijski ocean	visoka	
Tetrapturus audax	progasta jadrovnica	zahodni in vzhodni Indijski ocean	visoka	
Istiophorus platypterus	pacifiška pahljačasta mečarica	zahodni in vzhodni Indijski ocean	visoka	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III te priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Auxis rochei	trupec	zahodni in vzhodni Indijski ocean	srednja	
Auxis thazard	fregatni trupec	zahodni in vzhodni Indijski ocean	srednja	
Euthynnus affinis	vzhodni pegasti tun	zahodni in vzhodni Indijski ocean	srednja	
Thunnus tonggol	dolgorepi tun	zahodni in vzhodni Indijski ocean	srednja	
Scomberomorus guttatus	indopacifiška kraljevska skuša	zahodni in vzhodni Indijski ocean	srednja	
Scomberomorus commerson	progasta kraljevska skuša	zahodni in vzhodni Indijski ocean	srednja	
Prionace glauca	sinji morski pes	zahodni in vzhodni Indijski ocean	visoka	
Alopias superciliosus	velikooka morska lisica	zahodni in vzhodni Indijski ocean	visoka	
Carcharhinus falciformis	svilnati morski pes	zahodni in vzhodni Indijski ocean	visoka	
Carcharhinus longimanus	dolgoplavuti morski pes	zahodni in vzhodni Indijski ocean	visoka	
Alopias pelagicus	„Pelagic thresher shark“	zahodni in vzhodni Indijski ocean	visoka	
Sphyrna lewini	valovitoglava kladvenica	zahodni in vzhodni Indijski ocean	visoka	

Druge regionalne organizacije za upravljanje ribištva

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Znanstveno ime	Splošno ime	Geografsko območje	Prioriteta	Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa je pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.
Trachurus murphyi	„Jack mackerel“	območje Konvencije SPRFMO	visoka	
Euphausia superba	kril	območje Konvencije CCAMLR	visoka	

VRSTE Pri pripravi načrtov vzorčenja za zbiranje bioloških podatkov, kot je določeno v poglavju III priloge, se upoštevajo meje staležev, kot so jih določile pristojne regionalne organizacije za upravljanje ribištva ali regionalne ribiške organizacije, za vsak stalež pa se dodeli ustrezen napor vzorčenja.				Pogostost zbiranja bioloških spremenljivk
Dissostichus spp. *Dissostichus eleginoides in Dissostichus mawsoni*	zobate ribe	območje Konvencije CCAMLR	visoka	
Champsocephalus gunnari	antarktična ledna krokodilka	območje Konvencije CCAMLR	nizka	
Viri rib, mehkužcev, rakov in drugih sedentarnih vrst na območju pristojnosti, toda brez: (i) sedentarnih vrst, za katere velja ribolovna pristojnost obalnih držav v skladu s členom 77(4) Konvencije Združenih narodov o pomorskem mednarodnem pravu iz leta 1982, in (ii) izrazito selivskih vrst iz Priloge I h Konvenciji Združenih narodov o pomorskem mednarodnem pravu iz leta 1982.		območje Konvencije SIOFA		

BIOLOŠKI PODATKI

Tabela 1D

Vrste, ki se spremljajo v okviru programov za zaščito v Uniji ali v okviru mednarodnih obveznosti

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Ribe kostnice	Prave kostnice		
Jesetri	Acipenser spp.	Sredozemsko morje in Črno morje; Baltsko morje; OSPAR II, IV	Priloga II k Barcelonski konvenciji ([1]), Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol); OSPAR ([2]); HELCOM ([3])
Gladkoglavke	*Alepocephalidae*	vse regije	relevantno za globokomorski ribolov ([4])
Bairdijeva gladkoglavka	*Alepocephalus bairdii*	vse regije	relevantno za globokomorski ribolov
Rissojeva gladkoglavka	*Alepocephalus rostratus*	vse regije	relevantno za globokomorski ribolov
Črnomorska čepa	*Alosa immaculata*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Atlantska čepa	*Alosa alosa*	OSPAR II, III, IV	OSPAR
Ozimica	*Coregonus lavaretus*	OSPAR II	OSPAR
Trska	*Gadus morhua*	OSPAR II, III; Baltsko morje	OSPAR; HELCOM

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Dolgonosi morski konjiček	*Hippocampus guttulatus* (sinonim: *Hippocampus ramulosus*)	OSPAR II, III, IV, V	OSPAR
Kratkonosi morski konjiček	*Hippocampus hippocampus*	OSPAR II, III, IV, V	OSPAR
„Black Sea shad“	*Alosa tanaica*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Sinja antimora	*Antimora rostrata*	vse regije	relevantno za globokomorski ribolov
Črni morski meč	*Aphanopus carbo*	vse regije	relevantno za globokomorski ribolov
„Scabbardfish“	*Aphanopus intermedius*	vse regije	relevantno za globokomorski ribolov
Sladkovodni raki	*Astacus spp.*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
„Big-scale sand smelt“	*Atherina pontica*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Iglica	*Belone belone euxini Günther*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Sluzoglavke	*Beryx spp.*	vse regije	relevantno za globokomorski ribolov
„Brotula“	*Cataetyx laticeps*	vse regije	relevantno za globokomorski ribolov
Mala ozimica	*Coregonus albula*	Baltsko morje	Priporočilo z regionalnega usklajevalnega sestanka za Baltik
Bradavičarica, morski zajec	*Cyclopterus lumpus*	vse regije	relevantno za globokomorski ribolov
Špar	*Diplodus annularis*	Sredozemsko morje	Uredba Sveta (ES) št. 1967/2006 ([5]) (najmanjša velikost ohranjanja)
Pic	*Diplodus puntazzo*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Šarg	*Diplodus sargus*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Fratrc	*Diplodus vulgaris*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Patagonska zobata riba	*Dissostichus eleginoides*	vse regije	relevantno za globokomorski ribolov
Antarktična zobata riba	*Dissostichus mawsoni*	vse regije	relevantno za globokomorski ribolov

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Kirnje	*Epinephelus spp.*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Veleoki globokomorski kraljiček	*Epigonus telescopus*	vse regije	ranljiva vrsta; relevantno za globokomorski ribolov
Glavači	*Gobiidae*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Okun	*Helicolenus dactylopterus*	vse regije	relevantno za globokomorski ribolov
Navadni jezik	*Hippoglossus hippoglossus*	vse regije	relevantno za globokomorski ribolov
Oranžna sluzoglavka	*Hoplostethus atlanticus*	vse regije; OSPAR I, V	ranljiva vrsta; relevantno za globokomorski ribolov
Sredozemska sluzoglavka	*Hoplostethus mediterraneus*	vse regije	relevantno za globokomorski ribolov
Morski meč	*Lepidopus caudatus*	vse regije	relevantno za globokomorski ribolov
Ovčica	*Lithognathus mormyrus*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Zlati cipelj	*Liza aurata*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Dolgonosi cipelj	*Liza saliens*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Esmarkova ogorčica	*Lycodes esmarkii*	vse regije	relevantno za globokomorski ribolov
Repaki, razen okroglonosega repaka in čebulastookega repaka	*Macrouridae, razen Coryphaenoides rupestris in Macrourus berglax*	vse regije	relevantno za globokomorski ribolov
Čebulastooki repak	*Macrourus berglax*	vse regije	relevantno za globokomorski ribolov
Mol	*Merlangius merlangus*	Baltsko morje in Črno morje	Priporočilo z regionalnega usklajevalnega sestanka za Baltik; Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Jegulja	*Anguilla anguilla*	OSPAR I, II, III, IV; Baltsko morje	OSPAR; HELCOM
Atlantski losos	**Salmo salar*	OSPAR I, II, III, IV; Baltsko morje	OSPAR; HELCOM
Tun	**Thunnus thynnus*	OSPAR V	OSPAR; HELCOM

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Modri leng	*Molva dypterygia*	vse regije	relevantno za globokomorski ribolov
Globokomorska trska	*Mora moro*	vse regije	relevantno za globokomorski ribolov
Ciplji	*Mugil spp.*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
„Black gemfish“	*Nesiarchus nasutus*	vse regije	relevantno za globokomorski ribolov
„Snubnosed spiny eel“	*Notacanthus chemnitzii*	vse regije	relevantno za globokomorski ribolov
Evropski snetec	*Osmerus eperlanus*	Baltsko morje	Priporočilo z regionalnega usklajevalnega sestanka za Baltik; HELCOM
Divji ribon	*Pagellus acarne*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Okati ribon	*Pagellus bogaraveo*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Pagar	*Pagrus pagrus*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Orjaška kirnja, brodolomčar	*Polyprion americanus*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Orjaška kirnja, brodolomčar	*Polyprion americanus*	vse regije	relevantno za globokomorski ribolov
Skakavka	*Pomatomus saltatrix*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Rdeči okun	*Sebastes viviparus*	vse regije	relevantno za globokomorski ribolov
Beluga	*Huso huso*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Hrapavi okun	*Trachyscorpia cristulata*	vse regije	relevantno za globokomorski ribolov
Kostanjevka	*Brama spp.*	GSA 1.1, 1.2, 1.3 in GSA za Črno morje 29	Priloga VIII k Uredbi Sveta (ES) št. 894/97 ([6])
Lokarda	*Scomber colias Gmelin*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Kristalni glavač	*Crystallogobius linearis*	Črno morje	nacionalni načrti upravljanja
Morska podgana	*Chimaera monstrosa*	Baltsko morje	HELCOM

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
atlantska čepa	*Alosa alosa*	Baltsko morje	HELCOM
Čepa	*Alosa fallax*	Baltsko morje	HELCOM
Atlantski sled	*Clupea harengus subsp.*	Baltsko morje	HELCOM
Kosalj	*Abramis ballerus*	Baltsko morje	HELCOM
Zelenika	*Alburnus alburnus*	Baltsko morje	HELCOM
Bolen	*Aspius aspius*	Baltsko morje	HELCOM
Mrena	*Barbus barbus*	Baltsko morje	HELCOM
Globoček	*Gobio gobio*	Baltsko morje	HELCOM
Sabljevec	*Pelecus cultratus*	Baltsko morje	HELCOM
Pisanec	*Phoxinus phoxinus*	Baltsko morje	HELCOM
Ogrica	*Vimba vimba*	Baltsko morje	HELCOM
Nežica	*Cobitis taenia*	Baltsko morje	HELCOM
Morska postrv	*Salmo trutta*	Baltsko morje	HELCOM
Mala ozimica	*Coregonus albula*	Baltsko morje	HELCOM
„Baltic houting“	*Coregonus balticus, sinonim: Coregonus lavaretus, selitvena vrsta*	Baltsko morje	HELCOM
Maraena	*Coregonus maraena, sinonim: Coregonus lavaretus, vrsta, ki ni selitvena*	Baltsko morje	HELCOM
„Pallas's houting“	*Coregonus pallasii*	Baltsko morje	HELCOM
Evropski snetec	*Osmerus eperlanomarinus*	Baltsko morje	HELCOM
Mala morska spaka	*Lophius budegassa*	Baltsko morje	HELCOM
„Sea stickleback“	*Spinachia spinachia*	Baltsko morje	HELCOM
„Snake pipefish“	*Entelurus aequoreus*	Baltsko morje	HELCOM
Kačje šilo	*Nerophis ophidion*	Baltsko morje	HELCOM
„Worm pipefish“	*Nerophis lumbriciformis*	Baltsko morje	HELCOM

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Veliko šilo	*Syngnathus acus*	Baltsko morje	HELCOM
Ploskonoso šilo	*Syngnathus typhle*	Baltsko morje	HELCOM
Okroglonosi repak	*Centroscymnus coelolepis*	Baltsko morje	HELCOM
Vahnja	*Melanogrammus aeglefinus*	Baltsko morje	HELCOM
Polak	*Pollachius pollachius*	Baltsko morje	HELCOM
Leng	*Molva molva*	Baltsko morje	HELCOM
„Snakeblenny“	*Lumpenus lampretaeformis*	Baltsko morje	HELCOM
Veliki rdeči okun	*Sebastes marinus*	Baltsko morje	HELCOM
Rdeči okun	*Sebastes viviparus*	Baltsko morje	HELCOM
Kapelj	*Cottus gobio*	Baltsko morje	HELCOM
„Alpine bullhead“	*Cottus poecilopus*	Baltsko morje	HELCOM
„Shorthorn sculpin“	*Myoxocephalus scorpius*	Baltsko morje	HELCOM
„Longspined bullhead“	*Taurulus bubalis*	Baltsko morje	HELCOM
„Fourhorn sculpin“	*Triglopsis quadricornis*	Baltsko morje	HELCOM
Bradavičarica	*Cyclopterus lumpus*	Baltsko morje	HELCOM
„Striped seasnail“	*Liparis liparis*	Baltsko morje	HELCOM
„Montagu's seasnail“	*Liparis montagui*	Baltsko morje	HELCOM
Kovač	*Zeus faber*	Baltsko morje	HELCOM
Brancin	*Dicentrarchus labrax*	Baltsko morje	HELCOM
Pegasta ustnača	*Labrus bergylta*	Baltsko morje	HELCOM
Smokva	*Labrus mixtus*	Baltsko morje	HELCOM
„Corkwring wrasse“	*Symphodus melops*	Baltsko morje	HELCOM
Morski zmaj	*Trachinus draco*	Baltsko morje	HELCOM

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Ostrigar	*Anarhichas lupus*	Baltsko morje	HELCOM
„Lesser sandeel“	*Ammodytes marinus*	Baltsko morje	HELCOM
Mala peščenka	*Ammodytes tobianus*	Baltsko morje	HELCOM
„Painted goby“	*Pomatoschistus pictus*	Baltsko morje	HELCOM
Trupec	*Auxis rochei*	Baltsko morje	HELCOM
Pegasti tun	*Euthynnus alleteratus*	Baltsko morje	HELCOM
Bela palamida	*Orcynopsis unicolor*	Baltsko morje	HELCOM
Skuša	*Scomber scombrus*	Baltsko morje	HELCOM
Navadni jezik	*Hippoglossus hippoglossus*	Baltsko morje	HELCOM
Mečarica	*Xiphias gladius*	Baltsko morje	HELCOM
Črnuh	*Centrolophus niger*	Baltsko morje	HELCOM
Hrustančnice	Chondrichthyes		
„Narrow sawfish“	*Anoxypristis cuspidata*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Kljunati morski pes	*Deania calcea*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Gladki svetilec	*Etmopterus pusillus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Dwarf sawfish“	*Pristis clavata*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Green sawfish“	*Pristis zijsron*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Norveška kljunata raža	*Raja (Dipturus) nidarosiensis*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Raža trnjevka	*Raja clavata*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; OSPAR; HELCOM
Valovito progasta raža	*Raja undulata*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Pelaška morska lisica	*Alopias pelagicus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Velikooka morska lisica	*Alopias superciliosus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Morska lisica	*Alopias vulpinus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; HELCOM
Žarkasta raža	*Amblyraja radiata*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Morske mačke	*Apristurus spp.*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; ranljiva vrsta; relevantno za globokomorski ribolov
Svilnati morski pes	*Carcharhinus falciformis*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Galapagos shark“	*Carcharhinus galapagensis*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Dolgoplavuti morski pes	*Carcharhinus longimanus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Sivi morski pes	*Carcharhinus plumbeus*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
Morski vol	*Carcharias taurus*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
Beli morski volk	*Carcharodon carcharias*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Gulper shark“	*Centrophorus granulosus*	vsi oceani in morja	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga III k Barcelonski konvenciji; OSPAR
Globokomorski trneži	*Centrophorus spp.*	vse regije	relevantno za globokomorski ribolov
Luskasti globokomorski trnež	*Centrophorus squamosus*	vsi oceani in morja	regionalne organizacije za upravljanje ribištva, prioriteta; OSPAR
Črna morska mačka	*Centroscyllium fabricii*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; relevantno za globokomorski ribolov
Portugalski morski pes	*Centroscymnus coelolepis*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; relevantno za globokomorski ribolov; OSPAR
„Longnose velvet dogfish“	*Centroscymnus crepidater*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; ranljiva vrsta; relevantno za globokomorski ribolov
Morski pes orjak	*Cetorhinus maximus*	vsi oceani in morja	regionalne organizacije za upravljanje ribištva, prioriteta; OSPAR; HELCOM
Morska podgana	*Chimaera monstrosa*	vse regije	relevantno za globokomorski ribolov
Ovratničarski šesteroškrgar	*Chlamydoselachus anguineus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; ranljiva vrsta; relevantno za globokomorski ribolov
Temni morski pes	*Dalatias licha*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; ranljiva vrsta; relevantno za globokomorski ribolov
Morski bič	*Dasyatis pastinaca*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol); HELCOM

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Kljunati morski pes	*Deania calcea*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; relevantno za globokomorski ribolov
Kljunata raža	*Dipturus batis*	vsi oceani in morja	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji; OSPAR; HELCOM
Bela raža	**Rostroraja alba*	OSPAR II, III, IV	OSPAR
Veliki svetilec	*Etmopterus princeps*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; ranljiva vrsta; relevantno za globokomorski ribolov
Črni svetilec	*Etmopterus spinax*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; relevantno za globokomorski ribolov; HELCOM
„Winghead hammerhead“	*Eusphyra blochii*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Pepelasti morski pes	*Galeorhinus galeus*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji; HELCOM
Črnousta morska mačka	*Galeus melastomus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; relevantno za globokomorski ribolov
„Mouse catshark“	*Galeus murinus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; relevantno za globokomorski ribolov
„Spiny butterfly ray“	*Gymnura altavela*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
„Sharpnose sevengill shark“	*Heptranchias perlo*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga III k Barcelonski konvenciji
Šesteroškrgar	*Hexanchus griseus*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji; HELCOM
Veleoka morska podgana	*Hydrolagus mirabilis*	vse regije	relevantno za globokomorski ribolov
Atlantski mako	*Isurus oxyrinchus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Mako	*Isurus paucus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Atlantski morski pes	*Lamna nasus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; OSPAR; HELCOM
Peščena raža	*Leucoraja circularis*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
„Maltese skate“	*Leucoraja melitensis*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
„Reef manta ray“	*Manta alfredi*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Manta	*Manta birostris*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Longhorned mobula“	*Mobula eregoodootenkee*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Lesser devil ray“	*Mobula hypostoma*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Spinetail mobula“	*Mobula japanica*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Shortfin devil ray“	*Mobula kuhlii*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Mala manta	*Mobula mobular*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Munk’s devil ray“	*Mobula munkiana*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Lesser Guinean devil ray“	*Mobula rochebrunei*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Chilean devil ray“	*Mobula tarapacana*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Smoothtail mobula“	*Mobula thurstoni*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Pegasti morski pes	*Mustelus asterias*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga III k Barcelonski konvenciji
Navadni morski pes	*Mustelus mustelus*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga III k Barcelonski konvenciji
Črnopikčasti morski pes	*Mustelus punctulatus*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga III k Barcelonski konvenciji
Črnousta morska mačka	*Galeus melastomus*	Baltsko morje	HELCOM
Morska mačka	*Scyliorhinus canicula*	Baltsko morje	HELCOM
Žarkasta raža	*Amblyraja radiata*	Baltsko morje	HELCOM
„Shagreen ray“	*Leucoraja fullonica*	Baltsko morje	HELCOM
Električni skat	*Torpedo marmorata*	Baltsko morje	HELCOM

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
„Sailfin roughshark (Sharpback shark)“	*Oxynotus paradoxus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; ranljiva vrsta; relevantno za globokomorski ribolov
Drobnozobi pilar	*Pristis pectinata*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
Pilar	*Pristis pristis*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
Krokodilji morski pes	*Pseudocarcharias kamoharai*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Pelagični morski bič	*Pteroplatytrygon violacea*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Okrogla raža	*Raja fyllae*	vse regije	relevantno za globokomorski ribolov
Arktična raža	*Raja hyperborea*	vse regije	relevantno za globokomorski ribolov
Norveška kljunata raža	*Raja nidarosiensis*	vse regije	relevantno za globokomorski ribolov
Pegasta raža	*Raja montagui*	OSPAR I, II, III, IV	OSPAR; HELCOM
Orjaški kitovec	*Rhincodon typus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Blackchin guitarfish“	*Rhinobatos cemiculus*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
Navadni goslaš	*Rhinobatos rhinobatos*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
Kopjenosa morska podgana	*Rhinochimaera atlantica*	vse regije	relevantno za globokomorski ribolov
Bela raža	*Rostroraja alba*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
„Knifetooth dogfish“	*Scymnodon ringens*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; relevantno za globokomorski ribolov
Drugi morski psi	*Selachimorpha* (ali *Selachii*), *Batoidea* (opredeliti po posameznih vrstah v skladu s podatki o iztovarjanju, podatki iz raziskav ali podatkih o ulovu)	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; HELCOM
Grenlandski morski pes	*Somniosus microcephalus*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta; relevantno za globokomorski ribolov; HELCOM

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
valovitoglava kladvenica	*Sphyrna lewini*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
„Great hammerhead“	*Sphyrna mokarran*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Kladvenica	*Sphyrna zygaena*	vsi oceani	regionalne organizacije za upravljanje ribištva, prioriteta
Trnež	*Squalus acanthias*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga III k Barcelonski konvenciji; OSPAR; HELCOM
„Sawback angelshark“	*Squatina aculeata*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
Pegasti sklat	*Squatina oculata*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji
Sklat	*Squatina squatina*	vsi oceani ter Sredozemsko morje in Črno morje	regionalne organizacije za upravljanje ribištva, prioriteta; Priloga II k Barcelonski konvenciji; OSPAR; HELCOM
Morski piškur	*Petromyzon marinus*	OSPAR I, II, III, IV	OSPAR; HELCOM
Rečni piškur	*Lampetra fluviatilis*	Baltsko morje	HELCOM
Sesalci	Mammalia		
Kiti in delfini – vse vrste	Cetacea – *vse vrste*	vsa območja	Direktiva Sveta 92/43/EGS ([7])
Pritlikavi kit	*Balaenoptera acutorostrata*	Sredozemsko morje	Priporočilo GFCM ([8])/36/2012/2 in Priloga II k Barcelonski konvenciji
Grenlandski kit	*Balaena mysticetus*	OSPAR I	OSPAR
Sinji kit	*Balaenoptera musculus*	vsa območja OSPAR	OSPAR
Biskajski kit	*Eubalaena glacialis*	vsa območja OSPAR	OSPAR
Borealni kit, zajval	*Balaenoptera borealis*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Hrbtopluti kit, progasti kit	*Balaenoptera physalis*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Navadni delfin, navadna pliskavka	*Delphinus delphis*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Biskajski kit, ledni kit	*Eubalaena glacialis*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Dolgoplavuta mrka pliskavka, obloglavka	*Globicephala melas*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Okrogloglavi delfin	*Grampus griseus*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Pritlikavi glavač	*Kogia simus*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Kit grbavec	*Megaptera novaeangliae*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Blainvillov dvozob	*Mesoplodon densirostris*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Orka	*Orcinus orca*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Pristaniška rjava pliskavka	*Phocoena phocoena*	Sredozemsko morje; OSPAR II, III	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji; Direktiva 92/43/EGS; OSPAR
Glavač	*Physeter macrocephalus*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Mala orka	*Pseudorca crassidens*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Navadni progasti delfin	*Stenella coeruleoalba*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Brazdastozobi delfin	*Steno bredanensis*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Velika pliskavka	*Tursiops truncatus*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Cuvierjev kljunati kit	*Ziphius cavirostris*	Sredozemsko morje	Priporočilo GFCM/36/2012/2 in Priloga II k Barcelonski konvenciji
Sredozemska medvedjica	*Monachus monachus*	vsa območja	Priporočilo GFCM/35/2011/5 in Priloga II k Barcelonski konvenciji; Direktiva 92/43/EGS
„Saimaa ringed seal“	*Phoca hispida saimensis*	vsa območja	Direktiva 92/43/EGS
Sivi tjulenj	*Halichoerus grypus*	vsa območja	Direktiva 92/43/EGS
Navadni tjulenj	*Phoca vitulina*	vsa območja	Direktiva 92/43/EGS
„Baltic ringed seal“	*Phoca hispida bottnica*	vsa območja	Direktiva 92/43/EGS

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Ptice	Aves		
„Cory's Shearwater“	*Calonectris borealis*	vsa območja	Direktiva 2009/147/ES Evropskega parlamenta in Sveta ([9])
Veliki kormoran	*Phalacrocorax carbo*	vsa območja	Direktiva 2009/147/ES
Navadni strmoglavec	*Morus bassanus*	vsa območja	Direktiva 2009/147/ES
Mormon	*Fratercula arctica*	vsa območja	Direktiva 2009/147/ES
Balearski viharnik	*Puffinus mauretanicus*	vsa območja	Direktiva 2009/147/ES
Rečni galeb	*Larus ridibundus*	vsa območja	Direktiva 2009/147/ES
Črna raca	*Melanitta nigra*	vsa območja	Direktiva 2009/147/ES
Vranjek	*Phalacrocorax aristotelis*	vsa območja	Direktiva 2009/147/ES
Veliki viharnik	*Ardenna gravis*	vsa območja	Direktiva 2009/147/ES
Atlantski viharnik	*Puffinus puffinus*	vsa območja	Direktiva 2009/147/ES
Ledeni viharnik	*Fulmarus glacialis*	vsa območja	Direktiva 2009/147/ES
„Scopoli's Shearwater“	*Calonectris diomedea*	vsa območja	Direktiva 2009/147/ES
Črni viharnik	*Ardenna grisea*	vsa območja	Direktiva 2009/147/ES
Sredozemski viharnik	*Puffinus yelkouan*	vsa območja	Direktiva 2009/147/ES
Progastokljuni galeb	*Larus audouinii*	vsa območja	Direktiva 2009/147/ES
Islandski zvonec	*Bucephala islandica*	vsa območja	Direktiva 2009/147/ES
Siva bulverija	*Bulweria bulwerii*	vsa območja	Direktiva 2009/147/ES
Navadni zvonec	*Bucephala clangula*	vsa območja	Direktiva 2009/147/ES
Srebrni galeb	*Larus argentatus*	vsa območja	Direktiva 2009/147/ES
Ledni galeb	*Larus hyperboreus*	vsa območja	Direktiva 2009/147/ES
Veliki galeb	*Larus marinus*	vsa območja	Direktiva 2009/147/ES
Velika govnačka	*Catharacta skua*	vsa območja	Direktiva 2009/147/ES

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Rjavka	*Aythya marila*	vsa območja	Direktiva 2009/147/ES; Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Sivka	*Aythya ferina*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Rjavi galeb	*Larus fuscus*	vsa območja	Direktiva 2009/147/ES
Rakovičar	*Alle alle*	vsa območja	Direktiva 2009/147/ES
Dolgorepa govnačka	*Stercorarius longicaudus*	vsa območja	Direktiva 2009/147/ES
Mala njorka	*Alca torda*	vsa območja	Direktiva 2009/147/ES
Bodičasta govnačka	*Stercorarius parasiticus*	vsa območja	Direktiva 2009/147/ES
Polarni slapnik	*Gavia arctica*	vsa območja	Direktiva 2009/147/ES
Tropski viharnik	*Puffinus lherminieri*	vsa območja	Direktiva 2009/147/ES
Črna njorka	*Cepphus grylle*	vsa območja	Direktiva 2009/147/ES
Črna raca	*Melanitta americana*	vsa območja	Direktiva 2009/147/ES
Črnovrati ponirek	*Podiceps nigricollis*	vsa območja	Direktiva 2009/147/ES
Rumenonogi galeb	*Larus cachinnans*	vsa območja	Direktiva 2009/147/ES
Navadna gaga	*Somateria mollissima*	vsa območja	Direktiva 2009/147/ES
Temnokljuna lumna	*Uria aalge*	vsa območja	Direktiva 2009/147/ES
Ledni slapnik	*Gavia immer*	vsa območja	Direktiva 2009/147/ES
Veliki žagar	*Mergus merganser*	vsa območja	Direktiva 2009/147/ES
Čopasti ponirek	*Podiceps cristatus*	vsa območja	Direktiva 2009/147/ES
Harlekinka	*Histrionicus histrionicus*	vsa območja	Direktiva 2009/147/ES
Zlatouhi ponirek	*Podiceps auritus*	vsa območja	Direktiva 2009/147/ES
Polarni galeb	*Larus glaucoides*	vsa območja	Direktiva 2009/147/ES
Pisana gaga	*Somateria spectabilis*	vsa območja	Direktiva 2009/147/ES

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Zimska raca	*Clangula hyemalis*	vsa območja	Direktiva 2009/147/ES
Črnoglavi galeb	*Larus melanocephalus*	vsa območja	Direktiva 2009/147/ES
Sivi galeb	*Larus canus*	vsa območja	Direktiva 2009/147/ES
Srednji žagar	*Mergus serrator*	vsa območja	Direktiva 2009/147/ES
Rjavovrati ponirek	*Podiceps grisegena*	vsa območja	Direktiva 2009/147/ES
Rdečegrli slapnik	*Gavia stellata*	vsa območja	Direktiva 2009/147/ES
Zalivski galeb	*Larus genei*	vsa območja	Direktiva 2009/147/ES
Pisana raca	*Polysticta stelleri*	vsa območja	Direktiva 2009/147/ES
Lopatasta govnačka	*Stercorarius pomarinus*	vsa območja	Direktiva 2009/147/ES
Debelokljuna lumna	*Uria lomvia*	vsa območja	Direktiva 2009/147/ES
Beloliska	*Melanitta fusca*	vsa območja	Direktiva 2009/147/ES
Rumenokljuni slapnik	*Gavia adamsii*	vsa območja	Direktiva 2009/147/ES
Rumenonogi galeb	*Larus michahellis*	vsa območja	Direktiva 2009/147/ES
Madeirski švigavec	*Pterodroma madeira*	vsa območja	Direktiva 2009/147/ES
Ribji galeb	*Larus ichthyaetus*	vsa območja	Direktiva 2009/147/ES
Triprsti galeb	*Rissa tridactyla*	vsa območja	Direktiva 2009/147/ES
Rožnati pelikan	*Pelecanus onocrotalus*	vsa območja	Direktiva 2009/147/ES
Viharni strakoš	*Oceanodroma leucorhoa*	vsa območja	Direktiva 2009/147/ES
Ploskokljuni liskonožec	*Phalaropus fulicarius*	vsa območja	Direktiva 2009/147/ES
Ozkokljuni liskonožec	*Phalaropus lobatus*	vsa območja	Direktiva 2009/147/ES
Antarktični strakoš	*Oceanites oceanicus*	vsa območja	Direktiva 2009/147/ES
Polarna čigra	*Sterna paradisaea*	vsa območja	Direktiva 2009/147/ES
Madeirski strakoš	*Hydrobates castro*	vsa območja	Direktiva 2009/147/ES
Črna čigra	*Chlidonias niger*	vsa območja	Direktiva 2009/147/ES
Kaspijska čigra	*Hydroprogne caspia*	vsa območja	Direktiva 2009/147/ES

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Črnonoga čigra	*Gelochelidon nilotica*	vsa območja	Direktiva 2009/147/ES
Navadna čigra	*Sterna hirundo*	vsa območja	Direktiva 2009/147/ES
Zelenortski švigavec	*Pterodroma deserta*	vsa območja	Direktiva 2009/147/ES
Beli galeb	*Pagophila eburnea*	vsa območja	Direktiva 2009/147/ES
Bengalska čigra	*Thalasseus bengalensis*	vsa območja	Direktiva 2009/147/ES
Mali galeb	*Hydrocoloeus minutus*	vsa območja	Direktiva 2009/147/ES
Mala čigra	*Sternula albifrons*	vsa območja	Direktiva 2009/147/ES
„Monteiro's Stormpetrel“	*Hydrobates monteiroi*	vsa območja	Direktiva 2009/147/ES
Rožnata čigra	*Sterna dougallii*	vsa območja	Direktiva 2009/147/ES
Rožnati galeb	*Rhodostethia rosea*	vsa območja	Direktiva 2009/147/ES
Lastovičji galeb	*Xema sabini*	vsa območja	Direktiva 2009/147/ES
Kričava čigra	*Thalasseus sandvicensis*	vsa območja	Direktiva 2009/147/ES
Polarni galeb	*Larus thayeri*	vsa območja	Direktiva 2009/147/ES
Progastoglavi strakoš	*Pelagodroma marina*	vsa območja	Direktiva 2009/147/ES
Navadni strakoš	*Hydrobates pelagicus*	vsa območja	Direktiva 2009/147/ES
Rjavi galeb	*Larus fuscus fuscus*	OSPAR I	Seznam OSPAR ogroženih in izginjajočih vrst
Beli galeb	*Pagophila eburnea*	OSPAR I	Seznam OSPAR ogroženih in izginjajočih vrst
Pisana raca	*Polysticta stelleri*	OSPAR I	Seznam OSPAR ogroženih in izginjajočih vrst
Mali viharnik	*Puffinus assimilis baroli (auct.incert.)*	OSPAR V	Seznam OSPAR ogroženih in izginjajočih vrst
Balearski viharnik	*Puffinus mauretanicus*	OSPAR II, III, IV, V	Seznam OSPAR ogroženih in izginjajočih vrst
Triprsti galeb	*Rissa tridactyla*	OSPAR I, II	Seznam OSPAR ogroženih in izginjajočih vrst
Rožnata čigra	*Sterna dougallii*	OSPAR II, III, IV, V	Seznam OSPAR ogroženih in izginjajočih vrst

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Iberska lumna	*Uria aalge – iberska populacija (sinonima: Uria aalge albionis, Uria aalge ibericus)*	OSPAR IV	Seznam OSPAR ogroženih in izginjajočih vrst
Debelokljuna lumna	*Uria lomvia*	OSPAR I	Seznam OSPAR ogroženih in izginjajočih vrst
Plazilci	Reptilia		
„Kemp's ridley sea turtle“	*Lepidochelys kempii*	vsa območja	Direktiva 92/43/EGS; Priporočilo GFCM/35/2011/4 in Priloga II k Barcelonski konvenciji
Glavata kareta	*Caretta caretta*	vsa območja	Direktiva 92/43/EGS; Priporočilo GFCM/35/2011/4 in Priloga II k Barcelonski konvenciji; OSPAR
Usnjača	*Dermochelys coriacea*	vsa območja	Direktiva 92/43/EGS; Priporočilo GFCM/35/2011/4 in Priloga II k Barcelonski konvenciji; OSPAR
Prava kareta	*Eretmochelys imbricata*	vsa območja	Direktiva 92/43/EGS; Priporočilo GFCM/35/2011/4 in Priloga II k Barcelonski konvenciji
Orjaška črepaha	*Chelonia mydas*	vsa območja	Direktiva 92/43/EGS; Priporočilo GFCM/35/2011/4 in Priloga II k Barcelonski konvenciji
Nilska mehkoščitka	*Trionyx triunguis*	Sredozemsko morje	Priporočilo GFCM/35/2011/4 in Priloga II k Barcelonski konvenciji
Mehkužci	Mollusca		
Navadna venerica	*Chamelea gallina*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Trakasti donaks	*Donacilla cornea*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
„Eledone especies“	*Eledone spp.*	vsa območja	Nacionalni načrti upravljanja
Užitna klapavica	*Mytilus galloprovincialis*	vsa območja Sredozemlja	Nacionalni načrti upravljanja
Užitna klapavica	*Mytilus galloprovincialis*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Latvica	*Patella spp.*	Sredozemsko morje	Priloga II k Barcelonski konvenciji
Priseljena rapana	*Rapana venosa*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Progasta srčanka	*Acanthocardia tuberculata*	vsa območja	Nacionalni načrti upravljanja
Bodičasti volek	*Bolinus brandaris*	vsa območja	Nacionalni načrti upravljanja

Splošno ime	Znanstveno ime	Regija/regionalna organizacija za upravljanje ribištva	Pravni okvir
Lepotka	*Callista chione*	vsa območja	Nacionalni načrti upravljanja
Gladek donaks	*Donax trunculus*	vsa območja	Nacionalni načrti upravljanja
Islandska školjka	*Arctica islandica*	OSPAR II	OSPAR
„Azorean barnacle“	*Megabalanus azoricus*	OSPAR V; vsa območja, kjer se pojavlja	OSPAR
Škrlatni volek	*Nucella lapillus*	OSPAR II, III, IV	OSPAR
Ostriga	*Ostrea edulis*	OSPAR II	OSPAR
„Azorean limpet“	*Patella ulyssiponensis aspera*	vsa območja OSPAR, kjer se pojavlja	OSPAR
Raki	Crustacea		
Jastog	*Homarus gammarus*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Globokomorska rdeča rakovica	*Chaceon (Geryon) affinis*	vse regije	relevantno za globokomorski ribolov
Navadna kozica	*Crangon crangon*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Mala skalna kozica	*Palaemon adspersus*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Skalna kozica	*Palaemon elegans*	Črno morje	Priloga IV k Protokolu za ohranjanje biotske raznovrstnosti in krajine Črnega morja (Black Sea Biodiversity and Landscape Conservation Protocol)
Rarogi	*Palinuridae*	Sredozemsko morje	Uredba (ES) št. 1967/2006 (najmanjša velikost ohranjanja)
Ožigalkarji	Cnidaria		
Rdeča korala	*Corallium rubrum*	Sredozemsko morje	Priporočilo GFCM/36/2012/1 in Priporočilo GFCM/35/2011/2

(1) Barcelonska konvencija za varstvo morskega okolja in obalnega območja Sredozemlja.
(2) Konvencija OSPAR o varstvu morskega okolja severovzhodnega Atlantika.
(3) Konvencija HELCOM o varstvu morskega okolja območja Baltika.
(4) Uredba Sveta (ES) št. 2347/2002 z dne 16. decembra 2002 o določitvi posebnih pogojev dostopa in z njimi povezanih pravil za ribolov globokomorskih staležev (UL L 351, 28.12.2002, str. 6).
(5) Uredba Sveta (ES) št. 1967/2006 z dne 21. decembra 2006 o ukrepih za upravljanje za trajnostno izkoriščanje ribolovnih virov v Sredozemskem morju, spremembi Uredbe (EGS) št. 2847/93 in razveljavitvi Uredbe (ES) št. 1626/94 (UL L 409, 30.12.2006, str. 11).
(6) Uredba Sveta (ES) št. 894/97 z dne 29. aprila 1997 o nekaterih tehničnih ukrepih za ohranjanje ribolovnih virov (UL L 132, 23.5.1997, str. 1).
(7) Direktiva Sveta 92/43/EGS z dne 21. maja 1992 o ohranjanju naravnih habitatov ter prosto živečih živalskih in rastlinskih vrst (UL L 206, 22.7.1992, str. 7).
(8) Generalna komisija za ribištvo v Sredozemlju.
(9) Direktiva 2009/147/ES Evropskega parlamenta in Sveta z dne 30. novembra 2009 o ohranjanju prosto živečih ptic (UL L 20, 26.1.2010, str. 7).

Za prepovedane vrste: uporabijo se samo osebki, ki se ulovijo mrtvi. Po meritvah se zavržejo. Zbiranje podatkov poteka na letni ravni, posodabljanje/obdelava podatkov pa mora biti pravočasno/pravočasna, da ustreza časovnemu okviru ocen staleža.

Biološki podatki

Tabela 1E

Sladkovodne anadromne in katadromne vrste

Vrsta (domače ime)	Vrsta (znanstveno ime)	Območja, ki niso morska in na katerih se nahaja stalež/oznaka staleža
Jegulja	*Anguilla anguilla*	Enote za upravljanje staležev jegulj, kot so opredeljene v skladu z Uredbo Sveta (ES) št. 1100/2007 ([1])
Atlantski losos	*Salmo salar*	vsa območja naravne razširjenosti
Morska postrv	*Salmo trutta*	vse celinske vode, ki se iztekajo v Baltsko morje

([1]) Uredba Sveta (ES) št. 1100/2007 z dne 18. septembra 2007 o ukrepih za obnovo staleža evropske jegulje (UL L 248, 22.9.2007, str. 17).

Tabela 2

Ribolovna dejavnost po regiji

Raven 1	Raven 2	Raven 3	Raven 4	Raven 5	Raven 6	Razredi celotne dolžine (m) (d)					
Dejavnost	Razredi orodja	Skupine orodja	Vrsta orodja	Ciljni skupek vrst (a)	Velikost mrežnega očesa in druge selektivne naprave	< 10	10 - < 12	12 - < 18	18 - < 24	24 - < 40	40 & +
Ribolovna dejavnost	strgače	strgače	strgača, upravljana s plovila [DRB]	anadromne vrste (ANA) katadromne vrste (CAT) glavonožci (CEP) raki (CRU) pridnene vrste (DEF) globokomorske vrste (DWS) ribe kostnice (FIF) sladkovodne vrste (brez oznake) razno (MIS) mešano glaovnožci in pridnene vrste (MCF) mešano raki in pridnene vrste (MCF) mešano globokomorske in pridnene vrste (MDD) mešano pelagične in pridnene vrste (MCF) mehkužci (MOL) velike pelagične ribe (LPF) male pelagične ribe (SPF) velike pelagične ribe (LPF) in male pelagične ribe (SPF)	(b)						
			mehanizirana/sesalna strgača [HMD]		(b)						
	vlečne mreže	pridnene vlečne mreže	pridnena vlečna mreža s širilkami [OTB]		(b)						
			dvojna vlečna mreža s širilkami [OTT]		(b)						
			pridnena vlečna mreža, upravljana z dveh plovil [PTB]		(b)						
			vlečna mreža z gredjo [TBB]		(b)						
		pelagične vlečne mreže	pelagična vlečna mreža s širilkami [OTM]		(b)						
			pelagična vlečna mreža, upravljana z dveh plovil [PTM]		(b)						

Raven 1	Raven 2	Raven 3	Raven 4	Raven 5	Raven 6	Razredi celotne dolžine (m) (d)					
Dejavnost	Razredi orodja	Skupine orodja	Vrsta orodja	Ciljni skupek vrst (a)	Velikost mrežnega očesa in druge selektivne naprave	< 10	10 - < 12	12 - < 18	18 - < 24	24 - < 40	40 & +
	trnki in vrvice	ribiške palice in vrvice	ročne ribiške vrvice in ribiške palice [LHP] [LHM]		(b)						
			panula [LTL]		(b)						
		parangali	viseči parangali [LLD]		(b)						
			stoječi parangali [LLS]		(b)						
	pasti	pasti	vrše in pasti [FPO]		(b)						
			kogol [FYK]		(b)						
			nameščene nepokrite pregrade [FPN]		(b)						
			fiksne naprave za ograje in vrše (potrebna koda)		(b)						
	mreže	mreže	trislojna mreža [GTR]		(b)						
			stoječa zabodna mreža [GNS]		(b)						
			viseča mreža [GND]		(b)						
	potegalke	obkroževalne mreže	zaporna plavarica [PS]		(b)						
			mreže lampara [LA]		(b)						
		potegalke (c)	škotska potegalka [SSC]		(b)						
			danska potegalka [SDN]		(b)						

Raven 1	Raven 2	Raven 3	Raven 4	Raven 5	Raven 6	Razredi celotne dolžine (m) (d)					
Dejavnost	Razredi orodja	Skupine orodja	Vrsta orodja	Ciljni skupek vrst (a)	Velikost mrežnega očesa in druge selektivne naprave	< 10	10 - < 12	12 - < 18	18 - < 24	24 - < 40	40 & +
			potegalka, upravljana z dveh plovil [SPR]		(b)						
			obalna potegalka in potegalka odprtega morja [SB] [SV]		(b)						
	drugo orodje	drugo orodje	ribolov mladih jegulj (brez oznake)	mlada jegulja	(b)						
	razno (navesti)	razno (navesti)			(b)						
Druge dejavnosti razen ribolova				druge dejavnosti razen ribolova							
Neaktivno				neaktivno							

Opombe:
(a) V skladu z obstoječimi oznakami iz zadevnih uredb.
(b) V skladu z obstoječimi oznakami iz zadevnih uredb.
(c) Z napravami za zbiranje rib (FAD)/v prostih jatah.
(d) V Sredozemlju < 6 m in 6 m–12 m.

Tabela 3

Vrste, ki se zbirajo za rekreacijski ribolov

	Območje	Vrsta
1	Baltsko morje (podrazdelki ICES 22–32)	atlantski lososi, jegulje in morske postrvi (vključno v sladki vodi) ter trske
2	Severno morje (območja ICES IIIa, IV in VIId)	atlantski lososi in jegulje (vključno v skladi vodi); brancini, trske, polaki ter morski psi in skati
3	Vzhodna Arktika (območji ICES I in II)	atlantski lososi in jegulje (vključno v skladi vodi); trske, polaki ter morski psi in skati
4	Severni Atlantik (območja ICES V–XIV in območja NAFO)	atlantski lososi in jegulje (vključno v skladi vodi); brancini, trske, polaki, morski psi in skati ter izrazito selivske vrste ICCAT
5	Sredozemsko morje	jegulje (vključno v sladki vodi), morski psi in skati ter izrazito selivske vrste ICCAT
6	Črno morje	jegulje (vključno v sladki vodi), morski psi in skati ter izrazito selivske vrste ICCAT

Tabela 4

Spremenljivke za ribolovne dejavnosti

	Spremenljivke [1]	Enota
	Zmogljivost	
	Število plovil	število
	Tonaža (BT), kW, starost plovila	število
	Napor	
	Dnevi na morju	dnevi
	Trajanje ribolova (neobvezno)	ure
	Ribolovni dnevi	dnevi
	kW * ribolovni dnevi	število
	BT * ribolovni dnevi	število
	Število potovanj	število
	Število ribolovnih operacij	število
	Število mrež/Dolžina (*)	število/metri
	Število trnkov, število vrvic (*)	število
	Število vrš, pasti (*)	število
	Iztovarjanje	
	Vrednost iztovora skupaj in za vsako komercialno vrsto	euri
	Živa teža iztovora skupaj in za vsako vrsto	tone
	Cene za vsako komercialno vrsto	euri/kg

[1] Vse spremenljivke je treba sporočiti na ravni agregiranja (segment ribolovnih dejavnosti in flote), opredeljeni v tabeli 3 in tabeli 5B, ter po podregiji/ribolovnem območju, kot je opredeljeno v tabeli 5Cb.

(*) O zbiranju teh spremenljivk za plovila, krajša od 10 metrov, se je treba dogovoriti na ravni morske regije.

EKONOMSKI PODATKI FLOTE

Tabela 5A

Ekonomske spremenljivke za floto

Skupina spremenljivke	Spremenljivka	Enota
Prihodek	bruto vrednost iztovora	euri
	prihodek od oddaje kvotnih ali drugih ribolovnih pravic	euri
	drugi prihodki	euri
Stroški dela	stroški osebja	euri
	vrednost neplačanega dela	euri
Stroški energije	stroški energije	euri
Stroški popravil in vzdrževanja	stroški popravil in vzdrževanja	euri
Drugi operativni stroški	spremenljivi stroški	euri
	fiksni stroški	euri
	plačila za zakup/najem kvotnih ali drugih ribolovnih pravic	euri
Subvencije	subvencije za tekoče poslovanje	euri
	subvencije za naložbe	euri
Stroški kapitala	potrošnja stalnega kapitala	euri
Vrednost kapitala	vrednost fizičnega kapitala	euri
	vrednost kvotnih in drugih ribolovnih pravic	euri
Naložbe	naložbe v opredmetena sredstva, neto	euri
Finančni položaj	dolgoročni/kratkoročni dolg	euri
	sredstva skupaj	euri
Zaposlovanje	zaposlena posadka	število
	neplačana delovna sila	število
	skupno število opravljenih delovnih ur na leto	število

Skupina spremenljivke	Spremenljivka	Enota
Flota	število plovil	število
	povprečna celotna dolžina plovil	metri
	skupna tonaža plovil	BT
	skupna moč plovil	kW
	povprečna starost plovil	leta
Napor	dnevi na morju	dnevi
	poraba energije	litri
Število ribiških podjetij/enot	število ribiških podjetij/enot	število
Proizvodna vrednost po vrstah	vrednost iztovora za vsako vrsto	euri
	povprečna cena za vsako vrsto	euri/kg

EKONOMSKI PODATKI FLOTE

Tabela 5B

Razčlenitev flote

		Dolžinski razredi (LOA) [1]					
Aktivna plovila		0 m – < 10 m 0 m – < 6 m	10 m – < 12 m 6 m – < 12 m	12 m – < 18 m	18 m – < 24 m	24 m – < 40 m	40 m ali več
ki uporabljajo „aktivna“ orodja	plovila z vlečnimi mrežami z gredjo						
	plovila s pridneno vlečno mrežo in/ali pridneno potegalko						
	plovila z vlečnimi mrežami za pelagični ribolov						
	plovila z zapornimi plavaricami						
	plavajoči bagri						
	plovila, ki uporabljajo druga aktivna orodja						
	plovila, ki uporabljajo samo večnamenska aktivna orodja						

		Dolžinski razredi (LOA) (1)					
Aktivna plovila		0 m – < 10 m 0 m – < 6 m	10 m – < 12 m 6 m – < 12 m	12 m – < 18 m	18 m – < 24 m	24 m – < 40 m	40 m ali več
ki uporabljajo „pasivna“ orodja	plovila, ki uporabljajo trnke	(2)	(2)				
	plovila z visečimi in/ali pritrjenimi mrežami						
	plovila, ki uporabljajo vrše in/ali pasti						
	plovila, ki uporabljajo druga pasivna orodja						
	plovila, ki uporabljajo samo večnamenska pasivna orodja						
ki uporabljajo večnamenska orodja	plovila, ki uporabljajo aktivna in pasivna orodja						
Neaktivna plovila							

(1) Za plovila, krajša od 12 metrov, v Sredozemskem morju in Črnem morju, sta kategoriji dolžin 0 –< 6, 6 –< 12 metrov. Za vse druge regije sta opredeljeni kategoriji dolžin 0 –< 10, 10 –< 12 metrov.
(2) Plovila z dolžino manj kot 12 metrov, ki uporabljajo pasivna orodja v Sredozemskem morju in Črnem morju, je mogoče razčleniti glede na vrsto orodja.Opredelitev segmenta flote vključuje tudi navedbo nadregije in, če je na voljo, geografskega kazalnika za identifikacijo plovil, ki izvajajo ribolov v najbolj oddaljenih regijah in izključno zunaj voda EU.

EKONOMSKI PODATKI FLOTE

Tabela 5C

Geografska razčlenjenost po regijah

Podregija/Ribolovno območje	Regija	Nadregija
I	II	III
Sklop prostorskih enot na ravni 3, kot je opredeljeno v tabeli 3 (razdelek NAFO)	NAFO (območje FAO 21)	Baltsko morje; Severno morje; vzhodna Arktika; NAFO; razširjene severozahodne vode (območja ICES V, VI in VII) in jugozahodne vode
Sklop prostorskih enot na ravni 4, kot je opredeljeno v tabeli 3 (podrazdelek ICES)	Baltsko morje (območja ICES III b–d)	
Sklop prostorskih enot na ravni 3, kot je opredeljeno v tabeli 3 (razdelek ICES)	Severno morje (območji ICES IIIa in IV), vzhodna Arktika (območji ICES I in II)	
	severozahodne vode (območja ICES Vb (samo vode Unije), VI in VII)	
	severozahodne vode zunaj Unije (območji ICES Va in Vb) (samo vode zunaj Unije)	

Podregija/Ribolovno območje	Regija	Nadregija
I	II	III
Sklop prostorskih enot na ravni 3, kot je opredeljeno v tabeli 3 (razdelek ICES/CECAF)	jugozahodne vode (območja ICES VIII, IX in X (vode okoli Azorov), območja CECAF 34.1.1, 34.1.2 in 34.2.0 (vode okoli Madeire in Kanarskih otokov)	
Sklop prostorskih enot na ravni 4, kot je opredeljeno v tabeli 3 (GSA)	Sredozemsko morje (morske vode Sredozemlja vzhodno od črte 5° 36′ zahodne zemljepisne dolžine), Črno morje (zemljepisno podobmočje GFCM, kot je opredeljeno v Resoluciji FCM/33/2009/2)	Sredozemsko morje in Črno morje
Podobmočja vzorčenja regionalnih organizacij za upravljanje ribištva (razen GFCM)	druge regije, kjer ribolov izvajajo plovila Unije in ga upravljajo regionalne organizacije za upravljanje ribištva, v katerih ima Evropska unija status pogodbenice ali opazovalke (npr. ICCAT, IOTC, CECAF …)	druge regije

Tabela 6

Socialne spremenljivke za sektorja ribištva in ribogojstva

Spremenljivka	Enota
Zaposlenost po spolu	število
EPDČ po spolu	število
Neplačana delovna sila po spolu	število
Zaposlenost po starosti	število
Zaposlenost po stopnji izobrazbe	število za vsako stopnjo izobrazbe
Zaposlenost po državljanstvu	število iz EU, EGP in držav, ki niso članice EU/EGP
Zaposlenost po zaposlitvenem statusu	število
Nacionalni ekvivalent polnega delovnega časa (EPDČ)	število

Tabela 7

Ekonomske spremenljivke za sektor ribogojstva

Skupina spremenljivke	Spremenljivka	Enota
Prihodek (*)	bruto prodaja po posameznih vrstah	euri
	drugi prihodki	euri

Skupina spremenljivke	Spremenljivka	Enota
Stroški osebja	stroški osebja	euri
	vrednost neplačanega dela	euri
Stroški energije	stroški energije	euri
Stroški surovin	stroški za živino	euri
	stroški za krmo	euri
Popravila in vzdrževanje	popravila in vzdrževanje	euri
Drugi operativni stroški	drugi operativni stroški	euri
Subvencije	subvencije za tekoče poslovanje	euri
	subvencije za naložbe	euri
Stroški kapitala	potrošnja stalnega kapitala	euri
Vrednost kapitala	skupna vrednost sredstev	euri
Finančni rezultati	finančni prihodki	euri
	finančni odhodki	euri
Naložbe	neto naložbe	euri
Dolg	dolg	euri
Teža surovin	uporabljena živina	kg
	uporabljena ribja krma	kg
Teža prodaje	teža prodaje po posameznih vrstah	kg
Zaposlovanje	število zaposlenih	število/EPDČ
	neplačana delovna sila	število/EPDČ
	število opravljenih delovnih ur na zaposlenega in na neplačanega delavca	ure
Število podjetij	število podjetij (po kategorijah v zvezi s številom zaposlenih oseb)	število

(*) Vključuje neposredna plačila, npr. nadomestilo za ustavitev trgovanja, vračilo trošarine za gorivo ali podobna pavšalna plačila nadomestila; izključuje socialne prejemke in posredne subvencije, npr. znižane dajatve za vhodne surovine, kot je gorivo, ali subvencije za naložbe.

Tabela 8

Okoljske spremenljivke za sektor ribogojstva

Spremenljivka	Specifikacija	Enota
Uporabljena zdravila ali zdravljenja (1)	po tipu	gram
Smrtnost (2)		odstotek

(1) Ekstrapolirano iz podatkov, evidentiranih v skladu s točko 8(b) Priloge I k Uredbi (ES) št. 852/2004 Evropskega parlamenta in Sveta (UL L 139, 30.4.2004, str. 1).
(2) Ekstrapolirano kot odstotek nacionalne proizvodnje iz podatkov, evidentiranih v skladu z odstavkom 1(b) člena 8 Direktive Sveta 2006/88/ES (UL L 328, 24.11.2006, str. 14).

Tabela 9

Razčlenjenost, ki se uporabi za zbiranje podatkov o ribogojstvu (1)

	Tehnike ribogojstva (2)						Polikultura	Drstišča in vzgajališča (3)	Tehnike gojenja lupinarjev			
	Ribniki	Bazeni in kanali	Ograjeni in pregrajeni prostori (6)	Sistemi recirkulacije (5)	Druge metode	Kletke (7)	Vse metode		Gojenje s plavajočimi napravami		Gojenje na dnu (4)	Drugo
									Splavi	Vrvi		
Atlantski losos												
Postrv												
Brancin in špar												
Krap												
Tun												
Jegulja												
Jeseter (ikre za prehrano ljudi)												
Druge sladkovodne ribe												
Druge morske ribe												
Klapavice												

	Tehnike ribogojstva (2)						Polikultura	Drstišča in vzgajališča (3)	Tehnike gojenja lupinarjev			
	Ribniki	Bazeni in kanali	Ograjeni in pregrajeni prostori (6)	Sistemi recirkulacije (5)	Druge metode	Kletke (7)	Vse metode		Gojenje s plavajočimi napravami		Gojenje na dnu (4)	Drugo
									Splavi	Vrvi		
Ostrige												
Ladinke												
Raki												
Drugi mehkužci												
Več vrst												
Morske alge												
Drugi vodni organizmi												

(1) Za opredelitve tehnik ribogojstva glej Uredbo (ES) št. 762/2008.
(2) Podjetja se razčlenijo glede na njihovo glavno tehniko gojenja.
(3) Drstišča in vzgajališča so opredeljena kot prostori za umetno vzrejo, drstenje in gojenje vodnih živali v njihovih zgodnjih fazah življenjskega cikla. Za statistične namene so drstišča namenjena le za gojenje oplojenih iker. Nadaljnje življenjske faze nedoraslih vodnih živali naj bi se odvijale v vzgajališčih. Kadar so drstišča in vzgajališča tesno povezana, se statistični podatki nanašajo le na zadnje življenjske faze gojenih nedoraslih živali (COM(2006) 864 z dne 19. julija 2007).
(4) Tehnika gojenja na dnu zajema območja gojenja lupinarjev na območjih plimovanja (neposredno na tleh ali nekoliko dvignjeno).
(5) Sistemi recirkulacije so sistemi, v katerih se voda po čiščenju ponovno uporabi (na primer filtriranje).
(6) Ograjeni in pregrajeni prostori so opredeljeni kot vodna območja, omejena z mrežami in drugimi pregradami, ki omogočajo nenadzorovano izmenjavo vode in obsegajo celoten vodni steber med substratom in površino; običajno zajemajo veliko količino vode (COM(2006) 864 z dne 19. julija 2007).
(7) Kletke so opredeljene kot odprte ali pokrite ograjene strukture, zgrajene iz mrež ali katerega koli drugega prepustnega materiala, ki dopušča naraven prost pretok vode. Te strukture so lahko plavajoče, viseče ali pritrjene na substrat, tako da še vedno dopuščajo prosti pretok vode od spodaj (COM(2006) 864 z dne 19. julija 2007).

Tabela 10

Raziskave na morju

Naziv raziskave	Kratica	Območje	Obdobje	Glavne ciljne vrste
Baltsko morje				
Baltic International Trawl Survey (mednarodna raziskava vlečnih mrež v Baltiku)	BITS Q1 BITS Q4	IIIaS, IIIb–d	1. in 4. četrtletje	trska in druge pridnene vrste
Baltic International Acoustic Survey (Autumn) (mednarodna sonarna raziskava v Baltiku (jesen))	BIAS	IIIa, IIIb–d	september–oktober	sled in papalina
Gulf of Riga Acoustic Herring Survey (sonarna raziskava sledu v Riškem zalivu)	GRAHS	IIId	3. četrtletje	sled

Naziv raziskave	Kratica	Območje	Obdobje	Glavne ciljne vrste
Sprat Acoustic Survey (sonarna raziskava papaline)	SPRAS	IIId	maj	papalina in sled
Rügen Herring Larvae Survey (raziskava mladic sledu)	RHLS	IIId	marec–junij	sled
Severno morje in vzhodna Arktika (območji ICES I in II)				
International Bottom Trawl Survey (mednarodna raziskava pridnenih vlečnih mrež)	IBTS Q1 IBTS Q3	IIIa, IV	1. in 3. četrtletje	vahnja, trska, saj, sled, papalina, mol, skuša, norveški molič
North Sea Beam Trawl Survey (raziskava vlečnih mrež z gredjo v Severnem morju)	BTS	IVb, IVc,VIId	3. četrtletje	morska plošča, morski list
Demersal Young Fish Survey (raziskava pridnenih nedoraslih rib)	DYFS	obale Severnega morja	3. in 4. četrtletje	morska plošča, morski list, rjava kozica
Sole Net Survey (raziskava mrež za lovljenje morskega lista)	SNS	IVb, IVc	3. četrtletje	morski list, morska plošča
North Sea Sandeels Survey (raziskava prave peščenke v Severnem morju)	NSSS	IVa, IVb	4. četrtletje	prave peščenke
International Ecosystem Survey in the Nordic Seas (mednarodna raziskava ekosistemov v severnih morjih)	ASH	IIa	maj	sled, sinji mol
Redfish Survey in the Norwegian Sea and adjacent waters (raziskava rdečega okuna v Norveškem morju in sosednjih vodah)	REDNOR	II	avgust–september	rdeči okun
Mackerel egg Survey (raziskava iker skuše) (vsaka tri leta)	NSMEGS	IV	maj–julij	gojenje iker skuše
Herring Larvae survey (raziskava mladic sledu)	IHLS	IV,VIId	1. in 3. četrtletje	mladice sledu, papaline
NS Herring Acoustic Survey (sonarna raziskava sledu v Severnem morju)	NHAS	IIIa, IV, VIa	junij, julij	sled, papalina
Nephrops TVsurvey (raziskava škampov) (FU 3&4)	NTV3&4	IIIA	2. in 3. četrtletje	škampi
Nephrops TVsurvey (raziskava škampov) (FU 6)	NTV6	IVb	september	škampi
Nephrops TVsurvey (raziskava škampov) (FU 7)	NTV7	IVa	2. in 3. četrtletje	škampi
Nephrops TVsurvey (raziskava škampov) (FU 8)	NTV8	IVb	2. in 3. četrtletje	škampi
Nephrops TVsurvey (raziskava škampov) (FU 9)	NTV9	IVa	2. in 3. četrtletje	škampi

Naziv raziskave	Kratica	Območje	Obdobje	Glavne ciljne vrste
Severni Atlantik (območja ICES V–XIV in območja NAFO)				
International Redfish Trawl and Acoustic Survey (Biennial) (mednarodna raziskava vlečnih mrež za lov na rdečega okuna in sonarna raziskava (vsaki dve leti))	REDTAS	Va, XII, XIV; NAFO SA 1–3	junij/julij	rdeči okun
Flemish Cap Groundfish survey (raziskava pridnenih rib ob Flemskem rtu)	FCGS	3M	julij	pridnene vrste
Greenland Groundfish survey (raziskava grenlandskih pridnenih rib)	GGS	XIV, NAFO SA1	oktober/ november	trska, rdeči okun in druge pridnene vrste
3LNO Groundfish survey (raziskava pridnenih rib v coni 3LNO)	PLATUXA	NAFO 3LNO	2. in 3. četrtletje	pridnene vrste
Eastern IBTS 4th quarter (vzhodna raziskava IBTS, 4. četrtletje) (including Porcupine survey) (vključno z raziskavo ježevcev)	IBTS Q4	VIa, VII, VIII, IXa	4. četrtletje	pridnene vrste
Scottish Western IBTS (škotska zahodna raziskava IBTS)	IBTS Q1	VIa, VIIa	marec	trska in oslič, sled, skuša
ISBCBTS September (septembrska raziskava ISBCBTS)	ISBCBTS	VIIa f g	september	morski list, morska plošča
WCBTS	VIIe BTS	VIIe	oktober	morski list, morska plošča, morska spaka, rdeči jezik
Blue whiting survey (raziskava sinjega mola)		VI, VII	1. in 2. četrtletje	sinji mol
International Mackerel and Horse Mackerel Egg Survey (mednarodna raziskava iker skuše in šura) (vsaka tri leta)	MEGS	VIa, VII,VIII, IXa	januar–julij	gojenje iker skuše in šura
Sardine, Anchovy Horse Mackerel Acoustic Survey (sonarna raziskava sardele, sardona, šura)		VIII, IX	marec–april–maj	indeksi razširjenosti sardele, sardona, skuše, šura
Sardine DEPM (raziskava DEPM sardele) (vsaka tri leta)		VIIIc, IXa	2. in 4. četrtletje	biomasa drstitvenega staleža sardele in uporaba CUFES
Spawning/Pre spawning Herring/ Boarfish acoustic survey (sonarna raziskava drstenja/preddrstenja sledu/merjaščevke)		VIa, VIIa–g	julij, september, november, marec, januar	sled, papalina
Biomass of Anchovy (biomasa sardona)	BIOMAN	VIII	maj	biomasa drstitvenega staleža sardona (DEP)
Nephrops UWTV survey (offshore) (raziskava UWTV škampov (na morju))	UWTV (FU 11–13)	VIa	2. in 3. četrtletje	škampi

Naziv raziskave	Kratica	Območje	Obdobje	Glavne ciljne vrste
Nephrops UWTV (raziskava UWTV škampov) Irsko morje	UWTV (FU 15)	VIIa	avgust	škampi
Nephrops UWTV survey (raziskava UWTV škampov) Aransko otočje	UWTV (FU 17)	VIIb	junij	škampi
Nephrops UWTV survey (raziskava UWTV škampov) Keltsko morje	UWTV (FU 20-22)	VIIg, h, j	julij	škampi
Nephrops Survey (raziskava škampov) Offshore Portugal NepS (raziskava škampa na morju pri Portugalski)	UWTV (FU 28-29)	IXa	junij	škampi
Sredozemsko morje in Črno morje				
Pan-Mediterranean Acoustic Survey (vsesredozemska sonarna raziskava)	MEDIAS	GSA 1, 6, 7, 9, 10, 15, 16, 17, 18, 20, 22	pomlad–poletje (2. in 3. četrtletje)	majhne pelagične vrste
Bottom trawl survey in Black Sea (raziskava pridnenih vlečnih mrež v Črnem morju)	BTSBS	GSA 29	pomlad–jesen (2., 3. in 4. četrtletje)	romb
Pelagic trawl survey in Black Sea (raziskava pelagičnih vlečnih mrež v Črnem morju)	PTSBS	GSA 29	pomlad–jesen (2., 3. in 4. četrtletje)	papalina in mol
International bottom trawl survey in the Mediterranean (mednarodna raziskava pridnenih vlečnih mrež v Sredozemlju)	MEDITS	GSA 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 22, 23, 25	pomlad–poletje (2. in 3. četrtletje)	pridnene vrste

Tabela 11

Ekonomske in socialne spremenljivke za sektor predelovalne industrije, ki se lahko zbirajo prostovoljno

Skupina spremenljivke	Spremenljivka	Enota
EKONOMSKE SPREMENLJIVKE		
Prihodek	promet	euri
	drugi prihodki	euri
Stroški osebja	stroški osebja	euri
	vrednost neplačanega dela	euri
	plačilo za delavce zunanje agencije (neobvezno)	euri
Stroški energije	stroški energije	euri
Stroški surovin	nakup rib ali drugih surovin za proizvodnjo	euri

Skupina spremenljivke	Spremenljivka	Enota
Drugi operativni stroški	drugi operativni stroški	euri
Subvencije	subvencije za tekoče poslovanje	euri
	subvencije za naložbe	euri
Stroški kapitala	potrošnja stalnega kapitala	euri
Vrednost kapitala	skupna vrednost sredstev	euri
Finančni rezultati	finančni prihodki	euri
	finančni odhodki	euri
Naložbe	neto naložbe	euri
Dolg	dolg	euri
Zaposlovanje	število zaposlenih oseb	število
	nacionalni ekvivalent polnega delovnega časa (EPDČ)	število
	neplačana delovna sila	število
	število opravljenih delovnih ur na zaposlenega in na neplačanega delavca	število
Število podjetij	število podjetij	število
Teža surovin (NEOBVEZNO)	teža surovin na vrsto in poreklo (NEOBVEZNO)	kg

SOCIALNE SPREMENLJIVKE

Zaposlenost po spolu	število
Zaposlenost po starosti	število
Zaposlenost po stopnji izobrazbe	število za vsako stopnjo izobrazbe
Zaposlenost po državljanstvu	število za vsako državo na svetu
Nacionalni ekvivalent polnega delovnega časa (EPDČ)	število

ISSN 1977-0804 (elektronska različica)
ISSN 1725-5155 (tiskana različica)

Urad za publikacije Evropske unije
2985 Luxembourg
LUKSEMBURG

SL