IZVEDBENI SKLEP KOMISIJE (EU) 2023/1795

z dne 10. julija 2023

v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA

(notificirano pod dokumentarno številko C(2023) 4745)

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju 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) ([1]), zlasti člena 45(3) Uredbe,

ob upoštevanju naslednjega:

1. UVOD

(1) Uredba (EU) 2016/679 ([2]) določa pravila o prenosu osebnih podatkov od upravljavcev ali obdelovalcev v Uniji v tretje države in mednarodne organizacije, če taki prenosi spadajo na področje uporabe navedene uredbe. Pravila o mednarodnem prenosu podatkov vsebuje poglavje V navedene uredbe. Čeprav je pretok osebnih podatkov v države zunaj Evropske unije in iz njih ključen za širitev čezmejne trgovine in mednarodnega sodelovanja, je treba zagotoviti, da zaradi takih prenosov v tretje države in mednarodne organizacije ni ogrožena raven varstva osebnih podatkov, ki se zagotavlja v Uniji ([3]).

(2) V skladu s členom 45(3) Uredbe (EU) 2016/679 lahko Komisija z izvedbenim aktom odloči, da tretja država, ozemlje ali en oziroma več določenih sektorjev v tretji državi zagotavlja ustrezno varstvo. Pod tem pogojem se lahko osebni podatki v tretjo državo prenašajo brez dodatnega dovoljenja, kot je določeno v členu 45(1) in uvodni izjavi 103 Uredbe (EU) 2016/679.

(3) Kot je navedeno v členu 45(2) Uredbe (EU) 2016/679, mora sprejetje sklepa o ustreznosti temeljiti na celoviti analizi pravnega reda tretje države, kar vključuje pravila, ki se uporabljajo glede uvoznikov podatkov, ter omejitve in zaščitne ukrepe glede dostopa javnih organov do osebnih podatkov. Komisija mora v oceni ugotoviti, ali zadevna tretja država zagotavlja raven varstva, ki je „v osnovi enakovredna“ tisti, zagotovljeni v Uniji (uvodna izjava 104 Uredbe (EU) 2016/679). Ali je tako, je treba oceniti glede na zakonodajo Unije, predvsem Uredbo (EU) 2016/679, in sodno prakso Sodišča Evropske unije (Sodišče) ([4]).

([1]) (UL L 119, 4.5.2016, str. 1).
([2]) Za večjo preglednost je v Prilogo VIII vključen seznam okrajšav, ki se uporabljajo v tem sklepu.
([3]) Glej uvodno izjavo 101 Uredbe (EU) 2016/679.
([4]) Glej, nazadnje, sodbo z dne 16. julija 2020, Facebook Ireland in Schrems (sodba v zadevi Schrems II), C-311/18, EU:C:2020:559.

(4) Kot je pojasnilo Sodišče Evropske unije v sodbi z dne 6. oktobra 2015, Maximillian Schrems/Data Protection Commissioner ([5]) (v nadaljnjem besedilu: sodba v zadevi Schrems), C-362/14, v ta namen ni nujno, da se ugotovi identična raven varstva. To pomeni zlasti, da se lahko sredstva, ki jih zadevna tretja država uporablja za varstvo osebnih podatkov, razlikujejo od tistih, ki jih uporablja Unija, če se v praksi izkaže, da so učinkovita pri zagotavljanju ustreznega varstva ([6]). Standard ustreznosti torej ne zahteva doslednega posnemanja pravil Unije. Pač pa se prouči, ali tuji sistem kot celota z vsebino pravic do zasebnosti ter njihovim učinkovitim izvajanjem, nadzorom in izvrševanjem zagotavlja zahtevano raven varstva ([7]). Poleg tega bi morala Komisija v skladu z navedeno sodbo pri uporabi tega standarda zlasti oceniti, ali pravni okvir zadevne tretje države zagotavlja predpise, katerih namen je omejiti posege v temeljne pravice posameznikov, katerih podatki se prenašajo iz Unije, ki naj bi jih državni subjekti v tej državi lahko izvajali, kadar poskušajo doseči legitimne cilje, kot je nacionalna varnost, in ali zagotavlja učinkovito pravno varstvo v primeru takih posegov ([8]). Smernice v zvezi s tem zagotavlja tudi „referenčni dokument o ustreznosti“, ki ga je izdal Evropski odbor za varstvo podatkov in v katerem je nadalje pojasnjen ta standard ([9]).

(5) Veljavni standard v zvezi s takim posegom v temeljne pravice do zasebnosti in varstvo podatkov je Sodišče dodatno pojasnilo v svoji sodbi z dne 16. julija 2020 v zadevi Data Protection Commissioner/Facebook Ireland Limited in Maximillian Schrems (v nadaljnjem besedilu: sodba v zadevi Schrems II), C-311/18, s katero je bil razveljavljen Izvedbeni sklep Komisije (EU) 2016/1250 ([10]) o prejšnjem okviru čezatlantskega pretoka podatkov, tj. zasebnostnem ščitu EU-ZDA (zasebnostni ščit). Sodišče je menilo, da omejitve varstva osebnih podatkov, ki izhajajo iz notranje ureditve Združenih držav v zvezi z dostopom in uporabo podatkov, prenesenih iz Unije v Združene države za namene nacionalne varnosti, s strani javnih organov ZDA, niso urejene tako, da bi izpolnjevale zahteve, ki so v bistvu enakovredne zahtevam iz prava Unije glede potrebe in sorazmernosti takih posegov v pravico do varstva podatkov ([11]). Sodišče je tudi menilo, da ni na voljo pravnega sredstva pred organom, ki bi osebam, katerih podatki se prenesejo v Združene države, zagotavljal jamstva, ki so v bistvu enakovredna tistim, ki se zahtevajo s členom 47 Listine o pravici do učinkovitega pravnega sredstva ([12]).

(6) Komisija je po sodbi v zadevi Schrems II začela pogovore z vlado ZDA, da bi se sprejel morebiten nov sklep o ustreznosti varstva, ki bi izpolnjeval zahteve iz člena 45(2) Uredbe (EU) 2016/679, kakor jih razlaga Sodišče. Združene države so na podlagi teh razprav 7. oktobra 2022 sprejele Odredbo št. 14086 „Krepitev zaščitnih ukrepov za obveščevalne dejavnosti SIGINT ZDA“ (Odredba št. 14086), ki jo dopolnjuje uredba o sodišču za presojo varstva podatkov (*Data Protection Review Court*, v nadaljnjem besedilu: DPRC), ki jo je izdal pravosodni minister ZDA (*AG Regulation*, v nadaljnjem besedilu: uredba pravosodnega ministra) ([13]). Poleg tega je bil posodobljen okvir, ki se uporablja za poslovne subjekte, ki obdelujejo podatke, prenesene iz Unije na podlagi sedanjega sklepa – „okvira za varstvo zasebnosti podatkov med EU in ZDA“ (*Data Privacy Framework*, v nadaljnjem besedilu: DPF EU-ZDA ali DPF).

(7) Komisija je podrobno proučila zakonodajo in prakso ZDA, vključno z Odredbo št. 14086 in uredbo pravosodnega ministra. Na podlagi ugotovitev iz uvodnih izjav 9 do 200 Komisija ugotavlja, da ZDA zagotavljajo ustrezno varstvo osebnih podatkov, ki se na podlagi DPF EU-ZDA prenašajo od upravljavca oziroma obdelovalca v Uniji ([14]) certificiranim organizacijam v ZDA.

([5]) Sodba z dne 6. oktobra 2015, Maximillian Schrems/Data Protection Commissioner (v nadaljnjem besedilu: sodba v zadevi Schrems), C-362/14, EU:C:2015:650, točka 73.

([6]) Sodba v zadevi Schrems, točka 74.

([7]) Glej Sporočilo Komisije Evropskemu parlamentu in Svetu: Izmenjava in varstvo osebnih podatkov v globaliziranem svetu (COM (2017) 7 z dne 10. januarja 2017, oddelek 3.1, str. 6 in 7.

([8]) Sodba v zadevi Schrems, točki 88 in 89.

([9]) Evropski odbor za varstvo podatkov, Referenčni dokument o ustreznosti, WP 254 rev. 01, na voljo na povezavi: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

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

([11]) Sodba v zadevi Schrems II, točka 185.

([12]) Sodba v zadevi Schrems II, točka 197.

([13]) Poglavje 28, del 302 Zakonika Združenih držav (*U.S. Code of Federal Regulations*, v nadaljnjem besedilu: CFR).

([14]) Ta sklep velja za EGP. Sporazum o Evropskem gospodarskem prostoru (v nadaljnjem besedilu: Sporazum EGP) določa razširitev notranjega trga Evropske unije na tri države EGP, tj. Islandijo, Lihtenštajn in Norveško. Sklep Skupnega odbora EGP, s katerim je bila Uredba (EU) 2016/679 vključena v Prilogo XI k Sporazumu EGP, je bil sprejet 6. julija 2018, veljati pa je začel 20. julija 2018. Navedeni sporazum torej vključuje tudi Uredbo. Za namene sklepa se torej šteje, da sklici na EU in države članice EU vključujejo tudi države EGP.

(8) Ta sklep pomeni, da za prenos osebnih podatkov od upravljavcev in obdelovalcev v Uniji ([15]) certificiranim organizacijam v ZDA ni treba pridobiti nobenega dodatnega dovoljenja. Ne vpliva na neposredno uporabo Uredbe (EU) 2016/679 za take organizacije, če so izpolnjeni pogoji glede ozemeljske veljavnosti navedene uredbe iz njenega člena 3.

2. OKVIR ZA VARSTVO ZASEBNOSTI PODATKOV MED EU IN ZDA

2.1 Osebno in stvarno področje uporabe

2.1.1 *Certificirane organizacije*

(9) DPF EU-ZDA temelji na sistemu certificiranja, s katerim se organizacije v ZDA zavežejo sklopu načel zasebnosti, tj. „načelom okvira za varstvo zasebnosti podatkov med EU in ZDA“, vključno z dodatnimi načeli (v nadaljnjem besedilu skupaj: načela), ki jih je izdalo Ministrstvo za trgovino ZDA (*Department of Commerce*, v nadaljnjem besedilu: ministrstvo za trgovino) in jih vsebuje Priloga I k temu sklepu ([16]). Da bi bila organizacija upravičena do certificiranja na podlagi DPF EU-ZDA, morajo zanjo veljati preiskovalna in izvršilna pooblastila Zvezne komisije za trgovino (*Federal Trade Commission*, v nadaljnjem besedilu: FTC) ali Ministrstva za promet ZDA (*Department of Transportation*, v nadaljnjem besedilu: ministrstvo za promet) ([17]). Načela zasebnosti začnejo veljati takoj po certificiranju. Kot je podrobneje pojasnjeno v uvodnih izjavah 48 do 52, se od organizacij v DPF EU-ZDA zahteva, da vsako leto znova potrdijo svojo zavezanost načelom ([18]).

2.1.2 *Opredelitev pojma osebni podatki ter pojmov upravljavec in „posrednik“*

(10) Varstvo, ki ga zagotavlja DPF EU-ZDA, se uporablja za vse osebne podatke, ki se prenašajo iz Unije organizacijam v ZDA, ki so certificirale svojo zavezanost načelom pri ministrstvu za trgovino, razen podatkov, ki se zbirajo za objavo v časopisu ali po radiu in televiziji ali za drugo obliko javnega sporočanja novinarskega gradiva in informacij v predhodno objavljenem gradivu, razširjenem iz medijskih arhivov ([19]). Takih informacij zato ni mogoče prenašati na podlagi DPF EU-ZDA.

(11) V načelih so osebni podatki/osebne informacije opredeljeni enako kot v Uredbi (EU) 2016/679, tj. kot „podatki o določenem ali določljivem posamezniku, ki so zapisani v kateri koli obliki in spadajo na področje uporabe Splošne uredbe o varstvu podatkov ter jih organizacije v ZDA prejmejo iz Evropske unije“ ([20]). Zato zajemajo tudi psevdonimizirane (ali „kodirane s šifrirnim ključem“) raziskovalne podatke (tudi če ključ ni izmenjan s prejemno organizacijo v ZDA) ([21]). Podobno je pojem obdelave opredeljen kot „vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje ali razširjanje in izbris ali uničenje“ ([22]).

(12) DPF EU-ZDA se uporablja za organizacije v ZDA, ki se štejejo za upravljavce (tj. osebo ali organizacijo, ki sama ali v sodelovanju z drugimi določa namene in sredstva obdelave osebnih podatkov) ([23]), ali obdelovalce (tj. posrednike, ki delujejo v imenu upravljavca) ([24]). Obdelovalci v ZDA morajo biti pogodbeno zavezani, da delujejo samo po

([15]) Ta sklep ne vpliva na zahteve Uredbe (EU) 2016/679, ki se uporabljajo za subjekte (upravljavce in obdelovalce) v Uniji, ki prenašajo podatke, na primer glede omejitve namena, najmanjšega obsega podatkov, preglednosti in varnosti podatkov (glej tudi člen 44 Uredbe (EU) 2016/679).

([16]) V zvezi s tem glej sodbo v zadevi Schrems, točka 81, kjer je Sodišče potrdilo, da lahko sistem samocertificiranja zagotavlja ustrezno varstvo.

([17]) Priloga I, člen I.2. FTC ima široko pristojnost glede trgovinskih dejavnosti, z nekaterimi izjemami, npr. v zvezi z bankami, letalskimi prevozniki, zavarovalništvom in dejavnostmi splošnih telekomunikacijskih operaterjev (čeprav je bilo z odločbo pritožbenega sodišča ZDA za deveto okrožje z dne 26. februarja 2018 v zadevi FTC proti AT &T potrjeno, da je FTC pristojna za nesplošne dejavnosti takih subjektov). Glej tudi Prilogo IV, opomba 2. Ministrstvo za promet je pristojno za zagotavljanje skladnosti letalskih prevoznikov in agentov za prodajo vozovnic (za prodajo letalski prevoz), glej Prilogo V, oddelek A.

([18]) Priloga I, člen III.6.

([19]) Priloga I, člen III.2.

([20]) Priloga I, člen I.8.a.

([21]) Priloga I, člen III.14.g.

([22]) Priloga I, člen I.8.b.

([23]) Priloga I, člen I.8.c.

([24]) Glej npr. oddelek II.2.b ter oddelek II.3.b in 7.d, Priloge I, v katerih je pojasnjeno, da posredniki delujejo v imenu upravljavca v skladu z njegovimi navodili in posebnimi pogodbenimi obveznostmi.

navodilih upravljavca EU, kateremu pomagajo pri odgovorih posameznikom, ki uveljavljajo svoje pravice po načelih ([25]). Poleg tega mora obdelovalec v primeru podobdelave skleniti pogodbo s podobdelovalcem, ki zagotavlja enako raven varstva, kot jo zagotavljajo načela, in sprejeti ukrepe za zagotovitev njenega pravilnega izvajanja ([26]).

2.2 **Načela okvira za varstvo zasebnosti podatkov med EU in ZDA**

2.2.1 ***Omejitev namena in možnost izbire***

(13) Osebni podatki bi se morali obdelovati zakonito in pošteno. Zbirati bi se morali za določen namen in se nato uporabljati samo, če to ni nezdružljivo z namenom obdelave.

(14) Na podlagi DPF EU-ZDA je to zagotovljeno z različnimi načeli. Prvič, podobno kot na podlagi člena 5(1), točka (b), Uredbe (EU) 2016/679 organizacija na podlagi *načela o celovitosti podatkov in omejitve namena* ne sme obdelovati osebnih podatkov na način, ki ni združljiv z namenom, za katerega so bili podatki prvotno zbrani ali ki ga je posameznik, na katerega se nanašajo osebni podatki, naknadno odobril ([27]).

(15) Drugič, organizacija mora pred uporabo osebnih podatkov za nov (spremenjen) namen, ki je bistveno drugačen, vendar še vedno združljiv s prvotnim namenom, ali njihovim razkritjem tretji stranki v skladu z *načelom možnosti izbire* ([28]) posameznikom, na katere se nanašajo osebni podatki, z jasnim, razumljivim in dostopnim postopkom zagotoviti možnost ugovora (zavrnitve). Pomembno je, da to načelo ne nadomešča izrecne prepovedi nezdružljive obdelave ([29]).

([25]) Priloga I, člen III.10.a. Glej tudi smernice, ki jih je ministrstvo za trgovino pripravilo ob posvetovanju z Evropskim odborom za varstvo podatkov v okviru zasebnostnega ščita in v katerih so pojasnjene obveznosti obdelovalcev iz ZDA, ki prejmejo podatke iz Unije v navedenem okviru. Ker se ta pravila niso spremenila, so te smernice/pogosta vprašanja še vedno relevantni za DPF EU-ZDA (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Priloga I, člen II.3.b.

([27]) Priloga I, člen II.5.a. Združljivi nameni lahko vključujejo revizijo, preprečevanje goljufij ali druge namene, skladne s pričakovanji razumne osebe glede na kontekst zbiranja (glej Prilogo I, opomba 6).

([28]) Priloga I, člen II.2.a. To ne velja, če organizacija zagotavlja osebne podatke obdelovalcu, ki deluje v njenem imenu in na podlagi njenih navodil (Priloga I, člen II.2.b). Kljub temu mora organizacija imeti v tem primeru sklenjeno pogodbo in zagotoviti skladnost z načelom *odgovornosti za prenos tretjemu*, kot je podrobneje pojasnjeno v uvodni izjavi 43. Poleg tega je lahko načelo *možnosti izbire* (in tudi načelo *obvestila*) omejeno, če se osebni podatki obdelujejo v okviru skrbnega pregleda (v okviru morebitne združitve ali prevzema) ali revizij, in sicer v obsegu in tako dolgo, kot je potrebno, da se zadosti zakonskim ali javnim interesom, ali kolikor in dokler bi uporaba teh načel škodovala zakonitim interesom organizacije v konkretnem okviru preiskav na podlagi skrbnega pregleda ali revizij (Priloga I, člen III.4). Dopolnilno načelo 15 (Priloga I, člen III.15.a in b) prav tako določa izjemo od načela *možnosti izbire* (in tudi načel *obvestila* in *odgovornosti za prenos tretjemu*) za osebne podatke iz javno dostopnih virov (razen če izvoznik podatkov v EU navede, da za podatke veljajo omejitve, ki zahtevajo uporabo navedenih načel) ali za osebne podatke, zbrane iz evidenc, ki so odprte na vpogled širši javnosti (razen če so povezani s podatki iz evidenc, ki niso javne, in če se spoštujejo vsi pogoji glede vpogleda v podatke). Podobno dopolnilno načelo 14 (Priloga I, člen III.14.f) določa izjemo od načela *možnosti izbire* (in tudi načel *obvestila* in *odgovornosti za prenos tretjemu*) za obdelavo osebnih podatkov s strani podjetja za farmacevtske ali medicinske pripomočke za spremljanje varnosti in učinkovitosti njegovih izdelkov, če spoštovanje načel posega v izpolnjevanje zakonskih zahtev.

([29]) To velja za vse prenose podatkov na podlagi DPF EU-ZDA, tudi če se ti nanašajo na podatke, zbrane v zaposlitvenem razmerju. Čeprav lahko zato certificirana 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*. Izjemoma lahko organizacija uporablja osebne podatke za dodaten združljiv namen, ne da bi zagotovila *obvestilo* in *možnost izbire*, vendar le v obsegu in za obdobje, ki sta potrebna za preprečitev oškodovanja zmožnosti organizacije pri odločitvah o napredovanju delavcev, imenovanjih in drugih podobnih zaposlitvenih odločitvah (glej Prilogo I, oddelek III.9.b.(iv)). 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. Glej Prilogo I, člen III.9.b.(i).

2.2.2 ***Obdelava posebnih vrst osebnih podatkov***

(16) Pri obdelavi posebnih vrst podatkov bi morali veljati posebni zaščitni ukrepi.

(17) V skladu z *načelom možnosti izbire* se za obdelavo „občutljivih podatkov“, tj. osebnih podatkov, ki določajo zdravniško in zdravstveno stanje, rasno in etnično pripadnost, politična, verska in filozofska prepričanja, sindikalno članstvo, podatkov o spolnem življenju posameznika ali katerih koli drugih informacij, prejetih od tretje stranke, ki jih navedena stranka identificira in obravnava kot občutljive, uporabljajo posebni zaščitni ukrepi ([30]). To pomeni, da bodo certificirane organizacije vse podatke, ki se na podlagi prava Unije o varstvu podatkov štejejo za občutljive (vključno s podatki o spolni usmerjenosti, genetskimi podatki in biometričnimi podatki), na podlagi DPF EU-ZDA obravnavale kot občutljive.

(18) Praviloma morajo organizacije za uporabo občutljivih podatkov za namene, ki niso nameni, za katere so bili prvotno zbrani ali ki jih je posameznik naknadno odobril (tj. s privolitvijo), ali za njihovo razkritje tretjim strankam od posameznikov pridobiti izrecno pritrdilno soglasje (privolitev) ([31]).

(19) Takega soglasja ni treba pridobiti v omejenih okoliščinah, ki so podobne izjemam, določenim na podlagi prava Unije o varstvu podatkov ali primerljive z njimi, tj. če je obdelava občutljivih podatkov v življenjskem interesu osebe, potrebna za uveljavitev pravnih zahtevkov ali nujna za zagotovitev zdravstvene nege ali diagnoze ([32]).

2.2.3 ***Točnost, najmanjši obseg in varnost podatkov***

(20) Podatki bi morali biti točni in po potrebi posodobljeni. Prav tako bi morali biti osebni podatki ustrezni, relevantni ter ne bi smeli presegati namenov, za katere se obdelujejo; načeloma se jih ne bi smelo hraniti dlje, kot je potrebno za namene, za katere se obdelujejo.

(21) V skladu z *načelom celovitosti podatkov in omejitve namena* ([33]) morajo biti osebni podatki omejeni na tisto, kar je pomembno za obdelavo. Organizacije morajo prav tako v obsegu, potrebnem za namene obdelave, z ustreznimi ukrepi zagotoviti, da so podatki zanesljivi za nameravano uporabo, točni, popolni in trenutni.

(22) Poleg tega se lahko osebni podatki hranijo v obliki, ki omogoča identifikacijo posameznika (in s tem v obliki osebnih podatkov) ([34]), le dokler služijo namenom, za katere so bili prvotno zbrani ali ki jih je posameznik v skladu z *načelom možnosti izbire* naknadno odobril. Ta obveznost organizacijam ne preprečuje nadaljnje obdelave osebnih podatkov za daljša obdobja, temveč le za obdobje in v obsegu, v katerih se taka obdelava razumno uporablja za enega od naslednjih posebnih namenov, ki so podobni izjemam na podlagi prava Unije o varstvu podatkov ali primerljivi z njimi: arhiviranje v javnem interesu, novinarstvo, literaturo in umetnost, znanstvene in zgodovinske raziskave ter statistično analizo ([35]). Če se osebni podatki hranijo za enega od teh namenov, je njihova obdelava predmet zaščitnih ukrepov v skladu z načeli ([36]).

(23) Osebne podatke je treba obdelovati tudi tako, da je zagotovljena njihova varnost, vključno z varstvom pred nepooblaščeno ali nezakonito obdelavo in pred nenamerno izgubo, uničenjem ali poškodovanjem. Zato bi morali upravljavci in obdelovalci sprejeti ustrezne tehnične ali organizacijske ukrepe za varstvo osebnih podatkov pred morebitnimi grožnjami. Pri ocenjevanju teh ukrepov bi bilo treba upoštevati najnovejše znanstvene dosežke, s tem povezane stroške ter naravo, obseg, kontekst in namen obdelave, pa tudi tveganja za pravice posameznikov.

([30]) Priloga I, člen II.2.c.
([31]) Priloga I, člen II.2.c.
([32]) Priloga I, člen III.1.
([33]) Priloga I, člen II.5.
([34]) Glej Prilogo I, opomba 7, kjer je pojasnjeno, da se posameznik šteje za „določljivega“, če bi lahko organizacija ali tretja stranka navedenega posameznika glede na sredstva za identifikacijo, ki bodo pričakovano uporabljena, (ob upoštevanju, med drugim, stroškov in časa, potrebnega za identifikacijo, ter razpoložljive tehnologije v času obdelave) razumno prepoznala.
([35]) Priloga I, člen II.5.b.
([36]) *Prav tam*.

(24) Na podlagi DPF EU-ZDA se to zagotavlja z *načelom varnosti*, ki podobno kot člen 32 Uredbe (EU) 2016/679 določa, da je treba glede na tveganja, ki jih vključujeta obdelava in narava podatkov, sprejeti razumne in ustrezne varnostne ukrepe ([37]).

2.2.4 ***Preglednost***

(25) Posamezniki, na katere se nanašajo osebni podatki, morajo biti obveščeni o glavnih značilnostih obdelave svojih osebnih podatkov.

(26) To se zagotavlja z *načelom obvestila* ([38]), s katerim se podobno kot z zahtevami glede preglednosti na podlagi Uredbe (EU) 2016/679 od organizacij zahteva, da posameznike, na katere se nanašajo osebni podatki, med drugim obvestijo o (i) sodelovanju organizacije v DPF, (ii) vrsti zbranih podatkov, (iii) namenu obdelave, (iv) vrsti ali identiteti tretjih strank, ki jim bodo morda razkriti osebni podatki, in namenih takega razkritja, (v) njihovih pravicah posameznikov, (vi) načinu vzpostavitve stika z organizacijo ter (vii) razpoložljivih možnostih pravnih sredstev.

(27) To obvestilo mora biti jasno in nedvoumno, ko so posamezniki prvič zaprošeni za zagotovitev osebnih podatkov ali kakor hitro je izvedljivo za tem, v vsakem primeru pa pred uporabo podatkov za bistveno drugačne (vendar združljive) namene, ki niso tisti, za katere so bili prvotno zbrani, ali pred njihovim razkrijem tretji stranki ([39]).

(28) Poleg tega morajo organizacije svoje politike zasebnosti, ki izražajo načela, objaviti (ali jih v primeru podatkov o človeških virih takoj dati na voljo zadevnim posameznikom) ter navesti povezave na spletišče ministrstva za trgovino (s podrobnejšimi informacijami o certificiranju, pravicah posameznikov, na katere se nanašajo osebni podatki, razpoložljivih pritožbenih mehanizmih), seznam sodelujočih organizacij, vključenih v okvir za varstvo zasebnosti podatkov (seznam DPF), in spletišče ustreznega organa za alternativno reševanje sporov ([40]).

2.2.5 ***Pravice posameznikov***

(29) Posamezniki, na katere se nanašajo osebni podatki, bi morali imeti določene pravice, ki jih lahko uresničujejo zoper upravljavca ali obdelovalca, zlasti pravico do dostopa do podatkov, pravico ugovarjati obdelavi in pravico do popravka in izbrisa podatkov.

(30) V DPF EU-ZDA zagotavlja take pravice posameznikom *načelo dostopa* ([41]). Zlasti imajo posamezniki, na katere se nanašajo osebni podatki, pravico, da brez utemeljitve od organizacije pridobijo potrditev, da organizacija obdeluje osebne podatke, povezane z njimi, da jim podatke sporoči v razumnem času in da pridobijo informacije o namenu obdelave, kategorijah osebnih podatkov, ki se obdelujejo, in o prejemnikih (kategorijah), ki se jim podatki razkrijejo ([42]). Organizacije se morajo na zahteve za dostop odzvati v razumnem roku ([43]). Organizacija lahko postavi razumne omejitve glede številka poskusov v določenem obdobju, v katerem bodo izpolnjene zahteve za

([37]) Priloga I, člen II.4.a. Poleg tega DPF EU-ZDA v zvezi s podatki o človeških virih zahteva, da delodajalci ustrežejo prednostnim pravicam zaposlenih do zasebnosti z omejitvijo dostopa do osebnih podatkov, anonimizacijo nekaterih podatkov ali dodelitvijo kod ali psevdonimov (Priloga I, člen III.9.b.(iii)).

([38]) Priloga I, člen II.1.

([39]) Priloga I, člen II.1.b. Dopolnilno načelo 14 (Priloga I, člen III.14.b in c) določa posebne določbe za obdelavo osebnih podatkov v okviru zdravstvenih raziskav in kliničnih poskusov. To načelo organizacijam zlasti omogoča, da obdelujejo podatke kliničnih poskusov celo po umiku osebe iz poskusa, če je to bilo jasno navedeno v obvestilu, predloženem v trenutku, ko je posameznik privolil v sodelovanje. Podobno velja, kadar organizacija v DPF EU-ZDA prejme osebne podatke za namene zdravstvenih raziskav, saj jih lahko v skladu z načeli *obvestila* in *možnosti izbire* uporabi le za novo raziskovalno dejavnost. V tem primeru bi morale biti v obvestilu posamezniku načeloma zagotovljene informacije o morebitnih prihodnjih posebnih uporabah podatkov (npr. povezane študije). Če že od začetka ni mogoče vključiti vseh prihodnjih uporab podatkov (ker lahko uporaba podatkov za novo raziskavo izhaja iz novega razumevanja ali razvoja na področju medicine/raziskav), je treba vključiti pojasnilo, da se podatki v prihodnosti morda uporabijo za nepredvidene medicinske in farmacevtske raziskave. Če taka nadaljnja uporaba ni skladna s splošnimi raziskovalnimi nameni, za katere so bili podatki zbrani (tj. če so novi nameni bistveno drugačni, vendar še vedno združljivi s prvotnim namenom, glej uvodni izjavi 14 in 15), je treba pridobiti novo soglasje (tj. privolitev). Glej poleg tega posebne omejitve načela *obvestila* / izjeme od njega, opisane v opombi 28.

([40]) Priloga I, člen III.6.d.

([41]) Glej tudi dopolnilno načelo o dostopu (Priloga I, člen III.8).

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

([43]) Priloga I, člen III.8.i.

dostop nekega posameznika, in lahko zaračuna pristojbino, ki ni pretirano visoka, npr. kadar so zahteve očitno previsoke, zlasti zaradi njihove ponavljajoče se narave ([44]).

(31) Pravico dostopa do osebnih podatkov je mogoče omejiti v izjemnih okoliščinah, ki so podobne okoliščinam, določenim na podlagi prava Unije o varstvu podatkov, zlasti kadar bi bile kršene zakonite pravice drugih, kadar bi bili stroški ali izdatki za zagotovitev dostopa nesorazmerni s tveganji za zasebnost posameznika zadevnem primeru (čeprav izdatki in stroški niso prevladujoči dejavniki pri ugotavljanju, ali je zagotovitev dostopa razumna ali ne), kadar obstaja verjetnost, da bi razkritje podatkov poseglo v zaščito pomembnih nasprotujočih si javnih interesov, kot so nacionalna varnost, javna varnost ali obramba, kadar podatki vsebujejo zaupno tržno informacijo ali pa se podatki obdelujejo izključno za namene raziskav in statistike ([45]). Vsako zanikanje ali omejitev pravice je treba nujno in ustrezno utemeljiti, pri čemer mora organizacija dokazati, da so te zahteve izpolnjene ([46]). Organizacija mora pri tej presoji upoštevati zlasti interese posameznika ([47]). Če je mogoče informacijo ločiti od drugih podatkov, za katere se uporablja omejitev, mora organizacija prekriti zaščiteno informacijo in dati na voljo preostale podatke ([48]).

(32) Poleg tega imajo posamezniki, na katere se nanašajo osebni podatki, pravico, da dosežejo popravo ali spremembo netočnih podatkov ter izbris podatkov, ki so bili obdelani v nasprotju z načeli ([49]). Kot je pojasnjeno v uvodni izjavi 15, imajo posamezniki poleg tega pravico, da nasprotujejo obdelavi / zavrnejo obdelavo svojih podatkov za namene, ki se bistveno razlikujejo od namenov, za katere so bili podatki zbrani (vendar so združljivi z njimi), in da nasprotujejo razkritju / zavrnejo razkritje svojih podatkov tretjim strankam. Če se osebni podatki uporabljajo za namene neposrednega trženja, imajo posamezniki splošno pravico, da obdelavo kadar koli zavrnejo ([50]).

(33) V načelih niso izrecno obravnavane odločitve, ki vplivajo na posameznika, na katerega se nanašajo osebni podatki, na podlagi izključno samodejne obdelave osebnih podatkov. Vendar glede osebnih podatkov, zbranih v Uniji, velja, da vse odločitve, ki temeljijo na samodejni obdelavi, po navadi sprejme upravljavec v Uniji (ki ima neposredno razmerje z zadevnim posameznikom, na katerega se nanašajo osebni podatki), zato se zanj neposredno uporablja Uredba (EU) 2016/679 ([51]). To vključuje tudi primere prenosa, ko obdelavo izvaja tuji (npr. ameriški) poslovni subjekt, ki deluje kot zastopnik (obdelovalec) v imenu upravljavca iz Unije (ali kot podobdelovalec, ki deluje v imenu obdelovalca iz Unije, ta pa je podatke prejel od upravljavca podatkov iz Unije, ki jih je zbral) in nato na tej podlagi sprejme odločitev.

(34) To je bilo potrjeno s študijo, ki jo je Komisija naročila leta 2018 v okviru drugega letnega pregleda delovanja zasebnostnega ščita ([52]), v kateri je bilo ugotovljeno, da takrat ni bilo nobenega dokaza, da samodejno odločanje običajno izvajajo organizacije v zasebnostnem ščitu na podlagi osebnih podatkov, ki se prenašajo v okviru zasebnostnega ščita.

([44]) Priloga I, člen III.8.f.(i)–(ii) in g.

([45]) Priloga I, člen III.4; 8.b, c in e; 14.e, f in 15.d.

([46]) Priloga I, člen III.8.e.(ii). Organizacija mora posameznika obvestiti o razlogih za zavrnitev/omejitev in mu zagotoviti kontaktno točko za dajanje vseh nadaljnjih informacij, člen III.8.a.(iii).

([47]) Priloga I, člen III.8.a.(ii)–(iii).

([48]) Priloga I, člen III.8.a.(i).

([49]) Priloga I, člen II.6 in III.8.a.(i).

([50]) Priloga I, člen III.8.12.

([51]) Nasprotno pa velja, da so izjemni primeri, ko ima organizacija v ZDA neposreden odnos s posameznikom, na katerega se nanašajo osebni podatki, v Uniji, po navadi posledica tega, da se je navedena organizacija ciljno usmerila na posameznika v Uniji s ponujanjem blaga ali storitev ali s spremljanjem njegovega vedenja. V takem primeru se za samo organizacijo v ZDA uporablja Uredba (EU) 2016/679 (člen 3(2)), zato mora neposredno zagotoviti skladnost s pravom Unije o varstvu podatkov.

([52]) (SWD(2018) 497 final, oddelek 4.1.5). Študija je bila usmerjena v (i) obseg, v katerem organizacije v ZDA, ki so v zasebnostnem ščitu, sprejemajo odločitve, ki vplivajo na posameznike na podlagi samodejne obdelave osebnih podatkov, ki jih prenašajo podjetja v EU v okviru zasebnostnega ščita, ter (ii) zaščitne ukrepe za posameznike, ki jih ameriški zvezni zakon določa za to vrsto primerov, in pogoje uporabe teh zaščitnih ukrepov.

(35) Na področjih, kjer podjetja najverjetneje uporabljajo samodejno obdelavo osebnih podatkov za sprejemanje odločitev, ki vplivajo na posameznika (npr. dajanje posojil, nudenje hipotek, zaposlovanje, stanovanja in zavarovanje), zakonodaja ZDA vsekakor zagotavlja posebno varstvo pred zavrnilnimi odločitvami ([53]). 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 pravnih sredstev. Na področju potrošniških kreditov zakon o poštenem kreditnem poročanju (*Fair Credit Reporting Act*, v nadaljnjem besedilu: FCRA) in zakon o enakih možnostih pridobitve posojila (*Equal Credit Opportunity Act*, v nadaljnjem besedilu: ECOA) vsebujeta zaščitne ukrepe, ki potrošnikom zagotavljajo nekakšno pravico do pojasnila in pravico do izpodbijanja odločitve. Ta zakona sta pomembna na najrazličnejših področjih, vključno s krediti, zaposlovanjem, stanovanji in zavarovanjem. Poleg tega nekateri protidiskriminacijski zakoni, kot sta naslov VII zakona o državljanskih pravicah (*Civil Rights Act*) in zakon proti diskriminaciji v zvezi s prodajo in z najemom stanovanj in hiš (*Fair Housing Act*, v nadaljevanju: FHA), posameznikom zagotavljajo varstvo v zvezi z modeli, ki se uporabljajo pri samodejnem odločanju, ki bi lahko povzročili diskriminacijo na podlagi nekaterih značilnosti, in jih podeljujejo pravice do izpodbijanja takih odločitev, vključno s samodejnimi. Kar zadeva informacije o zdravstvenem stanju, pravilo o zasebnosti iz zakona o prenosljivosti zdravstvenega zavarovanja in odgovornostih pri njem (*Health Insurance Portability and Accountability Act*, v nadaljnjem besedilu: HIPAA) vzpostavlja nekatere pravice, podobne pravicam iz Uredbe (EU) 2016/679 v zvezi z dostopom do osebnih informacij o zdravstvenem stanju. Poleg tega smernice organov ZDA vsebujejo zahtevo, da izvajalci zdravstvenih storitev prejmejo informacije, ki jim omogočajo, da posameznike obvestijo o sistemih samodejnega odločanja, ki se uporabljajo v medicinskem sektorju ([54]).

(36) Ta pravila zato zagotavljajo varstvo, ki je podobno varstvu na podlagi prava Unije o varstvu podatkov v malo verjetnem primeru, v katerem bi odločitve sprejemala sama organizacija v DPF EU-ZDA.

2.2.6 ***Omejitve nadaljnjih prenosov podatkov***

(37) Raven varstva, zagotovljena osebnim podatkom, ki se iz Unije prenesejo v organizacije v ZDA, se z nadaljnjim prenosom takih podatkov prejemniku v Združenih državah ali v drugi državi ne sme poslabšati.

(38) Na podlagi *načela odgovornosti za prenos tretjemu* ([55]) se uporabljajo posebna pravila za tako imenovane prenose tretjemu, tj. prenose osebnih podatkov z organizacije v DPF EU-ZDA na tretjega upravljavca ali obdelovalca, ne glede na to, ali je ta v ZDA ali tretji državi zunaj ZDA (in Unije). Kakršen koli prenos tretjemu se lahko izvaja samo (i) za omejene in določene namene, (ii) na podlagi pogodbe med organizacijo v DPF EU-ZDA in tretjo stranko ([56]) (ali primerljivega dogovora v skupini podjetij ([57])) in (iii) samo, če navedena pogodba zagotavlja tretji stranki enako raven varstva, kot jo zagotavljajo načela.

(39) Ta obveznost glede zagotavljanja enake ravni varstva, kot jo zagotavljajo načela, v povezavi z *načelom celovitosti podatkov in omejitve namena* zlasti pomeni, 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 (v skladu z *načelom možnosti izbire*).

([53]) Glej na primer zakon o enakih možnostih pridobitve posojila (*Equal Credit Opportunity Act*) (člen 1691 in naslednji naslova 15 zakonodajne zbirke ZDA), zakon o pravičnem poročanju o kreditni sposobnosti (*Fair Credit Reporting Act*) (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*) (člen 3601 in naslednji naslova 42 zakonodajne zbirke ZDA). Poleg tega so se Združene države zavezale načelom Organizacije za gospodarsko sodelovanje in razvoj o umetni inteligenci, ki med drugim vključujejo načela o preglednosti ter pojasnjujejo zmožnost, varnost in odgovornost.

([54]) Glej na primer smernice, ki so na voljo na naslovu „2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans?“ (2042-Do katerih osebnih informacij o zdravstvenem stanju pri ponudnikih zdravstvenih storitev in v načrtih javnega zdravja imajo posamezniki pravico dostopati na podlagi HIPAA?) | HHS.gov.

([55]) Glej Prilogo I, člen II.3 in dopolnilno načelo o obveznih pogodbah za prenos tretjemu (Priloga I, člen III.10).

([56]) Kot izjema od tega splošnega načela lahko organizacija tretjemu prenaša osebne podatke majhnega števila zaposlenih, ne da bi s prejemnikom sklenila pogodbo za občasne potrebe, povezane z zaposlovanjem, npr. rezervacija leta, hotelske sobe ali zavarovalno kritje. Vendar mora organizacija tudi v tem primeru izpolnjevati načeli *obvestila* in *možnosti izbire* (glej Prilogo I, člen III.9.e).

([57]) Glej dopolnilno načelo o obveznih pogodbah za prenos tretjemu (Priloga I, 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 certificirane organizacije v ZDA še vedno odgovorne za skladnost z načeli, zagotavljalo močno spodbudo za uporabo instrumentov, ki so dejansko učinkoviti v praksi.

(40) *Načelo odgovornosti za prenos tretjemu* bi bilo treba razlagati tudi v povezavi z *načelom obvestila* in, v primeru prenosa tretjemu upravljavcu ([58]), z *načelom možnosti 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 in možnostih izbire, ter lahko nasprotujejo prenosom tretjemu (oziroma jih zavrnejo) ali morajo, v primeru občutljivih podatkov, dati „izrecno pritrdilno soglasje“ (privolitev) za prenos tretjemu.

(41) 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.

(42) V vseh primerih mora biti v pogodbi s tretjim prejemnikom določeno, da bo ta obvestil organizacijo v DPF EU-ZDA, če bo ugotovil, da ne more več izpolnjevati te obveznosti. V primeru take ugotovitve se mora obdelava s strani tretje stranke prenehati, ali pa je treba sprejeti druge razumne in ustrezne ukrepe za izboljšanje stanja ([59]).

(43) Dodatno varstvo se uporablja v primeru prenosa tretjemu posredniku (tj. obdelovalec). V takem primeru mora organizacija v ZDA zagotoviti, da posrednik deluje po njenih navodilih, in 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 ([60]). Ministrstvo za trgovino lahko od organizacije zahteva, naj zagotovi povzetek ali reprezentativni izvod določb o zasebnosti iz pogodbe ([61]). Kadar se v verigi (pod)obdelave pojavijo težave glede skladnosti, bo načeloma organizacija, ki deluje kot upravljavec osebnih podatkov, prevzela odgovornost, kot je navedeno v *načelu pritožbenega mehanizma, izvrševanja in odgovornosti*, razen če dokaže, da ni odgovorna za dogodek, ki povzroča škodo ([62]).

2.2.7 ***Odgovornost***

(44) V skladu z načelom odgovornosti morajo subjekti, ki obdelujejo podatke, sprejeti ustrezne tehnične in organizacijske ukrepe, da lahko uspešno izpolnjujejo svoje obveznosti glede varstva podatkov in dokažejo tako izpolnjevanje, predvsem pristojnim nadzornim organom.

(45) Ko se organizacija prostovoljno odloči za certificiranje ([63]) v na podlagi DPF EU-ZDA, je njeno dejansko izpolnjevanje načel obvezno in izvršljivo. Na podlagi *načela pritožbenega mehanizma, izvrševanja in odgovornosti* ([64]) morajo organizacije v DPF EU-ZDA zagotoviti učinkovite mehanizme za zagotovitev skladnosti z načeli. Organizacije morajo sprejeti tudi ukrepe za preverjanje ([65]), ali so njihove politike zasebnosti skladne z načeli in ali dejansko ravnajo v skladu z njimi. To se lahko izvede s sistemom samoocenjevanja, ki mora vključevati notranje postopke, ki zagotavljajo, da so zaposleni deležni usposabljanja o izvajanju politik organizacije glede zasebnosti in da se skladnost redno objektivno preverja, ali, pri zunanjih pregledih skladnosti, z metodami, ki lahko vključujejo revizijo, naključne preglede ali uporabo tehnoloških orodij.

([58]) 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.

([59]) 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 DPF EU-ZDA, ki nadzoruje obdelavo in po katere navodilih deluje posrednik. Glej Prilogo I, člen II.3.

([60]) Priloga I, člen II.3.b.

([61]) *Prav tam*.

([62]) Priloga I, člen II.7.d.

([63]) Glej tudi dopolnilno načelo o samocertificiranju (Priloga I, člen III.6).

([64]) Glej tudi dopolnilno načelo o reševanju sporov in izvrševanju (Priloga I, člen III.11).

([65]) Glej tudi dopolnilno načelo o preverjanju (Priloga I, člen III.7).

(46) Poleg tega morajo organizacije voditi evidenco o svojem izvajanju praks na podlagi DPF EU-ZDA in jo na zahtevo v okviru preiskave ali pritožbe zaradi neskladnosti dati na voljo neodvisnemu organu za reševanje sporov ali pristojnemu izvršnemu organu ([66]).

2.3 **Upravljanje, nadzor in izvrševanje**

(47) DPF EU-ZDA bo upravljalo in spremljalo ministrstvo za trgovino. Okvir zagotavlja mehanizme nadzora in izvrševanja za preverjanje in zagotavljanje, da organizacije v DPF EU-ZDA spoštujejo načela in da se obravnava vsako nespoštovanje načel. Ti mehanizmi so določeni v načelih (Priloga I) ter zavezah ministrstva za trgovino (Priloga III), FTC (Priloga IV) in ministrstva za promet (Priloga V).

2.3.1 ***Ponovno certificiranje***

(48) Za certificiranje na podlagi DPF EU-ZDA (ali vsakoletno ponovno certificiranje) se morajo organizacije javno zavezati spoštovanju načel, dati na voljo svoje politike zasebnosti in jih v celoti izvajati ([67]). V okviru svoje vloge za (ponovno) certificiranje morajo organizacije ministrstvu za trgovino predložiti informacije, med drugim o imenu zadevne organizacije, opisu namenov, za katere bo organizacija obdelovala osebne podatke, osebnih podatkih, ki jih bo zajemalo certificiranje, pa tudi o izbrani metodi preverjanja, ustreznem neodvisnem pritožbenem mehanizmu in zakonsko določenem organu, pristojnem za uveljavljanje skladnosti z načeli ([68]).

(49) Organizacije lahko prejmejo osebne podatke na podlagi DPF EU-ZDA od datuma, ko jih ministrstvo za trgovino uvrsti na seznam DPF. Za zagotovitev pravne varnost in preprečitev „lažnih navedb“ se organizacije, ki se certificirajo prvič, ne smejo javno sklicevati na svoje spoštovanje načel, dokler ministrstvo za trgovino ne ugotovi, da je vloga za certificiranje, ki jo je vložila organizacija, popolna, in organizacije ne doda na seznam DPF ([69]). Da bi se lahko še naprej sklicevale na DPF EU-ZDA za prejemanje podatkov iz Unije, morajo take organizacije vsako leto znova potrditi svojo udeležbo v okviru. Če organizacija iz katerega koli razloga zapusti DPF EU-ZDA, mora umakniti vse izjave, ki kažejo na to, da še naprej sodeluje v navedenem okviru ([70]).

(50) Kot je navedeno v zavezah iz Priloge III, bo ministrstvo za trgovino preverilo, ali organizacije izpolnjujejo vse zahteve za certificiranje in ali so uvedle (javno) politiko zasebnosti, ki vsebuje informacije, potrebne na podlagi *načela obvestila* ([71]). Ministrstvo za trgovino bo na podlagi izkušenj s postopkom (ponovnega) certificiranja v okviru zasebnostnega ščita izvedlo številne preglede, tudi za preverjanje, ali politike zasebnosti organizacij vsebujejo hiperpovezavo na pravilen obrazec za pritožbe na spletišču ustreznega pritožbenega mehanizma in, kadar je v vlogo za certificiranje vključenih več subjektov ali podružnic ene organizacije, ali politike zasebnosti vsakega od navedenih subjektov izpolnjujejo zahteve za certificiranje in ali so na voljo posameznikom, na katere se nanašajo osebni podatki ([72]). Poleg tega bo ministrstvo za trgovino po potrebi skupaj s FTC in ministrstvom za promet izvedlo navzkrižne preglede, da bi preverilo, ali so organizacije predmet nadzornega organa, navedenega v njihovih vlogah za (ponovno) certificiranje, in bo sodelovalo z organi za alternativno reševanje sporov za preverjanje, ali so organizacije registrirane v neodvisnem pritožbenem mehanizmu, navedenem v njihovi vlogi za (ponovno) certificiranje ([73]).

([66]) Priloga I, člen III.7.
([67]) Priloga I, člen I. 2.
([68]) Priloga I, člen III.6.b, in glej člen o preverjanju zahtev za samocertificiranje v Prilogi III.
([69]) Priloga I, opomba 12.
([70]) Priloga I, člen III.6.h.
([71]) Priloga I, člen III.6.a in opomba 12, glej pa tudi člen o preverjanju zahtev za samocertificiranje v Prilogi III.
([72]) Priloga III, oddelek „Preverilo zahteve za samocertificiranje“.
([73]) Podobno bo ministrstvo za trgovino sodelovalo s tretjo stranko, ki bo v vlogi skrbnika sredstev, zbranih s pristojbino za forum organov za varstvo podatkov (glej uvodno izjavo 73), da bi preverilo, ali so organizacije, ki izberejo organ za varstvo podatkov za svoj neodvisen pritožbeni mehanizem, plačale pristojbino za ustrezno leto. Glej člen o preverjanju zahtev za samocertificiranje v Prilogi III.

(51) Ministrstvo za trgovino bo organizacije obvestilo, da morajo za opravo (ponovnega) certificiranja obravnavati vse težave, ugotovljene med njegovim pregledom. Če se organizacija ne odzove v roku, ki ga določi ministrstvo za trgovino (kar zadeva ponovno certificiranje, bi se na primer pričakovalo, da bo postopek zaključen v 45 dneh) ([74]), ali svojega certificiranja ne opravi drugače, se bo štelo, da je od vloge odstopila. V takem primeru je lahko vsako zavajanje o sodelovanju v DPF EU-ZDA ali skladnosti z njim predmet izvršilnih ukrepov FTC ali ministrstva za promet ([75]).

(52) Za zagotovitev pravilne uporabe DPF 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. Za zagotovitev take preglednosti na „vstopni točki" se je ministrstvo za trgovino zavezalo, da bo vodilo seznam organizacij, ki so certificirale zavezanost načelom in spadajo v pristojnost vsaj enega od organov pregona, navedenih v prilogah IV in V k temu sklepu, ter javnosti omogočilo dostop do takega seznama ([76]). Ministrstvo za trgovino bo posodabljalo seznam na podlagi letne vloge organizacije za ponovno certificiranje ali kadar organizacija izstopi iz DPF EU-ZDA ali je izločena iz njega. Poleg tega bo ministrstvo za trgovino za zagotovitev preglednosti tudi na „izstopni točki" vodilo evidenco organizacij, ki so bile odstranjene s seznama, in javnosti omogočilo dostop do nje, pri čemer bo v vsakem primeru navedlo razloge za tako odstranitev ([77]). Nazadnje, v DPF EU-ZDA bo zagotovil povezavo na spletno mesto FTC, na katerem bodo navedeni izvršilni ukrepi FTC na podlagi navedenega okvira ([78]).

2.3.2 ***Spremljanje skladnosti***

(53) Ministrstvo za trgovino bo redno spremljalo dejansko izpolnjevanje načel DPF EU-ZDA s strani organizacij z različnimi mehanizmi ([79]). Zlasti bo pri naključno izbranih organizacijah izvajalo „preglede na kraju samem", pri nekaterih organizacijah pa tudi *ad hoc* preglede na kraju samem, kadar so ugotovljene morebitne težave v zvezi s skladnostjo (npr. ki jih ministrstvu za trgovino sporočijo tretje stranke), da bi preverilo, ali so (i) kontaktne točke za obravnavanje pritožb in zahtevkov posameznikov, na katere se nanašajo osebni podatki, na voljo in odzivne; ali je (ii) politika zasebnosti organizacije dostopna na spletišču in tudi prek hiperpovezave na spletišču ministrstva za trgovino; ali (iii) politika zasebnosti organizacije še naprej izpolnjuje zahteve za certificiranje in ali je (iv) s strani organizacij izbrani neodvisni mehanizem za reševanje sporov na voljo za obravnavanje pritožb ([80]).

(54) Če obstajajo verodostojni dokazi, da organizacija ne izpolnjuje svojih zavez na podlagi DPF EU-ZDA (tudi če ministrstvo za trgovino prejme pritožbe ali organizacija ne odgovori zadovoljivo na poizvedbe ministrstva za trgovino), bo ministrstvo za trgovino od organizacije zahtevalo, naj izpolni in predloži izčrpen vprašalnik ([81]). Organizacija, ki na vprašalnik ne odgovori zadovoljivo in pravočasno, bo napotena na ustrezen organ (FTC ali ministrstvo za promet) za morebitne izvršilne ukrepe ([82]). Ministrstvo za trgovino je v okviru svojih dejavnosti spremljanja v okviru zasebnostnega ščita redno izvajalo preglede na kraju samem, navedene v uvodni izjavi 53, in ves čas spremljalo javna poročila, ki so mu omogočila, da je ugotovilo, obravnavalo in rešilo težave v zvezi

([74]) Glej Prilogo III, opomba 2.
([75]) Glej člen o preverjanju zahtev za samocertificiranje v Prilogi III.
([76]) Informacije o upravljanju seznama DPF so na voljo v Prilogi III (glej navodilo v programu ministrstva za trgovino o upravljanju in nadzoru okvira za varstvo zasebnosti podatkov) in Prilogo I (člen I.3, člen I.4, III.6.d in člen III.11.g).
([77]) Glej navodilo v programu ministrstva za trgovino o upravljanju in nadzoru okvira za varstvo zasebnosti podatkov v Prilogi III.
([78]) Glej člen o prilagoditvi spletnega mesta okvira za varstvo zasebnosti podatkov ciljnim skupinam v Prilogi III.
([79]) Glej člen o izvajanju rednih pregledov skladnosti in ocenjevanj programa okvira za varstvo zasebnosti podatkov po uradni dolžnosti v Prilogi III.
([80]) Ministrstvo za trgovino lahko v okviru svojih dejavnosti spremljanja uporabi različna orodja, tudi za pregled prekinjenih povezav do politik zasebnosti, ali dejavno spremlja nove objave poročil, ki zagotavljajo verodostojne dokaze o neskladnosti.
([81]) Glej člen o izvajanju rednih pregledov skladnosti in ocenjevanj programa okvira za varstvo zasebnosti podatkov po uradni dolžnosti v Prilogi III.
([82]) Glej člen o izvajanju rednih pregledov skladnosti in ocenjevanj programa okvira za varstvo zasebnosti podatkov po uradni dolžnosti v Prilogi III.

s skladnostjo ([83]). Organizacije, ki vztrajno ne spoštujejo načel, bodo odstranjene s seznama DPF ter morajo vrniti ali izbrisati osebne podatke, prejete na podlagi navedenega okvira ([84]).

(55) V drugih primerih odstranitve, kot je prostovoljna prekinitev sodelovanja ali neizvedba ponovnega certificiranja, mora organizacija bodisi izbrisati bodisi vrniti podatke, ali pa jih lahko zadrži, če pri ministrstvu za trgovino vsako leto potrdi svojo zavezanost 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) ([85]). V tem primeru mora organizacija določiti tudi kontaktno točko v organizaciji za vsa vprašanja, povezana z DPF EU-ZDA.

2.3.3 *Odkrivanje in obravnavanje lažnih navedb o sodelovanju*

(56) Ministrstvo za trgovino bo spremljalo vse lažne navedbe o sodelovanju v DPF EU-ZDA ali nepravilni uporabi certifikacijske oznake DPF EU-ZDA po uradni dolžnosti in tudi na podlagi pritožb (tj. prejetih od organov za varstvo podatkov) ([86]). Ministrstvo za trgovino bo zlasti redno preverjalo, da organizacije, ki (i) prekinejo sodelovanje v DPF EU-ZDA, (ii) ne opravijo letnega ponovnega certificiranja (tj. so ga bodisi začele, vendar postopka letnega ponovnega certificiranja niso pravočasno zaključile, bodisi postopka letnega ponovnega certificiranja niso niti začele), (iii) so izločene kot udeleženec, zlasti zaradi „vztrajnega neizpolnjevanja načel“ ali (iv) ne opravijo začetnega certificiranja (tj. so ga začele, vendar postopka začetnega certificiranja niso pravočasno zaključile), odstranijo iz vseh ustreznih objavljenih politik zasebnosti sklice na DPF EU-ZDA, ki kažejo na to, da organizacija dejavno sodeluje v navedenem okviru ([87]). Ministrstvo za trgovino bo prav tako s spletnim iskanjem odkrivalo sklice na DPF EU-ZDA v politikah zasebnosti organizacij, vključno z odkrivanjem lažnih navedb organizacij, ki niso nikoli sodelovale v DPF EU-ZDA ([88]).

(57) Če ministrstvo za trgovino ugotovi, da sklici na DPF EU-ZDA niso bili odstranjeni ali da se nepravilno uporabljajo, bo organizacijo obvestilo o morebitni predložitvi zadeve FTC/ministrstvu za promet ([89]). Če organizacija ne odgovori zadovoljivo, bo ministrstvo za trgovino zadevo predložilo ustreznemu organu pregona za morebitne izvršilne ukrepe ([90]). Vsako zavajanje širše javnosti v zvezi z zavezanostjo organizacije načelom v obliki zavajajočih izjav ali praks je lahko predmet izvršilnih ukrepov FTC, ministrstva za promet ali drugih ustreznih izvršnih organov ZDA. Zavajanje ministrstva za trgovino se lahko preganja po zakonu o lažnih navedbah (*False Statements Act*) (člen 1001 naslova 18 zakonodajne zbirke ZDA).

([83]) Med drugim letnim pregledom zasebnostnega ščita je ministrstvo za trgovino sporočilo, da je pri 100 organizacijah izvedelo preglede na kraju samem, vprašalnik o skladnosti pa poslalo v 21 primerih (nato pa so bile ugotovljene težave odpravljene), glej delovni dokument služb Komisije SWD (2018) 497 final, str. 9. Podobno je ministrstvo za trgovino med tretjim letnim pregledom zasebnostnega ščita poročalo, da je s svojim spremljanjem javnih poročil ugotovilo tri primere in začelo v praksi izvajati preglede na kraju samem pri 30 podjetjih vsak mesec, kar je v 28 % primerov pripeljalo do nadaljnjega ukrepanja z vprašalniki o skladnosti (nato pa so bile ugotovljene težave nemudoma odpravljene ali, v treh primerih, rešene po opozorilnem dopisu), glej delovni dokument služb Komisije SWD (2019) 495 final, str. 8.

([84]) Priloga I, člen III.11.g. Vztrajno neupoštevanje načel pomeni, da organizacija zlasti noče ravnati v skladu s končno ugotovitvijo organa s samourejevalnim sistemom za varstvo zasebnosti, neodvisnega organa za reševanje sporov ali izvršnega organa.

([85]) Priloga I, člen III.6.f.

([86]) Glej člen o iskanju in obravnavi lažnih navedb o sodelovanju v Prilogi III.

([87]) *Prav tam*.

([88]) *Prav tam*.

([89]) *Prav tam*.

([90]) V okviru zasebnostnega ščita je ministrstvo za trgovino med tretjim letnim pregledom okvira poročalo, da je odkrilo 669 primerov lažnih navedb o sodelovanju (med oktobrom 2018 in oktobrom 2019), večina od katerih je bila odpravljena po opozorilnem dopisu ministrstva za trgovino, 143 zadev pa je predložilo FTC (glej uvodno izjavo 62 spodaj). Glej dokument služb Komisije SWD (2019) 495 final, str. 10.

2.3.4 ***Izvrševanje***

(58) Da se zagotovi ustrezna raven varstva podatkov v praksi, bi bilo treba vzpostaviti neodvisen nadzorni organ, pooblaščen za spremljanje in zagotavljanje skladnosti s pravili o varstvu podatkov.

(59) Organizacije v DPF EU-ZDA morajo biti v pristojnosti organov ZDA (FTC ali ministrstvo za promet), ki imajo potrebna preiskovalna in izvršilna pooblastila za učinkovito zagotavljanje skladnosti z načeli ([91]).

(60) FTC je neodvisen organ, ki ga sestavlja pet komisarjev, ki jih imenuje predsednik po posvetovanju senata in z njegovim soglasjem ([92]). Komisarji so imenovani za sedemletno obdobje in jih lahko razreši le predsednik, in sicer zaradi neučinkovitosti, zanemarjanja dolžnosti ali zlorabe uradnega položaja. FTC ne sme imeti več kot tri komisarje iz iste politične stranke, komisarji pa med svojim mandatom ne smejo opravljati nobenih drugih poslov, poklica ali zaposlitve.

(61) FTC lahko preiskuje skladnost z načeli, pa tudi lažne navedbe o spoštovanju načel ali sodelovanju v DPF EU-ZDA s strani organizacij, ki bodisi niso več na seznamu DPF bodisi se nikoli niso certificirale ([93]). FTC lahko uveljavi skladnost s sodnimi odločbami upravnih sodišč ali zveznega sodišča (vključno z odločbami o soglasju, doseženimi s poravnavami) ([94]) o predhodnih ali trajnih prepovedih ali z drugimi pravnimi sredstvi, sistematično pa bo spremljal skladnost s takimi odločbami ([95]). Če organizacije ne izpolnijo takih odločb, lahko FTC uveljavi denarne kazni in druga pravna sredstva, tudi za škodo, povzročeno s protipravnim ravnanjem. Vsaka odločba o soglasju, izdana organizaciji v DPF EU-ZDA, bo vsebovala določbe o samoporočanju ([96]), organizacije pa bodo morale objaviti vse ustrezne dele katerega koli poročila o skladnosti ali ocenjevalnega poročila, predloženega FTC, ki se nanašajo na DPF. FTC bo vodil tudi spletni seznam organizacij, za katere veljajo odločbe FTC ali sodne odločbe v zadevah, povezanih z DPF EU-ZDA ([97]).

(62) V zvezi z zasebnostnim ščitom je FTC v približno 22 primerih sprejel izvršilne ukrepe zaradi kršitev določenih zahtev okvira (npr. nepotrditev ministrstvu za trgovino, da je organizacija po izstopu iz okvira še naprej uporabljala varstvo zasebnostnega ščita, nepreverjanje s samoocenjevanjem ali zunanjim pregledom skladnosti z načeli, da je organizacija ravnala v skladu z okvirom) ([98]), in lažne navedbe o sodelovanju v okviru (npr. s strani organizacij, ki niso zaključile potrebnih korakov za pridobitev potrdila ali je njihovo potrdilo poteklo, vendar so zavajale o svojem nadaljnjem sodelovanju) ([99]). Ta izvršilni ukrep je bil med drugim posledica proaktivne uporabe upravnih sodnih pozivov za pridobitev gradiva od nekaterih udeležencev v zasebnostnem ščitu za pregled bistvenih kršitev obveznosti zasebnostnega ščita ([100]).

([91]) Organizacija v DPF EU-ZDA se mora javno zavezati spoštovanju načel, razkriti svoje politike zasebnosti v skladu s temi načeli in jih v celoti izvajati. Neizpolnjevanje načel se preganja na podlagi člena 5 zakona o FTC, ki prepoveduje nepoštena in goljufiva dejanja v trgovini ali v zvezi z njo (člen 45 naslova 15 zakonodajne zbirke ZDA) in člena 41712 naslova 49 zakonodajne zbirke ZDA, ki prevozniku ali agenciji za prodajo letalskih vozovnic prepoveduje nepošteno ali goljufivo ravnanje pri prodaji zračnega prevoza.

([92]) Člen 41 naslova 15 zakonodajne zbirke ZDA.

([93]) Priloga IV.

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

([95]) Glej člen o uveljavljanju in spremljanju odločb v Prilogi IV.

([96]) 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.

([97]) Priloga IV, člen o uveljavljanju in spremljanju odločb.

([98]) Dokument služb Komisije SWD (2019) 495 final, str. 11.

([99]) Glej primere, navedene na spletišču FTC, na voljo prek povezave https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Glej tudi dokument služb Komisije SWD (2017) 344 final, str. 17; dokument služb Komisije SWD (2018) 497 final, str. 12 in dokument služb Komisije SWD (2019) 495 final, str. 11.

([100]) Glej na primer „Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review“ (Pripravljene pripombe predsednika Josepha Simonsa ob drugem letnem pregledu zasebnostnega ščita) (ftc.gov).

(63) Na splošno je FTC v zadnjih letih sprejela izvršilne ukrepe v številnih primerih v zvezi s skladnostjo z določenimi zahtevami o varstvu podatkov, ki se zagotavljajo tudi v okviru DPF EU-ZDA, npr. v zvezi z načeli omejitve namena in hrambe podatkov ([101]), najmanjšega obsega podatkov ([102]), varnosti podatkov ([103]) in točnosti podatkov ([104]).

(64) Ministrstvo za promet ima izključno pristojnost za urejanje praks letalskih prevoznikov glede zasebnosti, v zvezi s praksami agencij za prodajo letalskih vozovnic glede zasebnosti pa si deli pristojnost s FTC. Uradniki ministrstva za promet si najprej prizadevajo za dosego poravnave in lahko, če to ni mogoče, uvedejo izvršilni postopek, ki vključuje predhodno obravnavo dokazov pred upravnim sodnikom pri ministrstvu za promet, ki je pooblaščen za izdajo odlokov o prepovedi in naložitev denarnih kazni ([105]). Upravni sodniki uživajo na podlagi zakona o upravnem postopku (*Administrative Procedure Act*, v nadaljnjem besedilu: APA) več vrst zaščite za zagotovitev njihove neodvisnosti in nepristranskosti. Na primer, razrešiti jih je mogoče le iz upravičenih razlogov; zadevam so dodeljeni po načelu rotacije; svojih dolžnosti ne smejo opravljati v neskladju s svojimi nalogami in obveznostmi upravnih sodnikov; zanje ne velja nadzor preiskovalne skupine organa, pri katerem so zaposleni (v tem primeru ministrstvo za promet), svojo funkcijo odločanja/izvrševanja pa morajo opravljati nepristransko ([106]). Ministrstvo za promet se je zavezalo spremljanju izvršilnih odlokov in zagotavlja, da so odloki, ki so posledica primerov na podlagi DPF EU-ZDA, na voljo na njegovem spletišču ([107]).

2.4 **Pravna sredstva**

(65) Posameznik, na katerega se nanašajo osebni podatki, mora imeti na voljo učinkovito upravno in sodno varstvo, da se zagotovita ustrezno varstvo in zlasti uresničevanje pravic posameznika.

(66) DPF EU-ZDA v skladu z *načelom pritožbenega mehanizma, izvrševanja in odgovornosti* zahteva, da organizacije zagotovijo pritožbeni mehanizem za posameznike, na katere vpliva neizpolnjevanje načel, ter s tem možnost, da posamezniki iz Unije, na katere se nanašajo osebni podatki, vložijo pritožbe v zvezi z neizpolnjevanjem načel s strani organizacij v DPF EU-ZDA in da se te pritožbe rešijo, če to zahteva odločitev, ki zagotavlja učinkovita pravna sredstva ([108]). Organizacije morajo v okviru svojega certificiranja izpolnjevati zahteve tega načela 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 ([109]).

([101]) Glej na primer sklep FTC v zadevi Drizly, LLC., ki med drugim zahteva, da družba (1) uniči vse osebne podatke, ki jih je zbrala in ki niso potrebni za zagotavljanje proizvodov ali storitev potrošnikom, (2) ne zbira ali shranjuje osebnih podatkov, razen če je to potrebno za posebne namene, določene v načrtu hrambe.

([102]) Glej na primer sklep FTC v zadevi CafePress (24. marec 2022), v skladu s katerim je treba med drugim čim bolj zmanjšati količino zbranih podatkov.

([103]) Glej npr. izvršilne ukrepe FTC v zadevah Drizly, LLC in CafePress, s katerimi je od zadevnih podjetij zahtevala, da vzpostavijo namenski varnostni program ali posebne varnostne ukrepe. Poleg tega glej v zvezi s kršitvami varstva podatkov tudi sklep FTC z dne 27. januarja 2023 v zadevi Chegg, poravnava z družbo Equifax iz leta 2019 (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Glej npr. zadevo RealPage, Inc. (16. oktober 2018), v kateri je FTC na podlagi FCRA sprejela izvršilne ukrepe proti družbi za preverjanje najemnikov, ki je lastnikom nepremičnin in družbam za upravljanje nepremičnin predložila informativna poročila o posameznikih na podlagi informacij iz zgodovine najemov, informacij iz javnih evidenc (vključno z zgodovino kaznivih dejanj in deložacij) in kreditnih informacij, ki so bile uporabljene kot dejavnik pri določanju možnosti dostopa do nastanitve. FTC je ugotovila, da družba ni sprejela razumnih ukrepov za zagotovitev točnosti informacij, ki jih je predložila na podlagi svojega orodja za avtomatizirano odločanje.

([105]) Glej člen o praksah izvrševanja v Prilogi V.

([106]) Glej člene 3105, 7521(a), 554(d) in 556(b)(3) naslova 5 zakonodajne zbirke ZDA.

([107]) Glej člen o spremljanju in javni objavi izvršilnih odlokov v zvezi s kršitvami DPF EU-ZDA v Prilogi V.

([108]) Priloga I, člen II.7.

([109]) Priloga I, člen III.11.

(67) Organizacije lahko izberejo neodvisne pritožbene mehanizme v Uniji ali ZDA. Kot je podrobneje pojasnjeno v uvodni izjavi 73, to vključuje možnost prostovoljne zaveze sodelovanju z organi za varstvo podatkov EU. Če organizacije obdelujejo podatke o človeških virih, je taka zaveza sodelovanju z organi za varstvo podatkov EU obvezna. Druge možnosti vključujejo neodvisno alternativno reševanje sporov ali v zasebnem sektorju razvite programe za varstvo zasebnosti, ki v svoja pravila vključujejo načela. Slednji morajo vključevati učinkovite mehanizme izvrševanja v skladu z zahtevami *načela pritožbenega mehanizma, izvrševanja in odgovornosti*.

(68) Tako DPF EU-ZDA posameznikom, na katere se nanašajo osebni podatki, zagotavlja številne možnosti, da uveljavljajo svoje pravice, vložijo pritožbe v zvezi z neizpolnjevanjem načel s strani organizacij v DPF EU-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, ministrstvu za trgovino ali ministrstvu za promet. Če se njihove pritožbe ne rešijo z nobenim od teh pritožbenih mehanizmov ali mehanizmov izvrševanja, lahko uveljavljajo zavezujočo arbitražo (Priloga I Priloge I k temu sklepu). Razen za arbitražni senat, za katerega je treba pred uveljavitvijo izčrpati nekatera pravna sredstva, lahko posamezniki uporabijo kateri koli ali vse mehanizme pravnih sredstev po lastni izbiri in jim ni treba izbrati določenega mehanizma ali slediti določenemu zaporedju.

(69) Prvič, posamezniki iz Unije, na katere se nanašajo osebni podatki, lahko spremljajo primere neizpolnjevanja načel z neposrednimi stiki z organizacijami v DPF EU-ZDA ([110]). Za lažje reševanje pritožb mora organizacija vzpostaviti učinkovit mehanizem pravnega varstva za obravnavanje takih pritožb. Zato mora politika zasebnosti organizacije 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 tudi o neodvisnem organu za reševanje sporov (glej uvodno izjavo 70). Organizacija mora po prejemu pritožbe, neposredno od posameznika ali prek ministrstva za trgovino na podlagi napotitve organa za varstvo podatkov, posamezniku v Uniji, na katerega se nanašajo osebni podatki, odgovoriti v 45 dneh ([111]). Podobno morajo organizacije nemudoma odgovoriti na poizvedbe in druge zahteve za informacije s strani ministrstva za trgovino ali organa za varstvo podatkov ([112]) (če se je organizacija zavezala, da bo sodelovala z organom za varstvo podatkov), ki se nanašajo na njihovo spoštovanje načel.

(70) 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 ([113]). Sankcije in pravna sredstva, ki jih naloži tak organ, morajo biti dovolj stroga, da zagotavljajo izpolnjevanje 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 ([114]). Neodvisni organi za reševanje sporov, ki jih imenuje organizacija, morajo na svoja javna spletišča vključiti ustrezne informacije v zvezi z DPF EU-ZDA in storitvami, ki jih zagotavljajo v skladu z njim ([115]). Vsako leto morajo objaviti letno poročilo s skupnimi statističnimi podatki v zvezi s temi storitvami ([116]).

([110]) Priloga I, člen III.11.d.(i).
([111]) Priloga I, člen III.11.d.(i).
([112]) To je organ za obravnavanje pritožb, ki ga imenuje forum organov za varstvo podatkov, določen v dopolnilnem načelu o vlogi organov za varstvo podatkov (Priloga I, člen III.5).
([113]) Priloga I, člen III.11.d.
([114]) Priloga I, člen II.7 in III.11.e.
([115]) Priloga I, člen III.11.d.(ii).
([116]) Letno poročilo mora vsebovati: (1) skupno število pritožb, povezanih z DPF EU-ZDA, 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.

(71) V okviru svojih postopkov pregleda skladnosti lahko ministrstvo za trgovino preveri, ali so se organizacije v DPF EU-ZDA dejansko registrirale v neodvisnih pritožbenih mehanizmih, v katerih naj bi bile po njihovih trditvah registrirane ([117]). Organizacije in odgovorni neodvisni pritožbeni mehanizmi morajo nemudoma odgovoriti na poizvedbe in zahteve ministrstva za trgovino za informacije v zvezi z DPF. EU-ZDA. Ministrstvo za trgovino bo sodelovalo z neodvisnimi pritožbenimi mehanizmi, da bi preverilo, ali na svojih spletiščih vključujejo informacije o načelih in storitvah, ki jih zagotavljajo na podlagi DPF EU-ZDA, in ali objavljajo letna poročila ([118]).

(72) Če organizacija ne upošteva odločitve organa za reševanje sporov ali samoregulativnega organa, mora slednji o taki neskladnosti obvestiti ministrstvo za trgovino in FTC (ali drug organ ZDA s pristojnostjo za preiskovanje neizpolnjevanja načel) ter pristojno sodišče ([119]). 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 lahko šteje za vztrajno neizpolnjevanje 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 DPF ([120]). Če se organizacija po odstranitvi s seznama še naprej sklicuje na certificiranje na podlagi DPF EU-ZDA, bo ministrstvo za trgovino zadevo predložilo FTC ali drugemu organu pregona ([121]).

(73) Tretjič, posamezniki lahko pritožbe vložijo tudi pri nacionalnem organu za varstvo podatkov v Uniji, ki lahko uporabi svoja preiskovalna in popravna pooblastila v skladu z Uredbo (EU) 2016/679. 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 prostovoljno sprejele nadzor organov za varstvo podatkov ([122]). 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 ([123]). V primeru neskladnosti z nasveti organa za varstvo podatkov bo organ za varstvo podatkov take primere predal ministrstvu za trgovino (ki lahko organizacije umakne s seznama DPF EU-ZDA) ali, za morebitne izvršilne ukrepe, FTC oziroma ministrstvu za promet (nesodelovanje z organi za varstvo podatkov ali nespoštovanje načel se lahko v skladu z zakonodajo ZDA kaznuje) ([124]).

(74) Za lažje sodelovanje na področju učinkovitega obravnavanja pritožb sta ministrstvo za trgovino in tudi FTC vzpostavila namensko kontaktno točko, ki je odgovorna za neposredno povezovanje z organi za varstvo podatkov ([125]). Navedene kontaktne točke organu za varstvo podatkov pomagajo pri poizvedbah v zvezi z izpolnjevanjem načel s strani organizacije.

(75) Nasvet organov za varstvo podatkov ([126]) se izda, ko sta oba udeleženca v sporu imela ustrezno priložnost za predložitev pripomb in kakršnih koli dokazov. Forum lahko svetuje takoj, ko to dopušča zahteva po dolžnem pravnem postopanju, praviloma v 60 dneh po prejemu pritožbe ([127]). Če organizacija tudi po 25 dneh po prejemu nasveta ne ravna v skladu z njim in če za zamudo ne poda zadovoljive obrazložitve, lahko forum sporoči svojo namero, da bo bodisi predložil zadevo FTC (ali drugemu izvršnemu organu ZDA) bodisi ugotovil, da gre za resno kršitev zaveze o sodelovanju. Pri prvi možnosti lahko to pripelje do pregona na podlagi člena 5 zakona o FTC (ali

([117]) Člen o preverjanju zahtev za samocertificiranje v Prilogi I.
([118]) Glej člen o lažjem sodelovanju z organi za alternativno reševanje sporov, k zagotavljajo storitve, povezane z načeli, v Prilogi III. Glej tudi Prilogo I, člen III.11.d.(ii)–(iii).
([119]) Glej Prilogo I, člen III.11.e.
([120]) Glej Prilogo I, člen III.11.g, zlasti točki (ii) in (iii).
([121]) Glej člen o iskanju in obravnavi lažnih navedb o sodelovanju v Prilogi III.
([122]) Priloga I, člen II.7.b.
([123]) Priloga I, člen III.5.
([124]) Priloga I, člen III.5.c.(ii).
([125]) Priloga III (glej člen o lažjem sodelovanju z organi za varstvo podatkov) in Priloga IV (glej člena o prednostni obravnavi in preiskovanju predloženih zadev in o sodelovanju z organi za varstvo podatkov EU pri izvrševanju).
([126]) Organi za varstvo podatkov bi morali pripraviti poslovnik neuradnega foruma organov za varstvo podatkov na podlagi svoje pristojnosti za organizacijo dela in medsebojno sodelovanje.
([127]) Priloga I, člen III.5.c.(i).

podobnega zakona) ([128]). Pri drugi možnosti bo forum obvestil ministrstvo za trgovino, ki bo neupoštevanje nasveta foruma organov za varstvo podatkov obravnavalo kot vztrajno neizpolnjevanje načel, zaradi česar bo organizacija črtana s seznama DPF.

(76) 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 EU.

(77) Posamezniki lahko pritožbo pri organih za varstvo podatkov vložijo tudi, če forum organov za varstvo podatkov ni bil imenovan kot organ za reševanje sporov organizacije. V teh primerih lahko organ za varstvo podatkov predloži take pritožbe ministrstvu za trgovino ali FTC. Ministrstvo za trgovino bo za olajšanje in povečanje sodelovanja na področju zadev, povezanih s posameznimi pritožbami in neizpolnjevanjem načel s strani organizacij v DPF EU-ZDA, vzpostavilo posebno kontaktno točko, ki bo delovala kot povezovalna točka in bo pomagala organu za varstvo podatkov pri poizvedbah v zvezi z neizpolnjevanjem načel s strani organizacije ([129]). Podobno se je FTC zavezal, da bo vzpostavil namensko kontaktno točko ([130]).

(78) Četrtič, ministrstvo za trgovino se je zavezalo, da bo sprejemalo, pregledalo in si po najboljših močeh prizadevalo rešiti pritožbe o neizpolnjevanju načel s strani organizacije ([131]). V ta namen ministrstvo za trgovino zagotavlja posebne postopke, s katerimi organi za varstvo podatkov posredujejo pritožbe namenski kontaktni točki, jih spremljajo in skupaj z organizacijami določijo nadaljnje ukrepe za olajšanje reševanja ([132]). Da bi pospešila obdelavo posameznih pritožb, se kontaktna točka neposredno poveže z ustreznim organom za varstvo podatkov glede težav v zvezi s skladnostjo in ga najpozneje v 90 dneh od predložitve pritožbe zlasti obvesti o statusu pritožbe ([133]). To posameznikom, na katere se nanašajo osebni podatki, omogoča, da pritožbe zaradi neizpolnjevanja načel s strani organizacij v DPF EU-ZDA predložijo neposredno svojemu nacionalnemu organu za varstvo podatkov in jih posredujejo ministrstvu za trgovino kot organu ZDA, ki upravlja DPF EU-ZDA.

(79) Če ministrstvo za trgovino na podlagi preverjanj po uradni dolžnosti, pritožb ali kakršnih koli drugih informacij ugotovi, da organizacija vztrajno ne spoštuje načel, lahko tako organizacijo odstrani s seznama DPF ([134]). Če kateri koli organ s samourejevalnim sistemom za varstvo zasebnosti, neodvisen 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 ([135]).

(80) Petič, organizacija v DPF EU-ZDA mora biti v pristojnosti organov ZDA, zlasti FTC ([136]), ki imajo potrebna preiskovalna in izvršilna pooblastila za učinkovito zagotavljanje skladnosti z načeli. FTC prednostno obravnava predložene zadeve glede neizpolnjevanja načel, ki jih je prejel 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 ugotovil, ali je bil kršen člen 5 zakona o FTC ([137]). FTC se je zavezal, da bo oblikoval standardiziran postopek za pošiljanje zadev, imenoval kontaktno točko organa za zadeve, ki jih predloži organ za varstvo podatkov, in izmenjeval informacije o predloženih zadevah. Poleg tega lahko sprejema pritožbe neposredno od posameznikov in na lastno pobudo izvaja preiskave DPF EU-ZDA, zlasti v okviru obsežnejšega preiskovanja zadev v zvezi z zasebnostjo.

([128]) Priloga I, člen III.5.c.(ii).
([129]) Glej člen o lažjem sodelovanju z organi za varstvo podatkov v Prilogi III.
([130]) Glej člen o prednostni obravnavi in preiskovanju predloženih zadev in o sodelovanju z organi za varstvo podatkov EU pri izvrševanju v Prilogi IV.
([131]) Glej na primer člen o lažjem sodelovanju z organi za varstvo podatkov v Prilogi III.
([132]) Priloga I, člen II.7.e in Priloga III, člen o lažjem sodelovanju z organi za varstvo podatkov.
([133]) *Prav tam*.
([134]) Priloga I, člen III.11.g.
([135]) Priloga I, člen III.11.g.
([136]) Organizacija v DPF EU-ZDA se mora javno zavezati izpolnjevanju načel, razkriti svoje politike zasebnosti v skladu s temi načeli in jih v celoti izvajati. Neizpolnjevanje načel se preganja na podlagi člena 5 zakona o FTC, ki prepoveduje nepoštena in goljufiva dejanja v trgovini ali v zvezi z njo.
([137]) Glej tudi podobne zaveze ministrstva za promet v Prilogi V.

(81) Šestič, če se pritožba posameznika ne reši z uporabo katere od navedenih možnosti pravnega varstva, lahko posameznik iz Unije, na katerega se nanašajo osebni podatki, v skrajnem primeru uveljavlja zavezujočo arbitražo „senata okvira za varstvo zasebnosti podatkov med EU in ZDA“ (senat DPF EU-ZDA) ([138]). Organizacije morajo posameznike obvestiti o možnosti, da uveljavijo zavezujočo arbitražo, in se po uveljavitvi te možnosti s strani posameznika odzvati tako, da pošljejo obvestilo zadevni organizaciji ([139]).

(82) Ta senat DPF EU-ZDA sestavlja skupina najmanj desetih 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 s tremi ([140]) arbitri.

(83) Ministrstvo za trgovino je za upravljanje arbitraž izbralo mednarodno središče za reševanje sporov (*International Centre for Dispute Resolution*, v nadaljnjem besedilu: ICDR), mednarodni oddelek ameriškega združenja za arbitražo (*American Arbitration Association*, v nadaljnjem besedilu: AAA). Postopke pred senatom DPF EU-ZDA urejata sklop dogovorjenih pravil arbitraže in kodeks ravnanja za imenovane arbitre. Spletišče ICDR-AAA posameznikom zagotavlja jasne in jedrnate informacije o arbitražnem mehanizmu in postopku za vložitev predloga o arbitraži.

(84) Pravila arbitraže, o katerih sta se dogovorila ministrstvo za trgovino in Komisija, dopolnjujejo DPF EU-ZDA, ki vsebuje več elementov, ki povečujejo dostopnost tega mehanizma za posameznike iz Unije, 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 Unije, 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, načeloma 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 DPF EU-ZDA, s katerimi se bodo krili stroški arbitražnega postopka do najvišjih zneskov, ki jih določijo organi ZDA v posvetovanju s Komisijo ([141]).

(85) Senat DPF EU-ZDA lahko zahteva nedenarno pravično nadomestilo za posameznika ([142]), ki je potrebno za odpravo neskladnosti z načeli. Čeprav senat upošteva druga pravna sredstva, ki so bila že pridobljena z drugimi mehanizmi DPF EU-ZDA med njegovim odločanjem, lahko posamezniki še vedno uporabijo arbitražo, če menijo, da so ta druga pravna sredstva nezadostna. To posameznikom iz Unije, na katere se nanašajo osebni podatki, omogoča, da uveljavljajo arbitražo v vseh primerih, v katerih se z ukrepanjem ali neukrepanjem organizacije v DPF EU-ZDA, neodvisnih pritožbenih mehanizmov ali pristojnih organov ZDA (na primer FTC) njihove pritožbe niso zadovoljivo rešile. Arbitraže ni dovoljeno uveljavljati, če ima organ za varstvo podatkov pravno pooblastilo za rešitev obravnavanega zahtevka v zvezi z organizacijo v DPF EU-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, bodisi 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.

([138]) Glej Prilogo I, Priloga I „Arbitražni model“.
([139]) Glej Prilogo I, člen II.1.a(xi) in II.7.c.
([140]) Strani se morata dogovoriti o številu arbitrov v senatu.
([141]) Priloga I Priloge I, člen G.6.
([142]) Posamezniki lahko v arbitraži zahtevajo odškodnino, vendar uveljavljanje arbitraže ne izključuje možnosti za vložitev zahtevka za odškodnino na rednih sodiščih v ZDA.

(86) Sedmič, če organizacija ne izpolnjuje zavez v zvezi z načeli in objavljeno politiko zasebnosti, so po zakonodaji ZDA na voljo dodatne možnosti pravnega sredstva, vključno z dodelitvijo odškodnine. Posamezniki lahko na primer pod določenimi pogoji uveljavljajo pravna sredstva (vključno z odškodnino) po državnih zakonih o varstvu potrošnikov v primeru goljufivih lažnih navedb, nepoštenih ali goljufivih dejanj ([143]), in po odškodninskem pravu (zlasti zaradi škodnih dejanj motečega posega v intimno zasebnost ([144]), prisvojitve imena ali podobnosti ([145]) in javnega razkritja zasebnih dejstev ([146])).

(87) Različne zgoraj opisane možnosti pravnega varstva skupaj zagotavljajo, da bodo vse pritožbe v zvezi z neskladnostjo certificiranih organizacij z DPF EU-ZDA učinkovito rešene in neskladnosti odpravljene.

3. DOSTOP DO OSEBNIH PODATKOV, KI JIH IZ EVROPSKE UNIJE PRENESEJO JAVNI ORGANI V ZDRUŽENIH DRŽAVAH, IN UPORABA TEH PODATKOV

(88) Komisija je proučila tudi omejitve in zaščitne ukrepe, vključno z nadzorom in posameznimi mehanizmi pravnih sredstev, ki so na voljo v pravu Združenih držav glede zbiranja in naknadne uporabe osebnih podatkov s strani javnih organov ZDA, tj. podatkov, ki se v javnem interesu zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti („vladni dostop“) prenašajo upravljavcem in obdelovalcem v ZDA ([147]). Komisija je pri oceni, ali pogoji, pod katerimi vlada dostopa do podatkov, prenesenih v Združene države, na podlagi tega sklepa izpolnjujejo preskus „osnovne enakovrednosti“ na podlagi člena 45(1) Uredbe (EU) 2016/679, kakor ga razlaga Sodišče glede na Listino o temeljnih pravicah, upoštevala več meril.

(89) Natančneje, vsaka omejitev pravice do varstva osebnih podatkov mora biti določena v zakonu, pravna podlaga, ki dovoljuje poseg v tako pravico, pa mora že sama opredeljevati obseg omejitve izvrševanja zadevne pravice ([148]). Da se izpolni zahteva glede sorazmernosti, v skladu s katero se lahko odstopanja od varstva osebnih podatkov in omejitve tega varstva uporabljajo le, kolikor je to nujno potrebno v demokratični družbi, da se dosežejo specifični cilji splošnega interesa, ki so enakovredni interesom, priznanim v Uniji, mora ta pravna podlaga poleg tega določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnih ukrepov, ter minimalne zahteve, tako da imajo osebe, katerih podatki so bili preneseni, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje njihovih osebnih podatkov pred tveganjem zlorab ([149]). Poleg tega morajo biti ta pravila in zaščitni ukrepi pravno zavezujoči

([143]) Glej npr. kalifornijske državne zakone o varstvu potrošnikov (kalifornijski civilni zakonik, členi 1750 do 1785 (zahod) zakona o pravnih sredstvih potrošnikov (*Consumers Legal Remedies Act*)); Okrožje Kolumbija (zakonik okrožja Kolumbija, členi 28–3901); Florida (floridski zakonik, členi 501.201 do 501.213, zakon o goljufivih in nepoštenih trgovinskih praksah (*Deceptive and Unfair Trade Practices Act*)); Illinois (815 Ill. državna odškodnina 505/1 do 505/12, zakon o potrošniških goljufijah in goljufivih poslovnih praksah (*Consumer Fraud and Deceptive Business Practices Act*)); Pensilvanija (73 pensilvanski zakonik s komentarjem, členi 201-1 do 201-9.3 (zahod) zakon o nepoštenih trgovinskih praksah in varstvu potrošnikov (*Unfair Trade Practices and Consumer Protection Law*).

([144]) Tj. v primeru namernega posega v posameznikove zasebne zadeve na način, ki bi bil za razumno osebo skrajno žaljiv (Preoblikovanje (2.) škodnih dejanj, člen 652(b)).

([145]) To škodno dejanje se uporablja v primeru prisvojitve in uporabe posameznikovega imena ali podobnosti za oglaševanje podjetja ali proizvoda ali za nekatere podobne poslovne namene (glej Preoblikovanje (2.) škodnih dejanj, člen 652C).

([146]) Tj. če se objavi informacija, ki se nanaša na zasebno življenje posameznika, če je to za razumno osebo skrajno žaljivo, informacija pa ni stvar zakonitega interesa javnosti (Preoblikovanje (2.) škodnih dejanj, člen 652D).

([147]) To je upoštevno tudi glede na oddelek I.5 Priloge I. V skladu s tem oddelkom lahko, podobno pri Splošni uredbi o varstvu podatkov, za skladnost z zahtevami glede varstva podatkov in pravicami, ki so del načel zasebnosti, veljajo omejitve. Vendar take omejitve niso absolutne, temveč se je nanje mogoče sklicevati le pod več pogoji, na primer v obsegu, ki je potreben za izvršitev sodne odredbe ali izpolnjevanje zahtev javnega interesa, kazenskega pregona ali nacionalne varnosti. V tem okviru in zaradi jasnosti se ta oddelek sklicuje tudi na pogoje iz Odredbe št. 14086, ki so med drugim ocenjeni v uvodnih izjavah 127–141.

([148]) Glej sodbo v zadevi Schrems II, točki 174 in 175 ter navedena sodna praksa. Glede dostopa javnih organov držav članic glej tudi sodbo z dne 6. oktobra 2020, Privacy International, C-623/17, EU:C:2020:790, točka 65, in sodbo z dne 6. oktobra 2020, La Quadrature du Net in drugi, združene zadeve C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 175.

([149]) Glej sodbo v zadevi Schrems II, točki 176 in 181 ter navedena sodna praksa. Glede dostopa javnih organov držav članic glej tudi sodbi v zadevi Privacy International, točka 68, in v zadevi La Quadrature du Net in drugi, točka 132.

in izvršljivi s strani posameznikov ([150]). Posamezniki, na katere se nanašajo osebni podatki, morajo zlasti imeti možnost uveljavljanja pravnih sredstev pred neodvisnim in nepristranskim sodiščem, da si tako zagotovijo dostop do osebnih podatkov, ki se nanje nanašajo, ali dosežejo popravek oziroma izbris takih podatkov ([151]).

3.1 **Dostop in uporaba s strani javnih organov ZDA za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj**

(90) Kar zadeva poseg v osebne podatke, ki se prenašajo na podlagi DPF EU-ZDA, pravo Združenih držav določa več omejitev glede dostopa do osebnih podatkov in njihove uporabe za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter zagotavlja nadzorne mehanizme in mehanizme pravnih sredstev, ki so v skladu z zahtevami iz uvodne izjave 89 tega sklepa. Pogoji, pod katerimi je tak dostop mogoč, in zaščitni ukrepi glede uporabe teh pooblastil so podrobneje ocenjeni v naslednjih oddelkih. V zvezi s tem je vlada ZDA (prek Ministrstva za pravosodje ZDA (*Department of Justice*, v nadaljnjem besedilu: ministrstvo za pravosodje) dala tudi zagotovila glede veljavnih omejitev in zaščitnih ukrepov (Priloga VI k temu sklepu).

3.1.1 ***Pravna podlaga, omejitve in zaščitni ukrepi***

3.1.1.1 *Omejitve in zaščitni ukrepi v zvezi z zbiranjem osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj*

(91) Kot je podrobneje pojasnjeno v uvodnih izjavah 92 do 99, lahko do osebnih podatkov, ki jih obdelujejo certificirane organizacije v ZDA in ki bi se prenašali iz Unije na podlagi DPF EU-ZDA, dostopajo zvezni tožilci in zvezni preiskovalni agenti v okviru različnih postopkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Ti postopki se uporabljajo na enak način, če se informacije pridobivajo od katere koli organizacije v ZDA, ne glede na državljanstvo ali prebivališče zadevnih posameznikov, na katere se nanašajo osebni podatki ([152]).

(92) Prvič, na zahtevo uradnika zveznega organa kazenskega pregona ali pravobranilca lahko sodnik izda nalog za preiskavo ali zaseg (vključno z elektronsko shranjenimi informacijami) ([153]). Tak nalog se lahko izda le, če obstaja „utemeljen sum ([154])“, da bodo „zasegljivi predmeti (dokazi kaznivega dejanja, nezakonito posedovani predmeti ali premoženje, zasnovano za uporabo ali namenjeno uporabi ali uporabljeno pri storitvi kaznivega dejanja) verjetno najdeni na kraju, navedenem v nalogu. V nalogu mora biti opredeljeno premoženje ali predmet, ki ga je treba zaseči, in imenovan sodnik, ki mu je treba nalog vrniti. Oseba, ki se preišče ali katere lastnina se preišče, lahko poskuša

([150]) Glej sodbo v zadevi Schrems II, točki 181 in 182.

([151]) Glej sodbo v zadevi Schrems I, točka 95, in sodbo v zadevi Schrems II, točka 194. V zvezi s tem je Sodišče Evropske unije poudarilo predvsem, da skladnost s členom 47 Listine o temeljnih pravicah, ki zagotavlja pravico do učinkovitega pravnega sredstva pred neodvisnim in nepristranskim sodiščem, „prispeva k ravni varstva, ki se zahteva v Uniji, in katere spoštovanje mora Komisija ugotoviti, preden sprejme sklep o ustreznosti na podlagi člena 45(1) Uredbe (EU) 2016/679“ (sodba v zadevi Schrems II, točka 186).

([152]) Glej Prilogo VI. V zvezi z zakonom o prisluškovanju telefonskim pogovorom (*Wiretap Act*), zakonom o shranjenih komunikacijah (*Stored Communications Act*, v nadaljnjem besedilu: SCA) in zakonom o snemalnikih klicev (*Pen Register Act*) (podrobneje pojasnjenimi v uvodnih izjavah 95 do 98) glej na primer Suzlon Energy Ltd/Microsoft Corp, 671 F.3d 726, 729 (pritožbeno sodišče devetega okrožja Združenih držav Amerike 2011).

([153]) Zvezna pravila o izvajanju kazenskega postopka, 41. V sodbi iz leta 2018 je vrhovno sodišče ZDA potrdilo, da morajo imeti organi kazenskega pregona nalog za preiskavo ali da mora obstajati izjema, zaradi katere nalog ni potreben, tudi za dostop do evidenc historičnih lokacijskih podatkov baznih postaj, ki zagotavljajo celovit pregled gibanja uporabnika, in da lahko uporabnik razumno pričakuje zasebnost v zvezi s takšnimi podatki (Timothy Ivory Carpenter/Združene države Amerike, št. 16-402, 585 U.S. (2018)). Posledično takih podatkov ni mogoče pridobiti od podjetja mobilne telefonije s sodno odločbo na podlagi utemeljenih razlogov za sum, da so informacije pomembne in bistvene v tekoči kazenski preiskavi, temveč se pri uporabi naloga zahteva dokazilo o obstoju utemeljenega suma.

([154]) V skladu z razlago vrhovnega sodišča je „utemeljen sum“ „praktičen, netehničen“ standard, ki zahteva „upoštevanje dejanskih in praktičnih vidikov vsakodnevnega življenja, na podlagi katerih razumne in preudarne osebe […] ravnajo“ (Illinois/Gates, 462 U.S. 213, 232 (1983)). Kar zadeva naloge za preiskavo, utemeljen sum obstaja, če obstaja enaka verjetnost, da bodo rezultat preiskave dokazi o odkritju kaznivega dejanja (prav tam).

doseči, da se izločijo dokazi, ki so bili pridobljeni ali izhajajo iz nezakonite preiskave, če se predložijo zoper njo med kazenskim postopkom ([155]). Če se od imetnika podatkov (npr. podjetja) zahteva, naj v skladu z nalogom razkrije podatke, lahko zahtevo po razkritju zlasti izpodbija kot neupravičeno obremenitev ([156]).

(93) Drugič, sodni poziv lahko izda velika porota (preiskovalni organ sodišča, ki ga sodnik ali sodnik nižjega sodišča vključi v poroto) v okviru preiskav nekaterih hudih kaznivih dejanj ([157]), običajno na zahtevo zveznega tožilca, s katerimi se od nekoga zahteva, naj predloži ali zagotovi poslovne evidence, elektronsko shranjene informacije ali druge stvarne predmete. Poleg tega različni zakoni dovoljujejo uporabo sodnih pozivov za predložitev ali zagotovitev poslovnih evidenc, elektronsko shranjenih informacij ali drugih stvarnih predmetov v preiskavah goljufij v zdravstvu zlorabe otrok, zaščite tajne službe, zadevah v zvezi z nadzorovanimi snovmi in preiskavah generalnega inšpektorja ([158]). V obeh primerih se informacije morajo nanašati na preiskavo, sodni poziv pa ne more biti nerazumen, tj. preširok, zatirajoč ali obremenjujoč (in ga lahko prejemnik izpodbija na tej podlagi) ([159]).

(94) Zelo podobni pogoji se uporabljajo za upravne sodne pozive, izdane za pridobitev dostopa do podatkov, ki jih hranijo podjetja v ZDA, za civilne ali regulativne namene („javni interes“). Pooblastila agencij s civilno in regulativno odgovornostjo za izdajo takih upravnih sodnih pozivov morajo biti določena z zakonom. Uporaba upravnega sodnega poziva je pogojena s „preizkusom razumnosti“, ki zahteva, da se preiskava izvaja v skladu z zakonitim namenom, da so informacije, ki se zahtevajo v sodnem pozivu, za ta namen upoštevne, da agencija še nima informacij, ki jih zahteva s sodnim pozivom, in da so bili izvedeni potrebni upravni postopki za izdajo sodnega poziva ([160]). V sodni praksi vrhovnega sodišča je bila pojasnjena tudi potreba po uravnoteženju pomena javnega interesa pri zahtevanih informacijah s pomenom interesov zasebnosti oseb in organizacij ([161]). Čeprav za uporabo upravnega sodnega poziva ni potrebna predhodna sodna odobritev, pa je predmet sodnega nadzora, če jo prejemnik izpodbija iz zgoraj navedenih razlogov ali če organ izdajatelj uveljavlja izvršitev sodnega poziva pred sodiščem ([162]). Poleg teh splošnih omejitev lahko iz posameznih zakonov izhajajo posebne (strožje) zahteve ([163]).

([155]) Mapp/Ohio, 367 U.S. 643 (1961).

([156]) Glej zadevo Vloga Združenih držav, 610 F.2d 1148, 1157 (pritožbeno sodišče tretjega okrožja Združenih držav Amerike 1979) (z odločitvijo, da „dolžno pravno postopanje zahteva obravnavo vprašanja o obremenjenosti, preden se telefonskemu podjetju z nalogom za preiskavo naloži obveznost zagotavljanja“ pomoči), in zadevo Vloga Združenih držav, 616 f.2d 1122 (pritožbeno sodišče devetega okrožja Združenih držav Amerike 1980).

([157]) Peti amandmaUstave ZDA določa, da velika porota vloži obtožnico za vsak „organizirani kriminal in [vsako] drugače zloglasno kaznivo dejanje.“ Velika porota je sestavljena iz 16 do 23 članov in določi, ali obstaja utemeljen sum, da je bilo storjeno kaznivo dejanje. Za tako ugotovitev imajo velike porote preiskovalna pooblastila, ki jim omogočajo izdajo sodnih pozivov.

([158]) Glej Prilogo VI.

([159]) Zvezna pravila o izvajanju kazenskega postopka, 17.

([160]) Združene države proti Powell, 379 U.S. 48 (1964).

([161]) Oklahoma Press Publishing Co.proti Walling, 327 U.S. 186 (1946).

([162]) Vrhovno sodišče je pojasnilo, da mora sodišče v primeru izpodbijanja upravnega sodnega poziva preučiti, (1) ali ima preiskava zakonito dovoljen namen, (2) ali je zadevno pooblastilo za izdajo sodnega poziva v pristojnosti kongresa in (3) ali so „zahtevani dokumenti upoštevni za preiskavo“. Sodišče je ugotovilo tudi, da mora biti zahtevek iz upravnega sodnega poziva „razumen“, tj. zahteva se, da je „določitev dokumentov, ki jih je treba predložiti, ustrezna, vendar ne pretirana, za namene zadevne preiskave“, vključno z „določnostjo“ pri „navedbi kraja, ki ga je treba preiskati, in oseb, ki jih je treba prijeti, ali stvari, ki jih je treba zaseči“.

([163]) Na primer, zakon o pravici do finančne zasebnosti vladne organe pooblašča, da na podlagi upravnega sodnega poziva pridobijo finančne evidence, ki jih ima finančna institucija, le če (1) obstaja razlog za domnevo, da so zahtevane evidence pomembne za zakonito preiskavo v okviru kazenskega pregona, in (2) če je bila stranki predložen izvod sodnega poziva ali vabila skupaj z obvestilom, v katerem je z razumno določnostjo navedena narava preiskave (člen 3405 naslova 12 zakonodajne zbirke ZDA). Drug primer je zakon o pravičnem poročanju o kreditni sposobnosti, ki agencijam, ki poročajo o potrošnikih, prepoveduje razkrivanje poročil o potrošnikih v odgovor na zahtevke na podlagi upravnega sodnega poziva (in jim omogoča le, da se odzovejo na sodne pozive velike porote ali sodne odločbe, člen 1681 in naslednji naslova 15 zakonodajne zbirke ZDA). Kar zadeva dostop do informacij o komunikacijah, se uporabljajo posebne zahteve zakona o shranjenih komunikacijah, vključno v zvezi z možnostjo uporabe upravnih sodnih pozivov (za podroben pregled glej uvodne izjave 96–97).

(95) Tretjič, več pravnih podlag omogočajo organom kazenskega pregona, da pridobijo dostop do podatkov o komunikaciji. Sodišče lahko izda sklep, ki dovoljuje zbiranje sprotnih nevsebinskih informacij glede klicanih telefonskih številk, usmerjanja, naslavljanja in signaliziranja o telefonski številki ali elektronski pošti (z uporabo snemalnika klicev ali naprave za pasti in sledenje), če ugotovi, da je organ potrdil, da so informacije, ki bodo verjetno pridobljene, pomembne za tekočo kazensko preiskavo ([164]). V sklepu je treba med drugim navesti identiteto osumljenca, če je znana; značilnosti komunikacije, za katero se sklep uporablja, in opredelitev kaznivega dejanja, na katero se nanašajo informacije, ki jih je treba zbrati. Uporaba snemalnika klicev ali naprave za pasti in sledenje je lahko dovoljena za obdobje največ 60 dni, ki je lahko podaljšano le z novo sodno odločbo.

(96) Poleg tega je dostop do informacij naročnikov, podatkov o prometu in shranjenih vsebin komunikacij, ki jih hranijo ponudniki internetnih storitev, telefonska podjetja in drugi tretji ponudniki storitev, za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj mogoče pridobiti na podlagi SCA ([165]). Za pridobivanje shranjene vsebine elektronskih komunikacij morajo organi kazenskega pregona načeloma pridobiti nalog od sodnika na podlagi utemeljenega suma, da zadevni račun vsebuje dokaze o kaznivem dejanju ([166]). Za informacije o registraciji naročnikov, naslove IP in povezane časovne žige ter podatke za obračunavanje lahko organi kazenskega pregona uporabijo sodni poziv. Za večino drugih shranjenih nevsebinskih informacij, kot so glave v elektronskem sporočilu brez vrstice z zadevo, mora organ kazenskega pregona pridobiti sodno odločbo, ki bo izdana, če sodnik meni, da obstajajo utemeljeni razlogi za sum, da so zahtevane informacije pomembne in bistvene za tekočo kazensko preiskavo.

(97) Ponudniki, ki prejmejo zahteve na podlagi SCA, lahko prostovoljno obvestijo stranko ali naročnika, čigar informacije se zahtevajo, razen če zadevni organ kazenskega pregona pridobi odredbo o zaščiti, ki prepoveduje tako obveščanje ([167]). Taka odredba o zaščiti je sodna odločba, ki od ponudnika elektronskih komunikacijskih storitev ali storitev daljinske obdelave, na katerega so naslovljeni nalog, sodni poziv ali sodna odločba, zahteva, da o obstoju naloga, sodnega poziva ali sodne odločbe ne obvešča nobene druge osebe, dokler se sodišču zdi primerno. Odredbe o zaščiti se izdajo, če sodišče ugotovi, da obstaja razlog za sum, da bi bila zaradi obveščanja resno ogrožena preiskava ali da bi se neupravičeno zavlačevala obravnava, npr. ker bi bilo ogroženo življenje ali fizična varnost posameznika, ker bi prišlo do bega pred pregonom, ker bi bile morebitne priče ustrahovane itd. Memorandum namestnika pravosodnega ministra (ki je zavezujoč za vse pravobranilce in agente pri ministrstvu za pravosodje) od tožilcev zahteva, da sprejmejo podrobno odločitev v zvezi s potrebo po odredbi o zaščiti, sodišču pa predložijo utemeljitev, kako so v konkretni zadevi izpolnjena zakonska merila za pridobitev odredbe o zaščiti ([168]). Memorandum tudi določa, da se v vlogah za izdajo odredbe o zaščiti na splošno ne sme zahtevati odlog obvestila za več kot eno leto. Če so v izjemnih okoliščinah morda potrebni sklepi z daljšo veljavnostjo, se lahko take sklepi zahtevajo le s pisnim soglasjem nadzornika, ki ga imenuje državni tožilec ZDA ali ustrezni pomočnik pravosodnega ministra. Poleg tega mora tožilec ob zaključku preiskave takoj oceniti, ali obstaja podlaga za ohranitev morebitnih veljavnih odredb o zaščiti, in če je ni, razveljaviti odredbo o zaščiti ter zagotoviti, da je ponudnik storitev o tem obveščen ([169]).

([164]) Člen 3123 naslova 18 zakonodajne zbirke ZDA.

([165]) Členi 2701–2713 naslova 18 zakonodajne zbirke ZDA.

([166]) Člen 2701(a)-(b)(1)(A) naslova 18 zakonodajne zbirke ZDA. Če je zadevni naročnik ali stranka obveščen (bodisi vnaprej bodisi v določenih okoliščinah z odloženim obvestilom), se lahko vsebina, shranjena več kot 180 dni, pridobi tudi na podlagi upravnega sodnega poziva ali sodnega poziva velike porote (člen 2701(b)(1)(B) naslova 18 zakonodajne zbirke ZDA) ali sodne odločbe (če obstajajo utemeljeni razlogi za sum, da so zahtevane informacije pomembne in bistvene za tekočo kazensko preiskavo (člen 2701(d) naslova 18 zakonodajne zbirke ZDA). Vendar v skladu s sodbo zveznega pritožbenega sodišča vladni preiskovalci take naloge za preiskavo na splošno pridobivajo od sodnikov za zbiranje vsebine zasebne komunikacije ali shranjenih podatkov od ponudnika komunikacijskih storitev. Združene države proti Warshak, 631 F.3d 266 (sodišče šestega okrožja Združenih držav Amerike, 2010).

([167]) Člen 2705(b) naslova 18 zakonodajne zbirke ZDA.

([168]) Glej memorandum o strožji politiki glede vlog za izdajo odredb o zaščiti (ali nerazkritju), ki ga je 19. oktobra 2017 izdal namestnik pravosodnega ministra Rod Rosenstein in je na voljo na naslovu https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Memorandum o dopolnilni politiki v zvezi z vlogami za izdajo odredb o zaščiti v skladu s členom 2705(b) naslova 18 zakonodajne zbirke ZDA, ki ga je 27. maja 2022 izdala namestnica pravosodnega ministra Lisa Moncao.

(98) Organi kazenskega pregona lahko tudi sprotno prestrezajo telefonsko, ustno ali elektronsko komunikacijo na podlagi sodne odločbe, v kateri sodnik ugotovi, da med drugim obstaja utemeljen sum, da bo prisluškovanje telefonskim pogovorom ali elektronsko prestrezanje privedlo do dokazov zveznega zločina ali do lokacije ubežnika, ki beži pred pregonom ([170]).

(99) Nadaljnje varstvo zagotavljajo najrazličnejše politike in smernice ministrstva za pravosodje, vključno s smernicami pravosodnega ministra za domače operacije FBI (*Attorney General Guidelines for Domestic FBI Operations*, v nadaljnjem besedilu: AGG-DOM), ki med drugim od Zveznega preiskovalnega urada (*Federal Bureau of Investigation*, v nadaljnjem besedilu: FBI) zahtevajo, da uporabi najmanj vsiljive preiskovalne metode, ki so izvedljive, ob upoštevanju vpliva na zasebnost in državljanske svoboščine ([171]).

(100) Glede na zagotovila vlade ZDA se zgoraj opisano enako ali večje varstvo uporablja za preiskave organov pregona na ravni države (v zvezi s preiskavami, ki se izvajajo v skladu z državnimi zakoni) ([172]). Natančneje, ustavne določbe ter zakoni in sodna praksa na državni ravni potrjujejo zgoraj navedeno varstvo pred nerazumnimi preiskavami in zasegi, saj zahtevajo izdajo naloga za preiskavo ([173]). Podobno kot na zvezni ravni se lahko nalogi za preiskavo izdajo le na podlagi dokaza utemeljenega suma, v njih pa morajo biti navedeni kraj, ki se preišče, ter oseba, ki jo je treba prijeti, ali stvar, ki se zaseže ([174]).

([170]) Členi 2510–2522 naslova 18 zakonodajne zbirke ZDA.

([171]) Smernice pravosodnega ministra za domače preiskave Zveznega preiskovalnega urada (FBI) (september 2008), na voljo na naslovu http://www.justice.gov/archive/opa/docs/guidelines.pdf. Dodatna pravila in politike, ki predpisujejo omejitve preiskovalnih dejavnosti zveznih tožilcev, so določene v priročniku za ameriške odvetnike (*United States Attorneys' Manual*), ki je na voljo na naslovu http://www.justice.gov/usam/united-states-attorneys-manual. Za odstopanje od teh smernic je treba pridobiti predhodno dovoljenje direktorja FBI, namestnika direktorja ali pomočnika izvršnega direktorja, ki ju imenuje direktor, razen če takega dovoljenja ni mogoče pridobiti zaradi neposrednega ali resnega ogrožanja varnosti oseb ali premoženja ali nacionalne varnosti (v tem primeru je treba o tem čim prej obvestiti direktorja ali drugo pooblaščeno osebo). V primeru nespoštovanja smernic mora FBI o tem obvestiti ministrstvo za pravosodje, ki nato obvesti pravosodnega ministra in namestnika pravosodnega ministra.

([172]) Glej Prilogo VI, opomba 2. Glej, na primer, tudi zadevo Arnold proti mestu Cleveland,67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) („Na področjih pravic posameznikov in državljanskih svoboščin ustava Združenih držav Amerike, kolikor velja za države, določa prag, pod katerega se odločbe državnih sodišč ne smejo spustiti“); zadevo Cooper proti Kaliforniji, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) („Naša ugotovitev seveda ne vpliva na pristojnost države, da uvede višje standarde za preiskave in zasege, kot jih zahteva zvezna ustava, če se za to odloči.“); Petersen proti mestu Mesa, 63 P.3d 309, 312 (Pritožbeno sodišče Arizone, 2003) („Čeprav se lahko z ustavo Arizone uvedejo strožji standardi za preiskave in zasege, kot so določeni z zvezno ustavo, sodišča v Arizoni ne smejo zagotavljati manjše zaščite, kot je določena s četrtim amandmajem“).

([173]) Večina držav je zaščito iz četrtega amandmaja ponovila v svojih ustavah. Glej ustavo Alabame, člen I, odstavek 5; ustavo Alaske, člen I, odstavek 14; 1; ustavo Arkansasa, člen II, odstavek 15; ustavo Kalifornije, člen I, odstavek 13; ustavo Kolorada, člen II, odstavek 7; ustavo Conneticuta, člen I, odstavek 7; ustavo Delawara, člen I, odstavek 6; ustavo Floride, člen I, odstavek 12; ustavo Georgie, člen I, odstavek I, točka XIII; ustavo Havajev, člen I, odstavek 7; ustavo Idaha, člen I, odstavek 17; ustavo Illinoisa, člen I, odstavek 6; ustavo Indiane, člen I, odstavek 11; ustavo Iowe, člen I, odstavek 8; listino o pravicah iz ustave Kansasa, člen 15; Ustavo Kentuckyja, člen 10; ustavo Louisiane, člen I, odstavek 5; ustavo Maina, člen I, odstavek 5; deklaracijo o pravicah iz ustave Massachusetsa, člen 14; ustavo Michigana, člen I, odstavek 11; ustavo Minnesote, člen I, odstavek 10; ustavo Misisipija, člen III, odstavek 23; ustavo Missourija, člen I, odstavek 15; ustavo Montane, člen II, odstavek 11; ustavo Nebraske, člen I, odstavek 7; ustavo Nevade, člen I, odstavek 18; ustavo New Hampshira, del 1, člen 19; ustavo New Jeseya, člen II, odstavek 7; ustavo New Mexica, člen II, odstavek 10; ustavo New Yorka, člen I, odstavek 12; ustavo Severne Dakote, člen I, odstavek 8; ustavo Ohia, člen I, odstavek 14; ustavo Oklahome, člen II, odstavek 30; ustavo Oregona, člen I, odstavek 9; ustavo Pensilvanije, člen I, odstavek 8; ustavo Rhode Islanda, člen I, odstavek 6; ustavo Južne Karoline, člen I, odstavek 10; ustavo Južne Dakote, člen VI, odstavek 11; ustavo Tennesseeja, člen I, odstavek 7; ustavo Teksasa, člen I, odstavek 9; ustavo Utaha, člen I, odstavek 14; ustavo Vermonta, poglavje I, člen 11; ustavo Zahodne Virginije, člen III, odstavek 6; ustavo Wisconsina, člen I, odstavek 11; ustavo Wyominga, člen I, odstavek 4. Druge države (npr. Maryland, Severna Karolina in Virginija) so v svoje ustave vključile posebna besedila v zvezi z nalogi, ki se sodno razlagajo tako, da zagotavljajo podobno ali višjo zaščito kot četrti amandma (glej deklaracijo o pravicah Marylanda, člen 26; ustavo Severne Karoline, člen I, odstavek 20; ustavo Virginije, člen I, odstavek 10 in zadevno sodno prakso, npr. Hamel proti državi, 943 A.2d 686, 701 (specialno pritožbeno sodišče Marylanda, 2008; Država proti Johnson, 861 S.E.2d 474, 483 (Severna Karolina 2021) in Lowe v. Commonwealthu, 337 S.E.2d 273, 274 (Virginija. 1985)). Poleg tega imata Arizona in Washington ustavne določbe, ki na bolj splošno varujejo zasebnost (ustava Arizone, člen 2, odstavek 8; Ustava Washingtona, člen I, odstavek 7), ki so jih sodišča razlagala tako, da zagotavljajo več zaščite kot četrti amandma (glej npr. Država proti Bolt, 689 P.2d 519, 523 (Arizona 1984), Država proti Ault, 759 P.2d 1320, 1324 (Arizona 1988), Država proti Myrick, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (Washington 1984), Država proti Young, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (Washington 1994)).

([174]) Glej npr. kalifornijski kazenski zakonik, člen 1524,3(b); člene 3.6–3.13 predpisov Alabame o kazenskem postopku; člen 10.79.035 spremenjenega zakonika Washingtona; oddelek 19.2-59 poglavja 5, naslova 19.2 virginijskega zakonika o kazenskem postopku.

3.1.1.2 *Nadaljnja uporaba zbranih informacij*

(101) Kar zadeva nadaljnjo uporabo zbranih podatkov s strani zveznih organov kazenskega pregona, nalagajo različni zakoni, smernice in standardi posebne zaščitne ukrepe. Z izjemo posebnih instrumentov, ki se uporabljajo za dejavnosti FBI (AGG-DOM in Navodila FBI za nacionalne preiskave in operacije), se zahteve, opisane v tem oddelku, na splošno uporabljajo za nadaljnjo uporabo podatkov s strani katerega koli zveznega organa, tudi podatkov, do katerih se dostopa v civilne ali regulativne namene. To vključuje zahteve, ki izhajajo iz obvestil/predpisov Urada za upravljanje in proračun, zveznega zakona o posodobitvi upravljanja informacijske varnosti, zakona o e-upravi in zakona o evidencah zveznih agencij.

(102) V skladu s pooblastilom, ki ga določata zakon Clinger-Cohen (*Clinger-Cohen Act*) (javno pravo 104–106, oddelek E) in zakon o računalniški varnosti iz leta 1987 (*Computer Security Act*) (javno pravo 100–235) je Urad za upravljanje in proračun (*Office of Management and Budget*, v nadaljnjem besedilu: OMB) izdal Okrožnico št. A-130, v kateri je določil splošne zavezujoče smernice, ki se uporabljajo za vse zvezne agencije (vključno z organi pregona) pri ravnanju z osebno določljivimi podatki ([175]). Okrožnica zlasti zahteva, da vse zvezne agencije „omejijo ustvarjanje, zbiranje, uporabo, obdelavo, shranjevanje, ohranjanje, razširjanje in razkrivanje osebno določljivih podatkov na tisto, kar je pravno dovoljeno, ustrezno in kar se razumno šteje za potrebno za pravilno izvajanje pooblaščenih nalog agencije“ ([176]). Poleg tega morajo zvezne agencije v razumno izvedljivi meri zagotoviti, da so osebno določljivi podatki točni, ustrezni, pravočasni in popolni in omejeni na minimum, ki je potreben za pravilno izvajanje nalog agencije. Splošneje morajo zvezne agencije vzpostaviti celovit program za varstvo zasebnosti, da bi zagotovile skladnost z veljavnimi zahtevami glede varstva zasebnosti, razviti in oceniti politike zasebnosti ter obvladovati tveganja za varstvo zasebnosti; upravljati postopke za odkrivanje in dokumentiranje primerov nespoštovanja zasebnosti ter poročanje o njih; ozaveščati o varstvu zasebnosti in razviti programe usposabljanja za zaposlene in pogodbene izvajalce ter vzpostaviti politike in postopke za zagotovitev, da je osebje odgovorno za izpolnjevanje zahtev in politik glede varstva zasebnosti ([177]).

(103) Poleg tega zakon o e-upravi (*E-Government Act*) ([178]) zahteva od vseh zveznih agencij (vključno z organi kazenskega pregona), da vzpostavijo varstvo informacijske varnosti, ki je sorazmerno s tveganjem in obsegom škode, ki bi nastala zaradi nepooblaščenega dostopa, uporabe, razkritja, motenj, spremembe ali uničenja; imeti glavnega uradnika za informiranje za zagotovitev izpolnjevanja zahtev glede informacijske varnosti in izvajati letna neodvisna ocenjevanja (npr. s strani generalnega inšpektorja, glej uvodno izjavo 109) svojega programa in praks informacijske varnosti ([179]). Podobno zvezni zakon o evidencah zveznih agencij (*Federal Records Act*, v nadaljnjem besedilu: FRA) ([180]) in dopolnilni predpisi ([181]) zahtevajo, da so informacije, ki jih hranijo zvezne agencije predmet zaščitnih ukrepih, s katerimi se zagotavljata fizična celovitost informacij in varstvo pred nepooblaščenim dostopom do njih.

(104) V skladu z zveznim zakonskim pooblastilom, vključno z zveznim zakonom o posodobitvi informacijske varnosti iz leta 2014 (*Federal Information Security Modernisation Act*), sta OMB in Nacionalni inštitut za standarde in tehnologijo (*National Institute of Standards and Technology*, v nadaljnjem besedilu: NIST) razvila standarde, ki so zavezujoči za zvezne agencije (vključno z organi kazenskega pregona) in v katerih so podrobneje navedene minimalne zahteve glede informacijske varnosti, ki jih je treba uvesti, vključno z nadzorom dostopa, zagotavljanjem ozaveščanja in usposabljanja, načrtovanjem ravnanja v izrednih razmerah, odzivanjem na incidente, orodji za revizije in odgovornost, zagotavljanjem celovitosti sistemov in informacij, izvajanjem ocen tveganja na področju varstva zasebnosti in varnosti itd. ([182]). Poleg tega morajo vse zvezne agencije (vključno z organi kazenskega pregona)

([175]) Tj. „podatki, ki se lahko uporabijo za razlikovanje ali sledenje posameznikove identitete, bodisi samostojno bodisi skupaj z drugimi podatki, ki so povezano ali povezljivo s konkretnim posameznikom“, glej Okrožnico OMB št. A-130, str. 33 (opredelitev „osebno določljivih podatkov“).

([176]) Okrožnica OMB št. A-130, „Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information“ (Upravljanje informacij kot strateškega vira, Dodatek II, Pristojnosti za osebno določljive podatke), 81 Fed. Reg. 49,689 (28. julij 2016), str. 17.

([177]) Člen 5(a)–(h), v Dodatku II.

([178]) Poglavje 36 naslova 44 zakonodajne zbirke ZDA.

([179]) Členi 3544–3545 naslova 44 zakonodajne zbirke ZDA.

([180]) FAC, člen 3105 naslova 44 zakonodajne zbirke ZDA.

([181]) Člen 1228,150 in naslednji zbirke zveznih predpisov št. 36, 1228,228, in Dodatek A.

([182]) Glej npr. Okrožnico OMB št. A-130; NIST SP 800-53, Rev. 5, „Security and Privacy Controls for Information Systems and Organizations“ (Nadzor varnosti in varstva zasebnosti za informacijske sisteme in organizacije) (10. december 2020) in „NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems“ (Standardi NIST za obdelavo zveznih informacij 200: minimalne varnostne zahteve za zvezne informacije in informacijske sisteme).

v skladu s smernicami OMB ohranjati in izvajati načrt za obravnavanje kršitev varnosti podatkov, tudi ko gre za odzivanje na take kršitve in ocenjevanje tveganj škode ([183]).

(105) Kar zadeva hrambo podatkov, FRA ([184]) od ameriških zveznih agencij (vključno z organi kazenskega pregona) zahteva, da določijo roke za hrambo (po izteku katerih morajo biti take evidence odstranjene), ki jih mora odobriti Uprava za nacionalne arhive in evidence (*National Archives and Record Administration*) ([185]). Trajanje roka za hrambo je določen glede na različne dejavnike, kot so vrsta preiskave, ali se dokazi še vedno nanašajo na preiskavo itd. AGG-DOM v zvezi z FBI določa, da mora FBI imeti vzpostavljen tak načrt hrambe evidenc in ohranjati sistem, ki omogoča takojšen priklic statusa preiskav in podlage zanje.

(106) Nazadnje, Okrožnica OMB št. A-130 vsebuje tudi nekatere zahteve za razširjanje osebno določljivih podatkov. Načeloma morata biti razširjanje in razkrivanje informacij, ki omogočajo identifikacijo posameznika, omejena na to, kar je zakonsko dovoljeno, ustrezno in razumno potrebno za pravilno izvajanje nalog agencije ([186]). Pri izmenjavi osebno določljivih podatkov z drugimi subjekti vlade morajo ameriške zvezne agencije po potrebi naložiti pogoje (vključno z izvajanjem posebnega nadzora varnosti in varstva zasebnosti), ki urejajo obdelavo informacij s pisnim soglasjem (vključno s pogodbami, sporazumi o uporabi podatkov, sporazumi o izmenjavi informacij in memorandumi o soglasju) ([187]). Kar zadeva razloge, na podlagi katerih se lahko informacije razširjajo, je v vodniku AGG-DOM in Navodilih FBI za nacionalne preiskave in operacije ([188]) na primer določeno, da je lahko FBI pravno zavezan, da to stori (npr. na podlagi mednarodnega sporazuma), ali da lahko v določenih okoliščinah razširja informacije, npr. drugim agencijam ZDA, če je razkritje združljivo z namenom, za katerega so bile informacije zbrane, in je povezano z njihovimi nalogami, kongresnim odborom, tujim agencijam, če so informacije povezane z njihovimi nalogami in je razširjanje v skladu z interesi Združenih držav, če je razširjanje zlasti potrebno za zaščito varnosti oseb ali premoženja ali za zaščito pred kaznivim dejanjem ali grožnjo za nacionalno varnost ali za njeno preprečevanje, razkritje pa je združljivo z namenom, za katerega so bile informacije zbrane ([189]).

3.1.2 ***Nadzor***

(107) Dejavnosti zveznih organov kazenskega pregona so predmet nadzora različnih organov ([190]). Kot je pojasnjeno v uvodnih izjavah 92–99, to v večini primerov vključuje predhodni sodni nadzor, s katerim je treba odobriti posamezne ukrepe za zbiranje, preden se lahko uporabijo. Poleg tega drugi organi nadzorujejo različne faze dejavnosti organov kazenskega pregona, vključno z zbiranjem in obdelavo osebnih podatkov. Ti sodni in nesodni organi skupaj zagotavljajo neodvisen nadzor nad organi kazenskega pregona.

([183]) Memorandum 17–12, „Preparing for and Responding to a Breach of Personally Identifiable Information“ (Priprava in odzivanje na kršitev varnosti osebno določljivih podatkov), na voljo na naslovu https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf in Okrožnica OMB št. A-130. Na primer, postopki za odzivanje ministrstva za pravosodje na kršitve varnosti podatkov, glej https://www.justice.gov/file/4336/download.

([184]) FRA, člen 3101 in naslednji naslova 44 zakonodajne zbirke ZDA.

([185]) Uprava za nacionalne arhive in evidence ima pooblastilo za ocenjevanje praks upravljanja evidenc agencij in lahko določi, ali je nadaljnja hramba nekaterih evidenc upravičena (člena 2904(c), 2906 naslova 44 zakonodajne zbirke ZDA).

([186]) Člen 5.f.1.(d) Okrožnice OMB št. A-130.

([187]) Člen 3(d) v Dodatku I k Okrožnici OMB št. A-130.

([188]) Glej tudi člen 14 Navodil FBI za nacionalne preiskave in operacije (DIOG).

([189]) AGG-DOM, Oddelek VI, B in C; člen 14 Navodil FBI za nacionalne preiskave in operacije (DIOG).

([190]) Mehanizmi, navedeni v tem oddelku, se uporabljajo tudi za zbiranje in uporabo podatkov s strani zveznih organov za civilne in regulativne namene. Zvezne civilne in regulativne agencije nadzorujejo njihovi generalni inšpektorji ter Kongres, vključno z uradom za odgovornost vlade, ki je revizijska in preiskovalna agencija Kongresa. Razen če je agencija imenovala uradnika za zasebnost in državljanske svoboščine – položaj, ki ga zaradi svojih pristojnosti na področju kazenskega pregona in nacionalne varnosti običajno imajo agencije, kot sta ministrstvo za pravosodje in ministrstvo za domovinsko varnost (*Department of Homeland Security*, v nadaljnjem besedilu: DHS), je za te naloge pristojen višji uradnik za agencije za področje zasebnosti (*Senior Agency Official for Privacy*, v nadaljnjem besedilu: SAOP). Vse zvezne agencije so pravno zavezane, da imenujejo SAOP, ki je odgovoren za zagotavljanje skladnosti agencije z zakoni o zasebnosti in nadzor nad s tem povezanimi zadevami. Glej npr. OMB M-16–24, Vloga in imenovanje višjih uradnikov agencije za področje zasebnosti (2016).

(108) Prvič, uradniki za varstvo zasebnosti in državljanskih svoboščin obstajajo na različnih ministrstvih, pristojnih za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ([191]). 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 vidike, povezane z varstvom zasebnosti ali državljanskih svoboščin, in da ima vzpostavljene ustrezne postopke za obravnavo pritožb posameznikov, ki menijo, da je bilo kršeno varstvo njihove zasebnosti ali državljanskih svoboščin. Vodje vsakega ministrstva ali agencije morajo zagotoviti, da imajo uradniki za varstvo zasebnosti in državljanskih svoboščin gradivo in vire za izpolnjevanje svojih pooblastil, da jim je zagotovljen dostop do vsega gradiva in osebja, potrebnega za opravljanje njihovih nalog, da so seznanjeni s predlaganimi spremembami politike in da se o slednjih opravijo posvetovanja z njimi ([192]). Uradniki za varstvo zasebnosti in državljanskih svoboščin redno poročajo Kongresu, tudi o številu in naravi pritožb, ki jih prejme ministrstvo/agencija in povzetku obravnave takih pritožb, opravljenih pregledih in preiskavah ter vplivu dejavnosti, ki jih je izvedel uradnik ([193]).

(109) Drugič, neodvisni generalni inšpektor nadzoruje dejavnosti ministrstva za pravosodje, vključno z FBI ([194]). Generalni inšpektorji so po zakonu neodvisni ([195]) in pristojni za izvajanje neodvisnih preiskav, revizij in inšpekcijskih pregledov programov in dejavnosti Ministrstva. Imajo dostop do vseh evidenc, poročil, revizij, pregledov, dokumentov, spisov, priporočil ali drugega ustreznega gradiva, po potrebi s sodnim pozivom, in lahko opravljajo zaslišanja ([196]). Čeprav generalni inšpektorji izdajajo samo nezavezujoča priporočila za popravne ukrepe, so njihova poročila, vključno s poročili o nadaljnjih ukrepih (ali odsotnosti ukrepov) ([197]), na splošno objavljena in poslana Kongresu, ki lahko na podlagi teh poročil opravlja svojo nadzorno funkcijo (glej uvodno izjavo 111) ([198]).

([191]) Glej člen 2000ee-1 naslova 42 zakonodajne zbirke ZDA. To vključuje na primer ministrstvo za pravosodje, Ministrstvo za domovinsko varnost ZDA (*Department of Homeland Security*, v nadaljnjem besedilu: ministrstvo za domovinsko varnost) in FBI. Poleg tega je na ministrstvu za domovinsko varnost glavni uradnik za varstvo zasebnosti pristojen za ohranjanje in krepitev varstva zasebnosti in spodbujanje preglednosti na Ministrstvu (člen 142, oddelek 222, naslova 6 zakonodajne zbirke ZDA). Vsi sistemi, vsa tehnologija, vse oblike in programi ministrstva za domovinsko varnost, pri katerih se zbirajo osebni podatki ali ki vplivajo na zasebnost, so predmet nadzora glavnega uradnika za varstvo zasebnosti, ki ima dostop do vseh evidenc, poročil, revizij, pregledov, dokumentov, spisov, priporočil in drugega gradiva, ki so na voljo Ministrstvu, in po potrebi s sodnim pozivom. Uradnik za varstvo zasebnosti mora letno poročati Kongresu o dejavnostih Ministrstva, ki vplivajo na zasebnost, vključno s pritožbami zaradi kršitev varstva zasebnosti.

([192]) Člen 2000ee-1(d) naslova 42 zakonodajne zbirke ZDA.

([193]) Glej člen 2000ee-1(f)(1)–(2) naslova 42 zakonodajne zbirke ZDA. Na primer, poročilo glavnega uradnika pri ministrstvu za pravosodje za varstvo zasebnosti in državljanskih svoboščin in glavnega uradnika za varstvo zasebnosti in državljanskih svoboščin, ki zajema obdobje od oktobra 2020 do marca 2021, kaže, da je bilo izvedenih 389 pregledov varstva zasebnosti, vključno z informacijskimi sistemi in drugimi programi (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) Podobno je bil z zakonom o domovinski varnosti iz leta 2002 (*Homeland Security Act*) ustanovljen Urad generalnega inšpektorja pri ministrstvu za domovinsko varnost.

([195]) Generalni inšpektorji imajo varen mandat in jih lahko razreši samo predsednik, ki mora pisno sporočiti Kongresu razloge za tako razrešitev.

([196]) Glej zakon o generalnih inšpektorjih iz leta 1978 (*Inspector General Act*), člen 6.

([197]) V zvezi s tem glej na primer pregled, ki ga je pripravil Urad generalnega inšpektorja pri ministrstvu za pravosodje v zvezi s svojimi priporočili in z obsegom, v katerem so se izvajala z nadaljnjimi ukrepi ministrstva in agencije, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

([198]) Glej zakon o generalnih inšpektorjih iz leta 1978, člena 4(5), 5. Na primer, Urad generalnega inšpektorja pri ministrstvu za pravosodje je nedavno objavil svoje polletno poročilo Kongresu (1. oktober 2021–31. marec 2022, https://oig.justice.gov/node/23596), ki zagotavlja pregled njegovih revizij, ocenjevanj, inšpekcijskih pregledov, posebnih pregledov in preiskav programov in dejavnosti ministrstva za pravosodje . Te dejavnosti so vključevale preiskavo nekdanjega pogodbenega izvajalca v zvezi z nezakonitim razkritjem elektronskega nadzora (prisluškovanja posamezniku) v tekoči preiskavi, ki je pripeljala do obsodbe pogodbenega izvajalca. Urad generalnega inšpektorja je vodil tudi preiskavo programov in praks agencij ministrstva za pravosodje za informacijsko varnost, ki vključuje preskušanje učinkovitosti politik in postopkov informacijske varnosti ter praks reprezentativnega podsklopa sistemov agencij.

(110) Tretjič, v obsegu, v katerem izvajajo protiteroristične dejavnosti, so oddelki s pristojnostmi kazenskega pregona pod nadzorom Nadzornega odbora za zasebnost in državljanske svoboščine (*Privacy and Civil Liberties Oversight Board*, v nadaljnjem besedilu: PCLOB), ki je neodvisna agencija v okviru izvršilne veje oblasti, sestavljena iz dvostrankarskega, petčlanskega odbora, ki ga imenuje Predsednik za fiksen šestletni mandat s soglasjem Senata ([199]). V skladu z njegovim statutom o ustanovitvi so PCLOB podeljena pooblastila na področju politik boja proti terorizmu in njihovega izvajanja z namenom varstva zasebnosti in državljanskih svoboščin. Pri pregledu lahko dostopa do vseh ustreznih evidenc, poročil, revizij, pregledov, dokumentov, spisov in priporočil agencije, vključno z zaupnimi informacijami, opravlja pogovore in prisostvuje zaslišanjem ([200]). Prejema poročila uradnikov za varstvo zasebnosti in državljanskih svoboščin več zveznih ministrstev/agencij ([201]), lahko izdaja priporočila vladi in organom kazenskega pregona ter redno poroča kongresnim odborom in predsedniku ([202]). Poročila odboru, vključno s poročili Kongresu, morajo biti čim bolj javno dostopna ([203]).

(111) Nazadnje, dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj so predmet nadzora posebnih odborov ameriškega Kongresa (odbori spodnjega doma in senata za pravosodje). Odbori za pravosodje na različne načine izvajajo redni nadzor, zlasti z obravnavami, preiskavami, pregledi in poročili ([204]).

3.1.3. ***Pravna sredstva***

(112) Kot je navedeno, morajo organi kazenskega pregona za zbiranje osebnih podatkov v večini primerov pridobiti predhodno sodno odobritev. Čeprav ta za upravne sodne pozive ni potrebna, so ti omejeni na posebne primere in bodo predmet neodvisnega sodnega nadzora vsaj v primerih, ko vlada zahteva izvršilni postopek pred sodiščem. Zlasti lahko prejemniki upravnih sodnih pozivov izpodbijajo te pozive pred sodiščem z utemeljitvijo, da so nerazumni, tj. preširoki, zatirajoči ali obremenjujoči ([205]).

(113) Posamezniki lahko pri organih kazenskega pregona najprej vložijo zahtevke ali pritožbe v zvezi z obdelavo svojih osebnih podatkov. To vključuje možnost, da se zahteva dostop do osebnih podatkov in njihov popravek ([206]). V zvezi z dejavnostmi, povezanimi z bojem proti terorizmu, lahko posamezniki vložijo pritožbo tudi pri uradnikih za zasebnost in državljanske svoboščine (ali drugih uradnikih za varstvo zasebnosti) v okviru organov kazenskega pregona ([207]).

(114) 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 ([208]). Te možnosti, ki vključujejo zlasti APA, zakon o dostopu do informacij javnega značaja (*Freedom of Information Act*, v nadaljnjem besedilu: FOIA) in zakon o zasebnosti elektronskih komunikacij (*Electronic Communications Privacy Act*, v nadaljnjem besedilu: ECPA), so na voljo vsem posameznikom, ne glede na njihovo državljanstvo, v skladu z morebitnimi veljavnimi pogoji.

([199]) Člani odbora morajo biti izbrani izključno na podlagi njihovih poklicnih kvalifikacij, dosežkov, javne podobe, strokovnega znanja na področju varstva zasebnosti in državljanskih svoboščin, ter ustreznih izkušenj in ne glede na politično pripadnost. V nobenem primeru ne smejo biti v odboru več kot trije člani, ki pripadajo isti politični stranki. Posameznik, imenovan v odbor, v času opravljanja funkcije člana odbora ne sme biti izvoljeni uslužbenec, uradnik ali zaposleni zvezne vlade, razen v svojstvu člana odbora. Glej člen 2000ee (h) naslova 42 zakonodajne zbirke ZDA.

([200]) Člen 2000ee (g) naslova 42 zakonodajne zbirke ZDA.

([201]) Glej člen 2000ee-1 (f)(1)(A)(iii) naslova 42 zakonodajne zbirke ZDA. Mednje sodijo ministrstvo za pravosodje, ministrstvo za obrambo, ministrstvo za domovinsko varnost in vsa druga ministrstva, agencije ali organi izvršilne oblasti, ki jih imenuje Odbor za nadzor zasebnosti in državljanskih svoboščin in jih je primerno vključiti.

([202]) Člen 2000ee (e) naslova 42 zakonodajne zbirke ZDA.

([203]) Člen 2000ee (f) naslova 42 zakonodajne zbirke ZDA.

([204]) Na primer, odbori organizirajo tematske obravnave (glej npr. nedavno obravnavo odbora spodnjega doma za pravosodje o „digitalnih mrežah za prestrezanje“, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), pa tudi obravnave rednega nadzora, npr. nadzora nad FBI in ministrstvom za pravosodje, glej https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 in https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

([205]) Glej Prilogo VI.

([206]) Okrožnica OMB št. A-130, Dodatek II, oddelek 3(a) in (f), ki od zveznih agencij zahteva, da na zahtevo posameznikov zagotovijo ustrezen dostop in popravke ter vzpostavijo postopke za sprejemanje in obravnavanje pritožb in zahtevkov v zvezi z zasebnostjo.

([207]) Glej člen 2000ee-1 naslova 42 zakonodajne zbirke ZDA, na primer v zvezi z ministrstvom za pravosodje in ministrstvom za domovinsko varnost. Glej tudi Memorandum OMB M-16–24, Vloga in imenovanje višjih uradnikov agencije za področje zasebnosti (2016).

([208]) Mehanizmi pravnih sredstev, navedeni v tem oddelku, se uporabljajo tudi za zbiranje in uporabo podatkov s strani zveznih organov za civilne in regulativne namene.

(115) Na splošno ima v skladu z določbami APA ([209]) o sodnem nadzoru „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 sodni nadzor ([210]). To vključuje možnost, da se sodišču predlaga, naj „ugotovi, da so ukrepanje, ugotovitve in sklepi agencije, za katere je bilo ugotovljeno, da so […] samovoljni, arbitrarni, da predstavljajo zlorabo diskrecijske pravice ali so drugače neskladni s pravom, nezakoniti in jih razveljavi“ ([211]).

(116) Natančneje, naslov II ECPA ([212]) 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 ([213]). 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 zadevnega posameznika, saj lahko vloži civilno tožbo pri zveznem sodišču ZDA za dejansko in kaznovalno odškodnino ter za pravično nadomestilo ali ugotovitveno odločbo zoper vladnega uslužbenca, ki je namerno storil taka nezakonita dajanja, ali Združene države.

(117) Poleg tega več drugih zakonov zagotavlja posameznikom pravico, da vložijo tožbo zoper javni organ ali uslužbenca ZDA zaradi obdelave njihovih osebnih podatkov; taki zakoni so zakon o prisluškovanju telefonskim pogovorom) ([214]), zakon o računalniških goljufijah in zlorabah (*Computer Fraud and Abuse Act*) ([215]), zvezni zakon o odškodninskih zahtevkih (*Federal Torts Claim Act*) ([216]), zakon o pravici do finančne zasebnosti (*Right to Financial Privacy Act*) ([217]) in FCRA ([218]).

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

([210]) Na splošno se sodni nadzor opravi le za „končno“ ukrepanje agencije in ne za „predhodno, postopkovno ali vmesno“ ukrepanje agencije. Glej Člen 704 naslova 5 zakonodajne zbirke ZDA.

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

([212]) Členi 2701–2712 naslova 18 zakonodajne zbirke ZDA.

([213]) ECPA 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; (ii) storitev daljinske obdelave, kot so storitve računalniškega shranjevanja ali obdelave.

([214]) V skladu z zakonom o prisluškovanju telefonskim pogovorom, členi 2510 in naslednji naslova 18 zakonodajne zbirke ZDA (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 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*) naslova 18 (členi 3121 do 3127 naslova 18 zakonodajne zbirke ZDA ter člen 2707 v zvezi s civilno tožbo).

([215]) Člen 1030 naslova 18 zakonodajne zbirke ZDA. V skladu z zakonom o računalniških goljufijah in zlorabah lahko oseba toži vsakega posameznika zaradi namernega nepooblaščenega dostopa (ali dostopa, ki presega pooblastila), da bi pridobila informacije od finančne institucije, računalniškega sistema vlade ZDA ali drugega navedenega računalnika, v nekaterih primerih tudi proti posameznemu vladnemu uslužbencu.

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

([217]) Člen 3401 naslova 12 zakonodajne zbirke ZDA in naslednji. V skladu z zakonom o pravici do finančne zasebnosti lahko oseba v nekaterih 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 sodni poziv ali nalog za preiskavo ali v skladu z omejitvami uradno ustno zahtevo in če je posameznik, čigar informacije se zahtevajo, obveščen o taki zahtevi.

([218]) Členi 1681 do 1681x naslova 15 zakonodajne zbirke ZDA. V skladu s FCRA lahko oseba toži kogar koli, ki ne izpolnjuje zahtev (zlasti zahteve po zakonitem dovoljenju) glede zbiranja, razširjanja in uporabe poročil o kreditni sposobnosti potrošnika, ali v nekaterih primerih vladno agencijo.

(118) Poleg tega ima v skladu s FOIA ([219]), člen 552 naslova 5 zakonodajne zbirke ZDA, vsaka oseba pravico do dostopa do evidenc zvezne agencije, tudi če vsebujejo osebne podatke posameznika. Po izčrpanju upravnih pravnih sredstev lahko posameznik tako pravico do dostopa uveljavlja na sodišču, razen če navedene evidence pred javnim razkritjem varuje izjema ali posebno izvzetje za organe kazenskega pregona ([220]). V tem primeru bo sodišče ocenilo, ali zadevni javni organ uporablja izjemo oziroma ali se je nanjo zakonito skliceval.

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

(119) Pravo Združenih držav vsebuje različne omejitve in zaščitne ukrepe glede dostopa do osebnih podatkov in njihove uporabe za namene nacionalne varnosti ter zagotavlja nadzorne mehanizme in mehanizme pravnih sredstev, ki so v skladu z zahtevami iz uvodne izjave 89 tega sklepa. Pogoji, pod katerimi je tak dostop mogoč, in zaščitni ukrepi glede uporabe teh pooblastil so podrobneje ocenjeni v naslednjih oddelkih.

3.2.1 ***Pravna podlaga, omejitve in zaščitni ukrepi***

3.2.1.1 *Veljavni pravni okvir*

(120) Osebni podatki, ki se prenašajo iz Unije v organizacije DPF EU-ZDA lahko zbirajo organi ZDA za namene nacionalne varnosti dovoljen na podlagi različnih pravnih instrumentov, so predmet posebnih pogojev in zaščitnih ukrepov.

(121) Ko so osebni podatki preneseni v organizacije v Združenih državah, lahko obveščevalne agencije ZDA zahtevajo dostop do takih podatkov za namene nacionalne varnosti le, kot je dovoljeno z zakonom, natančneje v skladu z zakonom o nadzoru tujih obveščevalnih podatkov (*Foreign Intelligence Surveillance Act*, v nadaljnjem besedilu: FISA), ali zakonskimi določbami, ki dovoljujejo dostop prek sodnih pozivov v zvezi z nacionalno varnostjo (*National Security Letters*, v nadaljnjem besedilu: NSL) ([221]). FISA vsebuje več pravnih podlag, ki se lahko uporabijo za zbiranje (in naknadno obdelavo) osebnih podatkov posameznikov iz Unije, na katere se nanašajo osebni podatki, ki se prenašajo na podlagi DPF EU-ZDA (člen 105 ([222]) FISA, člen 302 FISA ([223]), člen 402 FISA ([224]), člen 501 FISA ([225]) in člen 702 FISA ([226])), kot je podrobneje opisano v uvodnih izjavah 142–152.

([219]) Člen 552 naslova 5 zakonodajne zbirke ZDA.

([220]) Vendar so taka izvzetja opredeljena. Na primer v skladu s členom 552 (b)(7) naslova 5 zakonodajne zbirke ZDA so pravice iz FOIA izključene 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 oseba prikrajšana za pravico do poštenega ali nepristranskega sojenja, (C) če se lahko razumno pričakuje, da bo pomenila neupravičen poseg v zasebnost, (D) če se lahko razumno pričakuje, da bo razkrita identiteta zaupnega vira, vključno z državno, lokalno ali tujo agencijo ali organom ali katero koli zasebno institucijo, ki je zaupno priskrbela informacije, in, v primeru evidence ali informacij, ki jih je zbral organ kazenskega pregona med kazensko preiskavo, ali agencija, ki vodi zakonito obveščevalno preiskavo za zagotavljanje nacionalne varnosti, informacije, ki jih je priskrbel zaupni vir, (E) če bi se razkrile tehnike in postopki preiskav organov pregona ali pregona ali smernice za preiskave organov pregona 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 bo ogroženo življenje ali fizična varnost katerega koli posameznika“. Poleg tega, „[č]e se predloži zahteva, ki vključuje dostop do evidenc [kadar se lahko razumno pričakuje, da bi njihova priprava posegala v izvršilni postopek] in če (A) preiskava ali postopek vključuje morebitno kršitev kazenskega prava in če (B) obstaja razlog za sum, da (i) subjekt preiskave ali postopka ni seznanjen z njenim potekom in da (ii) bi bilo mogoče razumno pričakovati, da bo razkritje obstoja evidenc poseglo v izvršilni 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).

([221]) Člen 3414 naslova 12 zakonodajne zbirke ZDA; členi 1681u–1681v naslova 15 zakonodajne zbirke ZDA; in člen 2709 naslova 18 zakonodajne zbirke ZDA. Glej uvodno izjavo 153.

([222]) Člen 1804 naslova 50 zakonodajne zbirke ZDA, ki se nanaša na tradicionalno individualiziran elektronski nadzor.

([223]) Člen 1822 naslova 50 zakonodajne zbirke ZDA, ki se nanaša na fizične preiskave za namene tujih obveščevalnih služb.

([224]) Člen 1842 v povezavi s členom 1841(2) naslova 50 zakonodajne zbirke ZDA ter člen 3127 in naslova 18, ki se nanaša na namestitev snemalnikov klicev ali naprav za pasti in sledenje.

([225]) Člen 1861 naslova 50 zakonodajne zbirke ZDA, ki FBI omogoča, da vloži „vlogo za izdajo sklepa, ki dovoljuje, da mu javni prevoznik, javni objekt za nastanitev, fizično skladišče ali objekt za najem vozil izroči v posest evidence za preiskavo za zbiranje tujih obveščevalnih podatkov ali preiskavo, ki se nanaša na mednarodni terorizem“.

([226]) Člen 1881a naslova 50 zakonodajne zbirke ZDA, ki organom obveščevalne skupnosti ZDA omogoča, da od podjetij v ZDA zahtevajo dostop do podatkov, vključno z vsebino internetnih komunikacij, ki se nanašajo na nekatere nedržavljane ZDA zunaj ZDA, ob pravno zavezujoči pomoči ponudnikov storitev elektronskih komunikacij

(122) Obveščevalne agencije ZDA imajo tudi možnost zbiranja osebnih podatkov zunaj Združenih držav, med drugim osebnih podatkov v tranzitu med Unijo in Združenimi državami. Zbiranje zunaj Združenih držav temelji na Odredbi št. 12333 (Odredba št. 12333) ([227]), ki jo izda predsednik ([228]).

(123) Zbiranje SIGINT je oblika zbiranja obveščevalnih podatkov, ki je najustreznejša za sedanje ugotavljanje ustreznosti, saj se nanaša na zbiranje elektronskih komunikacij in podatke iz informacijskih sistemov. Tako zbiranje lahko izvajajo obveščevalne agencije ZDA v Združenih državah (na podlagi FISA) in tudi medtem, ko so podatki v tranzitu v Združene države (na podlagi Odredbe št. 12333).

(124) Predsednik ZDA je 7. oktobra 2022 izdal Odredbo št. 14086 o krepitvi zaščitnih ukrepov za obveščevalne dejavnosti SIGINT ZDA, ki določa omejitve in zaščitne ukrepe za vse obveščevalne dejavnosti SIGINT ZDA. Ta odredba v veliki meri nadomešča Predsedniško politično direktivo (*Presidential Policy Directive 28*, v nadaljnjem besedilu: PPD-28) ([229]), krepi pogoje, omejitve in zaščitne ukrepe, ki se uporabljajo za obveščevalne dejavnosti SIGINT (npr. na podlagi FISA in Odredbe št. 12333) ne glede na to, kje potekajo ([230]), in določa nov mehanizem pravnih sredstev, prek katerega lahko posamezniki uveljavijo in izvršijo te zaščitne ukrepe ([231]) (za več podrobnosti glej uvodne izjave 176 do 194). S tem v pravu ZDA izvaja rezultate pogovorov, ki so potekali med EU in ZDA po razveljavitvi sklepa Komisije o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit s strani Sodišča (glej uvodno izjavo 6). Zato je to posebno pomemben element pravnega okvira, ki se presoja v tem sklepu.

(125) Omejitve in zaščitni ukrepi, uvedeni z Odredbo št. 14086, dopolnjujejo omejitve in zaščitne ukrepe iz členov 702 FISA in Odredbe št. 12333. Obveščevalne agencije morajo pri izvajanju obveščevalnih dejavnosti SIGINT v skladu s členom 702 FISA in Odredbo št. 12333 uporabljati spodaj opisane zahteve (v oddelkih 3.2.1.2 in 3.2.1.3), npr. pri izbiri/identifikaciji kategorij tujih obveščevalnih podatkov, ki jih je treba pridobiti v skladu s členom 702 FISA, zbiranju tujih obveščevalnih podatkov ali protiobveščevalnih podatkov v skladu z Odredbo št. 12333 in sprejemanju odločitev o ciljnem osredotočanju na posameznike v skladu s členom 702 FISA in Odredbo št. 12333.

(126) Zahteve, določene v tej odredbi, ki jo je izdal predsednik, so zavezujoče za vso obveščevalno skupnost. Treba jih je treba nadalje izvajati s politikami in postopki agencije, s katerimi se prenašajo v konkretne smernice za vsakodnevno delovanje. V zvezi s tem imajo obveščevalne agencije ZDA na podlagi Odredbe št. 14086 največ eno leto časa, da posodobijo svoje obstoječe politike in postopke (tj. do 7. oktobra 2023) in jih uskladijo z zahtevami navedene odredbe. Take posodobljene politike in postopke je treba razviti v posvetovanju z generalnim državnim tožilcem, uradnikom za varstvo zasebnosti in državljanskih svoboščin z Urada za varstvo zasebnosti in državljanskih svoboščin v okviru Urada direktorja nacionalne obveščevalne službe (*Civil Liberties and Privacy Office of the Office of the Director of National Intelligence*, v nadaljnjem besedilu: ODNI CLPO) in PCLOB, tj. neodvisnim nadzornim organom, pooblaščenim za pregled politik izvršilne veje in njihovo izvajanje z namenom varstva zasebnosti in državljanskih svoboščin (v zvezi z vlogo in statusom PCLOB glej uvodno izjavo 110), in jih objaviti ([232]). Poleg tega bo PCLOB po uvedbi posodobljenih politik in postopkov izvedel pregled za zagotovitev, da

([227]) Odredba št. 12333: obveščevalne dejavnosti ZDA (*United States Intelligence Activities*), Zvezni register, zvezek 40, št. 235 (8. december 1981, kakor je bila spremenjena 30. julija 2008). Odredba št. 12333 splošneje opredeljuje cilje, usmeritve, naloge in pristojnosti v zvezi z obveščevalnimi prizadevanji ZDA (vključno z vlogo različnih organov obveščevalne skupnosti) ter določa splošne parametre za izvajanje obveščevalnih dejavnosti.

([228]) Na podlagi člen II ustave ZDA je za zagotavljanje nacionalne varnosti, vključno zlasti z zbiranjem tujih obveščevalnih podatkov, pristojen predsednik kot vrhovni poveljnik oboroženih sil.

([229]) Odredba št. 14086 nadomešča prejšnjo predsedniško direktivo, tj. PPD-28, razen njenega člena 3 in dopolnjujoče priloge (ki od obveščevalnih agencij zahteva, da letno pregledujejo svoje prednostne naloge in zahteve na področju obveščevalnih dejavnosti SIGINT, ob upoštevanju koristi obveščevalnih dejavnosti SIGINT za nacionalne interese ZDA ter tudi tveganj, ki jih predstavljajo navedene dejavnosti), in člena 6 (ki vsebuje splošne določbe), glej memorandum o nacionalni varnosti o delnem preklicu Predsedniške politične direktive 28, ki je na voljo na naslovu https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Glej člen 5(f) Odredbe št. 14086, ki pojasnjuje, da ima odredba enako področje uporabe kot PPD-28, ki se je v skladu z njegovo opombo 3 uporabljal za obveščevalno dejavnost SIGINT, ki se izvajajo za zbiranje komunikacij ali informacij o njih, razen obveščevalnih dejavnosti SIGINT, izvedenih za preskušanje ali razvoj zmogljivosti obveščevalnih dejavnosti SIGINT.

([231]) V zvezi s tem glej npr. člen 5(h) Odredbe št. 14086, ki pojasnjuje, da zaščitni ukrepi v odredbi pomenijo zakonito pravico in jih lahko zato posamezniki uveljavijo prek mehanizma pravnih sredstev.

([232]) Glej člen 2(c)(iv)(C) Odredbe št. 14086.

so skladni z Odredbo. V 180 dneh od zaključka takega pregleda PCLOB mora vsaka obveščevalna agencija skrbno preučiti in izvesti ali drugače obravnavati vsa priporočila PCLOB. Vlada ZDA je 3. julija 2023 objavila take posodobljene politike in postopke ([233]).

3.2.1.2 *Omejitve in zaščitni ukrepi v zvezi z zbiranjem osebnih podatkov za namene nacionalne varnosti*

(127) Odredba št. 14086 določa številne krovne zahteve, ki se uporabljajo za vse obveščevalne dejavnosti SIGINT (zbiranje, uporaba, razširjanje itd. osebnih podatkov).

(128) Prvič, take dejavnosti morajo temeljiti na zakonu ali predsedniškem pooblastilu in biti izvedene v skladu s pravom ZDA, vključno z ustavo ([234]).

(129) Drugič, vzpostavljeni morajo biti ustrezni zaščitni ukrepi za zagotovitev, da je varstvo zasebnosti in državljanskih svoboščin sestavni del premislekov pri načrtovanju takih dejavnosti ([235]).

(130) Zlasti se lahko vsaka obveščevalna dejavnost SIGINT izvaja le „po odločitvi, ki temelji na razumni presoji vseh ustreznih dejavnikov, da so dejavnosti potrebne za izboljšanje potrjenih prednostnih nalog obveščevalnih služb“ (v zvezi s pojmom „potrjene prednostne naloge obveščevalnih služb“ glej uvodno izjavo 135) ([236]).

(131) Poleg tega se lahko take dejavnosti izvajajo le „v obsegu in na način, ki je sorazmeren s potrjenimi prednostnimi nalogami obveščevalnih služb, za katere so bile dovoljene“ ([237]). Povedano drugače, treba je doseči ustrezno ravnovesje „med pomembnostjo uresničevane prednostne naloge obveščevalnih služb ter vplivom na varstvo zasebnosti in državljanskih svoboščin zadevnih posameznikov ne glede na njihovo državljanstvo ali prebivališče“ ([238]).

(132) Nazadnje, za zagotovitev skladnosti s temi splošnimi zahtevami, ki izražajo načela zakonitosti, nujnosti in sorazmernosti, so obveščevalne dejavnosti SIGINT predmet nadzora (za podrobnosti glej uvodne oddelek 3.2.2) ([239]).

(133) Te krovne zahteve so v zvezi z zbiranjem obveščevalnih podatkov v okviru SIGNIT dodatno utemeljene s številnimi pogoji in omejitvami, ki zagotavljajo, da je poseg v pravice posameznikov omejen na tisto, kar je potrebno in sorazmerno za izboljšanje zakonitega cilja.

(134) Prvič, Odredba omejuje razloge, na podlagi katerih se lahko podatki zbirajo v okviru obveščevalnih dejavnosti SIGINT, na dva načina. Po eni strani Odredba določa zakonite cilje, ki se lahko uresničujejo z zbiranjem obveščevalnih podatkov v okviru SIGNIT, npr. za razumevanje ali ocenjevanje zmogljivosti, namenov ali dejavnosti tujih organizacij, vključno z mednarodnimi terorističnimi organizacijami, ki predstavljajo sedanjo ali morebitno grožnjo za nacionalno varnost Združenih držav; za zaščito pred tujimi vojaškimi zmogljivostmi in dejavnostmi; za razumevanje ali ocenjevanje nadnacionalnih groženj, ki vplivajo na svetovno varnost, kot so podnebne in druge ekološke spremembe, tveganja za javno zdravje in humanitarne grožnje ([240]). Po drugi strani pa so v Odredbi navedeni nekateri cilji, ki se jih ne sme nikoli uresničevati z obveščevalnimi dejavnostmi SIGINT, npr. za namene

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

([234]) Člen 2(a)(i) Odredbe št. 14086.

([235]) Člen 2(a)(ii) Odredbe št. 14086.

([236]) Člen 2(a)(ii)(A) Odredbe št. 14086. Za to pa ni vedno potrebno, da je obveščevalna dejavnost SIGNIT edino sredstvo za izboljšanje vidikov potrjenih prednostnih nalog obveščevalnih služb. Zbiranje obveščevalnih podatkov v okviru SIGNIT se na primer lahko uporablja za zagotavljanje nadomestnih načinov potrjevanja (npr. za potrjevanje informacij, prejetih od drugih obveščevalnih virov ali za ohranjanje zanesljivega dostopa do enakih informacij) (člen 2(c)(i)(A) Odredbe št. 14086).

([237]) Člen 2(a)(ii)(B) Odredbe št. 14086.

([238]) Člen 2(a)(ii)(B) Odredbe št. 14086.

([239]) Člen 2(a)(iii) v povezavi s členom 2(d) Odredbe št. 14086.

([240]) Člen 2(b)(i) Odredbe št. 14086. Zaradi omejenega seznama zakonitih ciljev v Odredbi, ki ne zajema morebitnih prihodnjih groženj, Odredba omogoča Predsedniku, da ta seznam posodobi, če se pojavijo nove nacionalne varnostne zahteve, kot so nove grožnje za nacionalno varnost. Take posodobitve morajo biti načeloma objavljene, razen če predsednik odloči, da bi to samo po sebi pomenilo tveganje za nacionalno varnost Združenih držav (člen 2(b)(i)(B) Odredbe št. 14086).

obremenjevanja kritik, nestrinjanja ali svobode izražanja zamisli ali političnih mnenj s strani posameznikov ali medijev; za namene prikrajšanja ljudi na podlagi njihove narodnosti, rase, spola, spolne identitete, spolne usmerjenosti ali vere ali za zagotavljanje konkurenčne prednosti podjetjem iz ZDA ([241]).

(135) Poleg tega obveščevalne agencije zbiranja obveščevalnih podatkov v okviru SIGINT ne morejo upravičiti samo z zakonitimi cilji, določenimi v Odredbi št. 14086, temveč ga je treba za operativne namene dodatno utemeljiti s konkretnejšimi prednostnimi nalogami, za katere se lahko zbirajo obveščevalni podatki v okviru SIGINT. Povedano drugače, dejansko zbiranje lahko poteka le za izboljšanje bolj specifične prednostne naloge. Take prednostne naloge so določene v posebnem postopku, namenjenem zagotovitvi skladnosti z veljavnimi pravnimi zahtevami, vključno s tistimi, ki so povezane z varstvom zasebnosti in državljanskih svoboščin. Natančneje, obveščevalne prednostne naloge najprej razvije direktor nacionalne obveščevalne službe (prek t. i. okvira nacionalnih obveščevalnih prednostnih nalog) in ga predloži predsedniku v odobritev ([242]). Preden direktor predloži obveščevalne prednostne naloge predsedniku, mora v skladu z Odredbo št. 14086 od ODNI CLPO za vsako prednostno nalogo pridobiti oceno o tem, ali (1) ta izboljšuje enega ali več zakonitih ciljev, določenih v Odredbi; (2) ni bila zasnovana za zbiranje obveščevalnih podatkov v okviru SIGINT za prepovedan cilj, določen v Odredbi, niti se ne predvideva, da bo povzročila tako zbiranje in (3) je bila določena po ustreznem upoštevanju varstva zasebnosti in državljanskih svoboščin vseh ljudi ne glede na njihovo državljanstvo ali prebivališče ([243]). Če se direktor ne strinja z oceno CLPO, je treba predsedniku predložiti obe stališči ([244]).

(136) Zato ta postopek zlasti zagotavlja, da so vidiki varstva zasebnosti upoštevani od začetne faze razvoja prednostnih nalog obveščevalnih služb.

(137) Drugič, ko je bil prednostna naloga obveščevalnih služb določena, številne zahteve usmerjajo odločitev o tem, ali in v kakšnem obsegu se lahko zbirajo obveščevalni podatki v okviru SIGNIT za izboljšanje take prednostne naloge. Te zahteve operacionalizirajo krovno potrebo in standarde sorazmernosti, določene s členom 2(a) Odredbe.

(138) Zlasti se lahko obveščevalni podatki v okviru SIGINT zbirajo le „po ugotovitvi, da je na podlagi razumne presoje vseh ustreznih dejavnikov zbiranje potrebno za izboljšanje konkretne prednostne naloge obveščevalnih služb“ ([245]). Pri ugotavljanju, ali je konkretna dejavnost zbiranja obveščevalnih dejavnikov v okviru SIGINT potrebna za izboljšanje potrjenih prednostnih nalog obveščevalnih služb, morajo obveščevalne agencije ZDA upoštevati razpoložljivost, izvedljivost in ustreznost drugih manj vsiljivih virov in metod, vključno z diplomatskimi in javnimi viri ([246]). Kadar je taka alternativa na voljo, je treba dati prednost manj vsiljivim virom in metodam ([247]).

(139) Če se pri uporabi takih meril zbiranje SIGINT šteje za potrebno, mora biti „tako prilagojeno, kot je izvedljivo“ in „ne sme nesorazmerno vplivati na varstvo zasebnosti in državljanskih svoboščin“ ([248]). Za zagotovitev, da to ne vpliva nesorazmerno na varstvo zasebnosti in državljanskih svoboščin, tj. za vzpostavitev ustreznega ravnovesja med potrebami nacionalne varnosti in varstvom zasebnosti in državljanskih svoboščin, je treba ustrezno upoštevati vse ustrezne dejavnike, kot so narava uresničevanega cilja; vsiljivost dejavnosti zbiranja, vključno z njenim trajanjem; verjetni prispevek zbiranja k uresničevanemu cilju; razumno predvidljive posledice za posameznike ter narava in občutljivost podatkov, ki jih je treba zbirati ([249]).

([241]) Člen 2(b)(ii) Odredbe št. 14086.
([242]) Člen 102A zakona o nacionalni varnosti (*National Security Act*) in člen 2(b)(iii) Odredbe št. 14086.
([243]) V izjemnih primerih (zlasti kadar takega postopka ni mogoče izvesti zaradi potrebe po obravnavi nove ali nastajajoče obveščevalne zahteve) lahko take prednostne naloge določi neposredno predsednik ali vodja organa obveščevalne skupnosti, ki mora načeloma uporabiti enaka merila, kot so opisana v členu 2(b)(iii)(A)(1)-(3), glej člen 4(n) Odredbe št. 14086.
([244]) Člen 2(b)(iii)(C) Odredbe št. 14086.
([245]) Člen 2(b) in (c)(i)(A) Odredbe št. 14086.
([246]) Člen 2(c)(i)(A) Odredbe št. 14086.
([247]) Člen 2(c)(i)(A) Odredbe št. 14086.
([248]) Člen 2(c)(i)(B) Odredbe št. 14086.
([249]) Člen 2(c)(i)(B) Odredbe št. 14086.

(140) Kar zadeva vrsto zbiranja obveščevalnih podatkov v okviru SIGINT, mora biti zbiranje podatkov v Združenih državah, ki je najustreznejše za sedanje ugotavljanje ustreznosti, saj se nanaša na podatke, ki se prenašajo v organizacije v ZDA, vedno ciljno usmerjeno, kot je podrobneje opisano v uvodnih izjavah 142 do 153.

(141) „Množično zbiranje“ ([250]) se lahko izvaja le zunaj Združenih držav, na podlagi Odredbe št. 12333. V tem primeru je tudi treba v skladu z Odredbo št. 14086 dati prednost ciljno usmerjenemu zbiranju ([251]). Nasprotno je množično zbiranje dovoljeno le, če informacij, potrebnih za izboljšanje potrjenih prednostnih nalog obveščevalnih služb, ni mogoče razumno pridobiti s ciljno usmerjenim zbiranjem ([252]). Če je treba množično zbiranje podatkov izvesti zunaj Združenih držav, se uporabljajo posebni zaščitni ukrepi na podlagi Odredbe št. 14086 ([253]). Prvič, uporabljati je treba metode in tehnične ukrepe, da bi se zbrani podatki omejili le na tisto, kar je potrebno za izboljšanje potrjenih prednostnih nalog obveščevalnih služb, hkrati pa zmanjšalo zbiranje neupoštevnih informacij ([254]). Drugič, Odredba omejuje uporabo množično zbranih informacij (vključno s poizvedovanjem) na šest konkretnih ciljev, vključno z zaščito pred terorizmom, zajetjem talcev in zadrževanjem posameznikov v ujetništvu s strani ali v imenu tuje vlade, organizacije ali osebe; zaščito pred vohunjenjem, sabotažo ali umori; zaščito pred grožnjami zaradi razvijanja, posedovanja ali širjenja orožja za množično uničevanje ali povezanih tehnologij in nevarnosti itd ([255]). Nazadnje, vsako poizvedovanje po množično pridobljenih obveščevalnih podatkih v okviru SIGINT lahko poteka le, če je potrebno za izboljšanje potrjenih prednostnih nalog obveščevalnih služb, v skladu s temi šestimi cilji ter s politikami in postopki, pri katerih se ustrezno upošteva vpliv poizvedb na varstvo zasebnosti in državljanskih svoboščin vseh ljudi ne glede na njihovo državljanstvo ali prebivališče ([256]).

(142) Poleg zahtev Odredbe št. 14086 je zbiranje obveščevalnih podatkov v okviru SIGINT, ki je bilo preneseno na organizacijo v Združenih državah, predmet posebnih omejitev in zaščitnih ukrepov, ki jih ureja člen 702 FISA ([257]). Člen 702 FISA omogoča zbiranje tujih obveščevalnih podatkov s ciljnim osredotočanjem na nedržavljane ZDA, za katere se utemeljeno sklepa, da se nahajajo zunaj Združenih držav, ob zavezujoči pomoči ameriških ponudnikov storitev elektronskih komunikacij ([258]). Za zbiranje tujih obveščevalnih podatkov v skladu s členom 702 FISA pravosodni minister in direktor nacionalne obveščevalne službe predložita sodišču za nadzor nad tujo obveščevalno dejavnostjo (*Foreign Intelligence Surveillance Court*, v nadaljnjem besedilu: FISC) letni potrdili, v katerih so opredeljene

([250]) Tj. zbiranje velikih količin obveščevalnih podatkov v okviru SIGINT, ki se iz tehničnih ali operativnih razlogov pridobivajo brez uporabe diskriminant (npr. brez uporabe posebnih identifikatorjev ali izbirnih izrazov), glej člen 4(b) Odredbe št. 14086. V skladu z Odredbo št. 14086 in kot je podrobneje pojasnjeno v uvodni izjavi 141, množično zbiranje na podlagi Odredbe št. 12333 poteka le, če je potrebno za izboljšanje konkretnih potrjenih prednostnih nalog obveščevalnih služb ter predmet številnih omejitev in zaščitnih ukrepov, zasnovanih za zagotovitev, da dostop do podatkov ni neselektiven. Množično zbiranje je torej drugačno od zbiranja, ki poteka splošno in neselektivno („množičen nadzor“) brez omejitev in zaščitnih ukrepov.

([251]) Člen 2(c)(ii)(A) Odredbe št. 14086.

([252]) Člen 2(c)(ii)(A) Odredbe št. 14086.

([253]) Posebna pravila o množičnem zbiranju iz Odredbe št. 14086 se uporabljajo tudi za ciljno zbiranje obveščevalnih podatkov v okviru SIGINT, pri katerem se začasno uporabljajo podatki, pridobljeni brez uporabe diskriminant (npr. posebnih izbirnih izrazov ali identifikatorjev), tj. množično (kar je mogoče le zunaj ozemlja Združenih držav). To ne velja, kadar se taki podatki uporabljajo le za podporo začetni tehnični fazi dejavnosti ciljnega zbiranja obveščevalnih podatkov v okviru SIGINT, se hranijo le za kratko obdobje, potrebno za dokončanje te faze, in se takoj zatem izbrišejo (člen 2(c)(ii)(D) Odredbe št. 14086). V tem primeru mora biti edini namen začetnega zbiranja brez uporabe diskriminant omogočiti ciljno zbiranje informacij z uporabo posebnega identifikatorja ali izbirnega izraza. V takem scenariju se v vladne podatkovne zbirke vnesejo le podatki, ki ustrezajo uporabi določene diskriminante, preostali podatki pa se hkrati uničijo. Tako ciljno usmerjeno zbiranje zato še naprej urejajo splošna pravila, ki se uporabljajo za zbiranje obveščevalnih podatkov v okviru SIGINT, med drugim člen 2(a)–(b) in člen 2(c)(i) Odredbe št. 14086.

([254]) Člen 2(c)(ii)(A) Odredbe št. 14086.

([255]) Člen 2(c)(ii)(B) Odredbe št. 14086. Če se pojavijo nove nacionalne varnostne zahteve, kot so grožnje za nacionalno varnost, lahko predsednik ta seznam posodobi. Take posodobitve morajo biti načeloma objavljene, razen če predsednik odloči, da bi že to pomenilo tveganje za nacionalno varnost Združenih držav (člen 2(c)(ii)(C) Odredbe št. 14086). V zvezi s poizvedbami množično zbranih podatkov glej člen 2(c)(iii)(D) Odredbe št. 14086.

([256]) Člen 2(a)(ii)(A) v povezavi s členom 2(c)(iii)(D) Odredbe št. 14086. Glej tudi Prilogo VII.

([257]) Člen 1881 naslova 50 zakonodajne zbirke ZDA.

([258]) Člen 1881a (a) naslova 50 zakonodajne zbirke ZDA. Kot je navedel PCLOB, nadzor iz člena 702 zlasti „zajema izključno ciljno osredotočanje na določene osebe [nedržavljane ZDA], v zvezi s katerimi je bila oblikovana individualizirana ugotovitev“ (Nadzorni odbor za zasebnost in državljanske svoboščine, „Report on the Surveillance Program Operated Pursuant to Section 702 if the Foreign Intelligence Surveillance Act“ (Poročilo o programu nadzora, ki se izvaja v skladu s členom 702 FISA, 2. julij 2014, Poročilo o členu 702, str. 111). Glej tudi poročilo CLPO v okviru Agencije za nacionalno varnost (*National Security Agency*, v nadaljnjem besedilu: NSA), „NSA's Implementation of Foreign Intelligence Surveillance Act“ (Izvajanje člena 702 zakona o nadzoru tujih obveščevalnih podatkov (*Foreign Intelligence Act*) s strani NSA), 16. april 2014. Izraz „ponudnik storitev elektronskih komunikacij“ je opredeljen v členu 1881 (a)(4) naslova 50 zakonodajne zbirke ZDA.

kategorije tujih obveščevalnih podatkov, ki jih je treba pridobiti ([259]). Potrdili morata biti podprti s postopki izbire cilja, postopki zmanjševanja in poizvedovanja, ki jih je odobrilo tudi sodišče in so pravno zavezujoči za obveščevalne službe ZDA.

(143) FISC je neodvisno sodišče ([260]), ustanovljeno z zveznim zakonom, zoper njegove odločbe pa se je mogoče pritožiti pred pritožbenim sodiščem za nadzor nad tujo obveščevalno dejavnostjo (*Foreign Intelligence Surveillance Court of Review*, v nadaljnjem besedilu: FISCR) ([261]), nazadnje pa pred vrhovnim sodiščem ZDA ([262]). Sodišču FISC (in FISCR) pomaga stalni senat petih pravobranilcev in petih tehničnih strokovnjakov, ki imajo strokovno znanje in izkušnje na področju nacionalne varnosti in državljanskih svoboščin ([263]). Iz te skupine sodišče imenuje posameznika, ki deluje kot *amicus curiae* za pomoč pri obravnavi kakršne koli vloge za izdajo sklepa ali ponovni preizkus, ki po mnenju sodišča predstavlja novo ali pomembno razlago prava, razen če sodišče ugotovi, da tako imenovanje ni primerno ([264]). S tem se zlasti zagotovi, da so vidiki varstva zasebnosti ustrezno izraženi v presoji 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 posamezniku ali organizaciji dovoli, da vloži predlog za dopustitev stališča *amicus curiae* ([265]).

(144) FISC ponovno preizkusi skladnost certifikacije in povezanih postopkov (zlasti postopkov izbire cilja in zmanjšanja) z zahtevami FISA. Če meni, da zahteve niso izpolnjene, lahko certifikacijo v celoti ali delno zavrne in zahteva spremembo postopkov ([266]). V zvezi s tem je FISC večkrat potrdil, da njegov ponovni preizkus postopkov izbire cilja in zmanjšanja iz člena 702 ni omejen na postopke, kakor so zapisani, temveč vključuje tudi način izvajanja postopkov s strani vlade ([267]).

(145) Odločitve o ciljnem osredotočanju na posameznike sprejme Agencija za nacionalno varnost (*National Security Agency*, v nadaljnjem besedilu: NSA, ki je obveščevalna agencija, pristojna za ciljno osredotočanje na podlagi člena 702 FISA) v skladu s postopki izbire cilja, ki jih je odobril FISC, ki od NSA zahteva, da na podlagi vseh okoliščin oceni, ali obstaja verjetnost, da bo s ciljnim osredotočanjem na določeno osebo, pridobljena kategorija tujih obveščevalnih podatkov, opredeljenih v potrdilu ([268]). Ta ocena mora biti podrobno opredeljena in temeljiti na

([259]) Člen 1881a (g) naslova 50 zakonodajne zbirke ZDA.

([260]) FISC sestavljajo sodniki, 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 iz 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 1803 (a) naslova 50 zakonodajne zbirke ZDA. Sodnikom pomagajo izkušeni sodni uradniki, ki sestavljajo pravno osebje sodišča in pripravljajo pravne analize zahtev za zbiranje podatkov. Glej 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, na voljo na https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

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

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

([263]) Člen 1803 (i)(1) in (3)(A) naslova 50 zakonodajne zbirke ZDA.

([264]) Člen 1803 (i)(2)(A) naslova 50 zakonodajne zbirke ZDA.

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

([266]) Glej npr. mnenje FISC z dne 18. oktobra 2018, ki je na voljo na https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, kakor je bilo potrjeno v mnenju drugostopenjskega sodišča za nadzor tujih obveščevalnih podatkov z dne 12. julija 2019, na voljo na https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) Glej npr. FISC, predhodno mnenje in sklep 35 (18. november 2020) (odobren za javno objavo 26. aprila 2021), (Priloga D).

([268]) Člen 1881a(a) naslova 50 zakonodajne zbirke ZDA, Postopki, ki jih uporablja NSA za ciljno osredotočanje na nedržavljane ZDA, za katere se utemeljeno sklepa, da se nahajajo zunaj Združenih držav, za pridobivanje tujih obveščevalnih podatkov v skladu s členom 702 FISA iz leta 1978, kakor je bil spremenjen marca 2018 (postopki izbire cilja s strani NSA), na voljo na https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, p. 1-4, further explained in PCLOB report, str. 41 in 42.

dejstvih ter posredovati analitično presojo, specializirano usposabljanje in izkušnje analitika ter tudi naravo tujih obveščevalnih podatkov, ki jih je treba pridobiti ([269]). Izbira cilja poteka z opredelitvijo t. i. izbirnikov, ki opredeljujejo posebna komunikacijska sredstva, kot je e-poštni naslov ali telefonska številka ciljne osebe, nikoli pa ključnih besed ali imen posameznika ([270]).

(146) Analitiki NSA najprej identificirajo nedržavljane ZDA v tujini, katerih nadzor bo na podlagi ocene analitikov zagotovil ustrezne tuje obveščevalne podatke, navedene v potrdilu ([271]). Kot je določeno v postopkih izbire cilja s strani NSA, lahko NSA nadzor nad ciljno osebo izvaja le, ko je o njej že nekaj izvedela ([272]). To lahko izhaja iz informacij iz različnih virov, na primer človeška inteligenca. S temi drugimi viri se morajo analitiki seznaniti tudi s konkretnim izbirnikom (tj. komunikacijski račun), ki ga uporablja morebitna tarča. Po identifikaciji teh oseb in odobritvi ciljnega osredotočanja nanje z mehanizmom obseženih pregledov v okviru NSA ([273]) se izbirnikom, ki opredelijo komunikacijska sredstva (kot so e-poštni naslovi), ki jih uporabljajo ciljne osebe, „dodelijo naloge“ (tj. izbirniki se razvijejo in uporabljajo) ([274]).

(147) Za izbiro ciljne osebe mora NSA dokumentirati dejansko stanje ([275]), po začetnem ciljnem osredotočanju pa redno potrjevati, da je standardu izbire cilja še vedno zadoščeno ([276]). Ko standardu izbire cilja ni več zadoščeno, je treba zbiranje končati ([277]). Uradniki uradov za nadzor obveščevalnih podatkov pri ministrstvu za pravosodje, za katere velja obveznost poročanja o vsaki kršitvi FISC in Kongresu, vsaka dva meseca preverjajo skladnost izbora vsake ciljne osebe s strani NSA, njene evidence o vsaki zabeleženi oceni izbire cilja in utemeljitve s postopki izbire cilja ([278]). Pisna dokumentacija NSA omogoča lažji nadzor FISC, ali se za konkretne posameznike uporablja pravilno ciljno osredotočanje na podlagi člena 702 FISA, v skladu z njegovimi nadzornimi pooblastili, opisanimi v uvodnih izjavah 173 in 174 ([279]). Nazadnje, tudi direktor nacionalne obveščevalne službe (*Director of National Intelligence*, v nadaljnjem besedilu: DNI) mora vsako leto poročati o skupnem številu ciljnih oseb na podlagi člena 702 FISA v javnih letnih statističnih poročilih o preglednosti. Podjetja, ki prejmejo navodila na podlagi člena 702 FISA lahko (v poročilih o preglednosti) objavijo zbirne podatke o zahtevah, ki jih prejmejo ([280]).

([269]) Postopki izbire cilja s strani NSA, str. 4.

([270]) Glej poročilo PCLOB o členu 702, str. 32 in 33 ter 45 z nadaljnjimi sklici. Glej tudi polletno oceno skladnosti s postopki in smernicami, izdanimi v skladu s členom 702 FISA, ki sta jo predložila pravosodni minister in direktor nacionalne obveščevalne službe, obdobje poročanja: 1. december 2016–31. maj 2017, str. 41 (oktober 2018), na voljo na naslovu: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) Poročilo PCLOB o členu 702, str. 42 in 43.

([272]) Postopki izbire cilja s strani NSA, str. 2.

([273]) Poročilo PCLOB o členu 702, str. 46. Na primer, NSA mora preveriti, ali obstaja povezava med ciljno osebo in izbirnikom, dokumentirati tuje obveščevalne podatke, za katere se pričakuje, da bodo 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.

([274]) Člen 1881a (h) naslova 50 zakonodajne zbirke ZDA.

([275]) Postopki izbire cilja s strani NSA, str. 8. Glej tudi poročilo PCLOB o členu 702, str. 46. Nepredložitev pisne utemeljitve predstavlja primer neskladnosti dokumentacije, ki mora biti sporočen FISC in Kongresu. Glej polletno oceno skladnosti s postopki in smernicami, izdanimi v skladu s členom 702 FISA, ki sta jo predložila pravosodni minister in DNI, obdobje poročanja: 1. december 2016–31. maj 2017, str. 41 (oktober 2018), Poročilo ministrstva za pravosodje/ODNI o skladnosti, predloženo FISC za obdobje december 2016–maj 2017 na strani A-6, na voljo na naslovu https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Glej vlogo vlade ZDA, predloženo FISC, „2015 Summary of Notable Section 702 Requirements“ (Povzetek pomembnejših zahtev na podlagi člena 702 iz leta 2015), na str. 2 in 3 (15. julij 2015), in informacije, zagotovljene v Prilogi VII.

([277]) Glej vlogo vlade ZDA, predloženo FISC, „2015 Summary of Notable Section 702 Requirements“ (Povzetek pomembnejših zahtev na podlagi člena 702 iz leta 2015), na str. 2 in 3 (15. julij 2015), ki določa, da „[č]e vlada pozneje oceni, da z nadaljnjo dodelitvijo naloge izbirnika ciljne osebe verjetno ne bodo pridobljeni tuji obveščevalni podatki, se zahteva takojšnja ukinitev naloge, zavlačevanje z umikom pa lahko povzroči primer neskladnosti, o katerem je treba poročati“. Glej tudi informacije, zagotovljene v Prilogi VII.

([278]) Poročilo PCLOB o členu 702, str. 70 do 72; pravilo 13(b)poslovnika FISC ZDA, na voljo na spletišču https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) Glej tudi Poročilo ministrstva za pravosodje/ODNI o skladnosti, predloženo FISC za obdobje december 2016–maj 2017 na strani A-6.

([280]) Člen 1874 naslova 50 zakonodajne zbirke ZDA.

(148) Kar zadeva druge pravne podlage za zbiranje osebnih podatkov, ki se prenašajo v organizacije v ZDA, se uporabljajo različni omejitve in zaščitni ukrepi. Na splošno je množično zbiranje podatkov izrecno prepovedano na podlagi člena 402 FISA (pooblastilo za snemalnike klicev ter naprave za pasti in sledenje) in z uporabo NSL, namesto tega pa je potrebna uporaba posebnih „izbirnih izrazov“ ([281]).

(149) Za izvajanje tradicionalnega individualiziranega elektronskega nadzora (v skladu s členom 105 FISA) morajo obveščevalne agencije pri FISC vložiti vlogo z izjavo o dejstvih in okoliščinah, na katere se sklicujejo v utemeljitvi, da obstaja utemeljen sum, da sredstvo uporablja ali jo bo uporabila tuja sila ali agent tuje sile ([282]) FISC bo med drugim ocenil, ali na podlagi predstavljenih dejstev obstaja utemeljen sum, da to dejansko drži ([283]).

(150) Za izvajanje preiskave prostorov ali lastnine, ki je namenjena inšpekcijskemu pregledu, zasegu itd. informacij, gradiva ali lastnine (npr. računalniška naprava) na podlagi člena 301 FISA, je potrebna vloga za izdajo sklepa FISC ([284]). V taki vlogi mora biti med drugim dokazano, da obstaja utemeljen sum, da je tarča take preiskave tuja sila ali agent tuje sile; da prostor ali lastnina, ki ga oziroma jo je treba preiskati, vsebuje tuje obveščevalne podatke, in da ima prostor, ki ga je treba preiskati, v lasti, uporabi, posesti tuje sile (ali njenega agenta), ali pa je v prenosu njej oziroma njemu ali od nje oziroma njega ([285]).

(151) Podobno je za namestitev snemalnikov klicev ali naprav za pasti in sledenje (v skladu s členom 402 FISA) potrebna vloga za izdajo sklepa FISC (ali sodnika nižjega sodišča ZDA) ter uporaba posebnega izbirnega izraza, tj. izraza, ki izrecno opredeljuje osebo, račun itd. in se uporablja za čim večjo razumno omejitev obsega iskanih informacij ([286]). To pooblastilo se ne nanaša na vsebino komunikacij, temveč na podatke o stranki ali naročniku, ki uporablja storitev (kot so ime, naslov, številka naročnika, trajanje/vrsta opravljene storitve, vir/mehanizem plačila).

(152) Člen 501 FISA ([287]), ki omogoča zbiranje poslovnih evidenc javnega prevoznika (tj. vsake osebe ali subjekta, ki prevaža ljudi ali lastnino po kopnem, z železnico, po vodi ali zraku proti plačilu), javni objekt za nastanitev (npr. hotel, motel ali gostišče), objekt za najem vozil ali fizično skladišče (tj. ki zagotavlja prostor za skladiščenje blaga in materialov ali opravlja storitve v zvezi s takim skladiščenjem) ([288]), prav tako zahteva vlogo, vloženo pri FISC ali predloženo sodniku nižjega sodišča. V tej vlogi morajo biti navedene zahtevane evidence ter konkretna in utemeljena dejstva, ki upravičujejo razlog za sum, da je oseba, na katero se nanašajo evidence, tuja sila ali agent tuje sile ([289]).

(153) Nazadnje, NLS so dovoljeni v skladu z različnimi zakoni, obveščevalnim agencijam pa omogočajo, da od nekaterih subjektov (npr. finančnih institucij, agencijah za poročanje o kreditni sposobnosti, ponudnikov storitev elektronskih komunikacij) pridobijo nekatere informacije (ki ne vključujejo vsebine komunikacij), ki jih vsebujejo poročila o kreditni sposobnosti, finančni podatki, elektronski podatki o naročnikih in poslih ([290]). Zakon, ki dovoljuje dostop do elektronskih komunikacij, določa, da lahko NLS uporablja le FBI, in zahteva, da se v zahtevah uporablja izraz, ki specifično opredeljuje osebo, subjekt, telefonsko številko ali račun ter da zahteva potrjuje, da so informacije pomembne za odobreno preiskavo nacionalne varnosti za zaščito pred mednarodnim terorizmom ali tajnimi obveščevalnimi dejavnostmi ([291]). Prejemniki NSL ga imajo pravico izpodbijati na sodišču ([292]).

([281]) Člen 1842(c)(3) naslova 50 zakonodajne zbirke ZDA, v zvezi z NSL pa člen 3414(a)(2) naslova 12; člen 1681u naslova 15 zakonodajne zbirke ZDA; člen1681v(a) naslova 15 zakonodajne zbirke ZDA; in člen 2709(a) naslova 18 zakonodajne zbirke ZDA.

([282]) „Agent tuje sile“ lahko vključuje nedržavljane ZDA in sodelujejo v mednarodnem terorizmu ali mednarodnem širjenju orožja za množično uničevanje (vključno s pripravljalnimi dejanji) (člen 1801 (b)(1) naslova 50 zakonodajne zbirke ZDA).

([283]) Člen 1804 naslova 50 zakonodajne zbirke ZDA. V zvezi z izbiro izbirnih izrazov glej tudi člen 1841(4).

([284]) Člen 1821(5) naslova 50 zakonodajne zbirke ZDA.

([285]) Člen 1823(a) naslova 50 zakonodajne zbirke ZDA.

([286]) Člen 1842 v povezavi s členom 1841(2) naslova 50 zakonodajne zbirke ZDA in člen 3127 naslova 18.

([287]) Člen 1862 naslova 50 zakonodajne zbirke ZDA.

([288]) Členi 1861–1862 naslova 50 zakonodajne zbirke ZDA.

([289]) Člen 1862(b) naslova 50 zakonodajne zbirke ZDA.

([290]) Člen 3414 naslova 12 zakonodajne zbirke ZDA; členi 1681u–1681v naslova 15 zakonodajne zbirke ZDA; in člen 2709 naslova 18 zakonodajne zbirke ZDA.

([291]) Člen 2709(b) naslova 18 zakonodajne zbirke ZDA.

([292]) Npr. člen 2709(d) naslova 18 zakonodajne zbirke ZDA.

3.2.1.3 *Nadaljnja uporaba zbranih informacij*

(154) Obdelava osebnih podatkov, ki jih obveščevalne agencije ZDA zbirajo z obveščevalnimi dejavnostmi SIGINT, je predmet številnih zaščitnih ukrepov.

(155) Prvič, vsaka obveščevalna agencija mora zagotoviti ustrezno varnost podatkov in nepooblaščenim osebam preprečiti dostop do osebnih podatkov, zbranih z obveščevalnimi dejavnostmi SIGINT. V zvezi s tem so v različnih instrumentih, vključno z zakoni, smernicami in standardi, podrobneje navedene minimalne zahteve glede informacijske varnosti, ki jih je treba uvesti (npr. večfaktorska avtentikacija, šifriranje itd.) ([293]). Dostop do zbranih podatkov mora biti omejen na pooblaščeno, usposobljeno osebje, ki mora biti seznanjeno z informacijami za opravljanje svojih nalog ([294]). Splošneje morajo obveščevalne agencije svojim zaposlenim zagotoviti ustrezno usposabljanje, vključno s postopki poročanja in obravnavanje kršitev prava (vključno z Odredbo št. 14086) ([295]).

(156) Drugič, obveščevalne agencije morajo izpolnjevati standarde obveščevalne skupnosti glede točnosti in nepristranskosti, zlasti v zvezi z zagotavljanjem kakovosti in zanesljivosti podatkov, upoštevanjem alternativnih virov informacij in nepristranskostjo pri izvajanju analiz ([296]).

(157) Tretjič, kar zadeva hrambo podatkov, Odredba št. 14086 pojasnjuje, da za osebne podatke nedržavljanov ZDA veljajo enaki roki za hrambo kot za podatke državljanov ZDA ([297]). Obveščevalne agencije morajo opredeliti konkretna obdobja hrambe in/ali dejavnike, ki jih je treba upoštevati pri določanju dolžine veljavnih obdobij hrambe (npr. ali so informacije dokaz kaznivega dejanja; ali gre za tuje obveščevalne informacije; ali so informacije potrebne za zagotavljanje varnosti oseb ali organizacij, vključno z žrtvami ali tarčami mednarodnega terorizma), ki so določene v različnih pravnih instrumentih ([298]).

(158) Četrtič, v zvezi z razširjanjem osebnih podatkov, zbranih z obveščevalnimi dejavnostmi SIGINT, se uporabljajo posebna pravila. V skladu s splošno zahtevo se lahko osebni podatki nedržavljanov ZDA razširjajo le, če to vključuje isto vrsto informacij, ki se lahko razširjajo o državljanih ZDA, npr. informacije, potrebne za zaščito varnosti osebe ali organizacije (kot so ciljne osebe, žrtve ali talci mednarodnih terorističnih organizacij) ([299]). Poleg tega se osebni podatki ne smejo razširjati le zaradi državljanstva osebe ali države prebivanja ali da bi se zaobšle zahteve Odredbe št. 14086 ([300]). Razširjanje na ravni vlade ZDA lahko poteka le, če pooblaščeni in usposobljeni posameznik

([293]) Člen 2(c)(iii)(B)(1) Odredbe št. 14086. Glej tudi naslov VIII zakona o nacionalni varnosti (v katerem so podrobno navedene zahteve za dostop do zaupnih informacij), člen 1.5 Odredbe št. 12333 (ki zahteva, da vodje agencij obveščevalne skupnosti spoštujejo izmenjavo informacij in varnostnih smernic, varstvo zasebnosti informacij in druge pravne zahteve, direktiva o nacionalni varnosti 42, „Nacionalna politika za varnost telekomunikacijskih in informacijskih sistemov nacionalne varnosti“ (ki odboru za sisteme nacionalne varnosti odreja, da izvršnim službam in agencijam zagotovi sistemsko-varnostne smernice za sisteme nacionalne varnosti) in memorandum o nacionalni varnosti 8, „Izboljšanje kibernetske varnosti nacionalne varnosti, ministrstva za obrambo in sistemov obveščevalne skupnosti“ (ki določa časovnice in smernice za način, kako se bodo izvajale zahtev glede kibernetske varnosti za sisteme nacionalne varnosti, vključno z večfaktorsko avtentikacijo, šifriranjem, tehnologijami v oblaku in storitvami odkrivanja končne točke)

([294]) Člen 2(c)(iii)(B)(2) Odredbe št. 14086. Poleg tega je do osebnih podatkov, za katere ni bila sprejeta dokončna odločitev o hrambi, dovoljeno dostopati le za sprejetje take odločitve ali v njeno podporo ali za opravljanje pooblaščenih upravnih, preizkuševalnih, razvojnih, varnostnih ali nadzornih funkcij (člen 2(c)(iii)(B)(3) Odredbe št. 14086).

([295]) Člen 2(d)(ii) Odredbe št. 14086.

([296]) Člen 2(c)(iii)(C) Odredbe št. 14086.

([297]) Člen 2(c)(iii)(A)(2)(a)-(c) Odredbe št. 14086. Splošneje, vsaka agencija mora uvesti politike in postopke, zasnovane tako, da čim bolj zmanjšajo razširjanje in hrambo osebnih podatkov, zbranih z obveščevalnimi dejavnostmi SIGINT (člen 2(c)(iii)(A) Odredbe št. 14086).

([298]) Glej npr. člen 309 zakona o pooblastilih za obveščevalno dejavnost za davčno leto 2015 (*Intelligence Authorization Act For Fiscal Year 2015*); postopke zmanjšanja, ki jih sprejmejo posamezne obveščevalne agencije v skladu s členom 702 FISA in odobri FISC; postopke, ki sta jih odobrila pravosodni minister in FRA (v skladu s katerimi morajo zvezne agencije ZDA, vključno z agencijami za nacionalno varnost, določiti obdobja hrambe svojih evidenc, ki jih mora odobriti Uprava za nacionalne arhive in evidence).

([299]) Člen 2(c)(iii)(A)(1)(a) in 5(d) Odredbe št. 14086 v povezavi s členom 2.3 Odredbe št. 12333.

([300]) Člen 2(c)(iii)(A)(1)(b) in (e) Odredbe št. 14086.

utemeljeno sumi, da se mora prejemnik seznaniti z informacijami ([301]) in jih bo ustrezno varoval ([302]). Za ugotovitev, ali se lahko osebni podatki razširjajo prejemnikom zunaj vlade ZDA (vključno s tujo vlado ali mednarodno organizacijo), je treba za namene razširjanja upoštevati naravo in obseg podatkov, ki se razširjajo, in morebiten škodljiv vpliv na zadevno osebo ali osebe ([303]).

(159) Nazadnje, za lažji nadzor skladnosti z veljavnimi pravnimi zahtevami in tudi učinkovitimi pravnimi sredstvi mora vsaka obveščevalna agencija v skladu z Odredbo št. 14086 hraniti ustrezno dokumentacijo o zbiranju obveščevalnih podatkov v okviru SIGINT. Zahteve glede dokumentacije zajemajo elemente, kot so dejanska podlaga za oceno, da je konkretna dejavnost zbiranja potrebna za izboljšanje potrjenih prednostnih nalog obveščevalnih služb ([304]).

(160) Poleg zgoraj navedenih zaščitnih ukrepov iz Odredbe št. 14086 za uporabo informacij, zbranih z dejavnostmi SIGINT, za vse obveščevalne agencije ZDA veljajo bolj splošne zahteve glede omejitve namena, najmanjšega obsega podatkov, točnosti, varnosti, hrambe in razširjanja, ki izhajajo zlasti iz Okrožnice OMB št. A-130, zakona o e-upravi, zakona o evidencah zveznih agencij (glej uvodne izjave 101–106) in smernic Odbora za sisteme nacionalne varnosti (*Committee on National Security Systems*, v nadaljnjem besedilu: CNSS) ([305]).

3.2.2 ***Nadzor***

(161) Dejavnosti obveščevalnih agencij ZDA so predmet nadzora različnih organov.

(162) Prvič, Odredba št. 14086 zahteva, da ima vsaka obveščevalna agencija višje uradnike za pravne zadeve, nadzor in skladnost, da se zagotovi skladnost z veljavno zakonodajo ZDA ([306]). Zlasti morajo izvajati reden nadzor nad obveščevalnimi dejavnostmi SIGINT in zagotavljati odpravo vsake neskladnosti. Obveščevalne agencije morajo takim uradnikom za izvajanje njihovih nadzornih funkcij zagotoviti dostop do vseh ustreznih informacij in ne smejo sprejeti nobenih ukrepov, s katerimi bi ovirale ali neustrezno vplivale na njihove dejavnosti nadzora ([307]). Poleg tega je treba vsak pomemben primer neskladnosti ([308]), ki ga ugotovi uradnik za nadzor ali kateri koli drug zaposleni, nemudoma sporočiti vodji obveščevalne agencije in DNI, ki morata zagotoviti sprejetje vseh potrebnih ukrepov za odpravo pomembnega primera neskladnosti in preprečitev njegove ponovitve ([309]).

(163) To nadzorno funkcijo uradniki izpolnjujejo v vlogi imenovanih presojevalcev skladnosti, pa tudi kot uradniki za varstvo zasebnosti in državljanskih svoboščin ter generalni inšpektorji ([310]).

([301]) Glej npr. AGG-DOM, ki na primer določa, da lahko FBI razširja informacije le, če se mora prejemnik z njimi seznaniti, da bi lahko izpolnil svoje naloge ali zaščitil javnost.

([302]) Člen 2(c)(iii)(A)(1)(c) Odredbe št. 14086. Obveščevalne agencije lahko na primer razširjajo informacije v okoliščinah, ki so pomembne za kazensko preiskavo ali so povezane s kaznivim dejanjem, na primer tako, da razširjajo opozorila o grožnjah z ubojem, hudo telesno poškodbo ali ugrabitvijo; razširjajo informacije o kibernetskih grožnjah, incidentih ali vdorih ter obveščajo žrtve ali opozarjajo morebitne žrtve kaznivih dejanj.

([303]) Člen 2(c)(iii)(A)(1)(d) Odredbe št. 14086.

([304]) Člen 2(c)(iii)(E) Odredbe št. 14086.

([305]) Glej politiko CNSS št. 22, Politika obvladovanja tveganja na področju kibernetske varnosti, in navodilo št. 1253, ki vsebuje podrobne smernice o varnostnih ukrepih, ki jih je treba uvesti za nacionalne varnostne sisteme.

([306]) Člen 2(d)(i)(A)-(B) Odredbe št. 14086.

([307]) Člena 2(d)(i)(B)-(C) Odredbe št. 14086.

([308]) Tj. sistemska ali namerna neskladnost z veljavno zakonodajo ZDA, ki bi lahko okrnila ugled ali integriteto organa obveščevalne skupnosti ali drugače povzročila dvom o primernosti dejavnosti obveščevalne skupnosti, tudi glede morebitnega bistvenega vpliva na interese zadevne osebe ali oseb v zvezi z varstvom zasebnosti in državljanskih svoboščin, glej člen 5(l) Odredbe št. 14086.

([309]) Člen 2(d)(iii) Odredbe št. 14086.

([310]) Člen 2(d)(i)(B) Odredbe št. 14086.

(164) Tako kot v primeru organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj so uradniki za varstvo zasebnosti in državljanskih svoboščin v vseh obveščevalnih agencijah ([311]). Pooblastila teh uradnikov običajno zajemajo nadzor nad postopki za zagotovitev, da zadevno ministrstvo/agencija ustrezno upošteva vidike, povezane z varstvom zasebnosti ali državljanskih svoboščin, in da ima vzpostavljene ustrezne postopke za obravnavo pritožb posameznikov, ki menijo, da je bilo kršeno varstvo njihove zasebnosti ali državljanskih svoboščin (in v nekaterih primerih, kot je Urad direktorja nacionalne obveščevalne službe (*Office of the Director of National Intelligence*, v nadaljnjem besedilu: ODNI), so lahko sami pooblaščeni za preiskovanje pritožb ([312])). Vodje obveščevalnih agencij morajo zagotoviti, da imajo uradniki za varstvo zasebnosti in državljanske svoboščine vire za izpolnjevanje svojih pooblastil, da jim je zagotovljen dostop do vsega gradiva in osebja, potrebnega za opravljanje njihovih nalog, da so seznanjeni s predlaganimi spremembami politike in da se o slednjih opravijo posvetovanja z njimi ([313]). Uradniki za varstvo zasebnosti in državljanskih svoboščin redno poročajo Kongresu in PCLOB, tudi o številu in naravi pritožb, ki jih prejme ministrstvo/agencija v povzetku obravnave takih pritožb, opravljenih pregledih in preiskavah ter vplivu dejavnosti, ki jih je izvedel uradnik ([314]).

(165) Drugič, vsaka obveščevalna agencija ima svojega neodvisnega generalnega inšpektorja, ki je med drugim pristojen za nadzor tujih obveščevalnih dejavnosti. To v okviru ODNI vključuje Urad generalnega inšpektorja obveščevalne skupnosti (*Office of the Inspector General of the Intelligence Community*) s celovito pristojnostjo nad celotno obveščevalno skupnostjo, ki je pooblaščena za preiskovanje pritožb ali informacij, ki se nanašajo na domnevno nezakonito ravnanje ali zlorabo pooblastila v zvezi s programi ali z dejavnostmi ODNI in/ali obveščevalne skupnosti ([315]). Tako kot v primeru organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (glej uvodno izjavo 109) so generalni inšpektorji zakonsko neodvisni ([316]) in pristojni 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 zakonodaje ([317]). Imajo dostop do vseh evidenc, poročil, revizij, pregledov, dokumentov,

([311]) Glej člen 2000ee-1 naslova 42 zakonodajne zbirke ZDA. To vključuje na primer ministrstvo za zunanje zadeve, ministrstvo za pravosodje, ministrstvo za domovinsko varnost, ministrstvo za obrambo, NSA, Centralno obveščevalno agencijo (*Central Intelligence Agency*, v nadaljnjem besedilu: CIA), FBI in ODNI.

([312]) Glej člen 3(c) Odredbe št. 14086.

([313]) Člen 2000ee-1(d) naslova 42 zakonodajne zbirke ZDA.

([314]) Glej člen 2000ee-1(f)(1), (2) naslova 42 zakonodajne zbirke ZDA. Na primer, poročilo Urada NSA za varstvo zasebnosti, državljanskih svoboščin in preglednosti (*Civil Liberties, Privacy and Transparency Office*), ki zajema obdobje januar 2021–junij 2021, kaže, da je urad izvedel 591 pregledov učinkov na varstvo zasebnosti in državljanskih svoboščin v različnih okvirih, npr. v zvezi z dejavnostmi zbiranja, dogovori in odločbami o izmenjavi informacij, odločbami o hrambi podatkov itd., ob upoštevanju različnih dejavnikov, kot so količina in vrsta informacij, povezanih z dejavnostjo, vpleteni posamezniki, namen in predvidena uporaba podatkov, zaščitni ukrepi, uvedeni za ublažitev morebitnih tveganj za varstvo zasebnosti itd. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Podobno poročila Urada CIA za varstvo zasebnosti in državljanskih svoboščin (*Office of Privacy and Civil Liberties*) za obdobje januar–junij 2019 zagotavljajo informacije o nadzornih dejavnostih Urada, npr. pregledu skladnosti s smernicami pravosodnega ministra na podlagi Odredbe št. 12333 v zvezi s hrambo in z razširjanjem informacij, s smernicami za izvajanje PPD-28 in z zahtevami za ugotavljanje in obravnavo kršitev varstva podatkov, vsebujejo pa tudi preglede uporabe osebnih podatkov in ravnanja z njimi (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Tega generalnega inšpektorja imenuje predsednik ob potrditvi senata, razreši pa ga lahko le predsednik.

([316]) Generalni inšpektorji imajo varen mandat in jih lahko razreši samo predsednik, ki mora pisno sporočiti Kongresu razloge za tako razrešitev. 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, na podlagi tega pa lahko naloži odgovornost ustreznemu direktorju. Glej npr. zakon o generalnih inšpektorjih iz leta 1978, člen 8 (za Ministrstvo za obrambo); člen 8E (za ministrstvo za pravosodje), člen 8G(d)(2)(A), (B) (za NSA); člen 403q (b) naslova 50 zakonodajne zbirke ZDA (za CIO); zakon o pooblastilih za obveščevalno dejavnost za davčno leto 2010, člen 405(f) (za obveščevalno skupnost).

([317]) Zakon o generalnih inšpektorjih iz leta 1978, kakor je bil spremenjen, javno pravo 117-108 z dne 8. aprila 2022. Na primer, kot je pojasnjeno v polletnem poročilu generalnega inšpektorja NSA Kongresu, ki zajema obdobje od 1. aprila 2021 do 31. marca 2022, je izvedel presoje ravnanja s podatki državljanov ZDA, zbranimi na podlagi Odredbe št. 12333, obdelave za odstranjevanje netočnih obveščevalnih podatkov v okviru SIGINT, avtomatiziranega orodja za izbiro cilja, ki ga uporablja NSA, in skladnosti s pravili o dokumentaciji in poizvedbah v zvezi z zbiranjem na podlagi člena 702 FISA, v okviru tega pa izdal več priporočil (glej https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, str. 5 do 8 in https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, str. 10 do 13). Glej tudi nedavne revizije in preiskave, ki jih je opravil generalni inšpektor obveščevalne skupnosti v zvezi z informacijsko varnostjo in nepooblaščenimi razkritji zaupnih informacij s področja nacionalne varnosti (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, str. 8, 11 ter https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, str. 19 in 20).

spisov, priporočil ali drugega ustreznega gradiva, po potrebi s sodnim pozivom, in lahko opravljajo zaslišanja ([318]). Generalni inšpektorji odstopijo zadeve suma kršitev kazenskega prava organom pregona, vodjem agencij pa izdajajo priporočila za popravne ukrepe ([319]). Čeprav njihova priporočila niso zavezujoča, so njihova poročila, vključno s poročili o nadaljnjih ukrepih (ali odsotnosti ukrepov) ([320]), na splošno objavljena in poslana Kongresu, ki lahko na podlagi teh poročil opravlja svojo nadzorno funkcijo (glej uvodni izjavi 168 in 169) ([321]).

(166) Tretjič, obveščevalni nadzorni odbor (*Intelligence Oversight Board*, v nadaljnjem besedilu: IOB), ustanovljen v okviru predsedniškega obveščevalnega svetovalnega odbora (*President's Intelligence Advisory Board*, v nadaljnjem besedilu: PIAB), nadzoruje skladnost obveščevalnih organov ZDA z ustavo in vsemi veljavnimi pravili ([322]). PIAB je svetovalni organ v okviru izvršnega urada predsednika, ki ga sestavlja 16 članov, ki jih imenuje predsednik in niso iz vlade ZDA. IOB sestavlja največ pet članov, ki jih predsednik imenuje izmed članov PIAB. V skladu z Odredbo št. 12333 ([323]) morajo vodje vseh obveščevalnih agencij IOB poročati o vsaki obveščevalni dejavnosti, za katero obstaja razlog za sum, da je morda nezakonita ali v nasprotju z Odredbo ali predsedniško direktivo. Za zagotovitev, da ima IOB dostop do informacij, potrebnih za izvajanje njegovih funkcij, Odredba št. 13462 DNI in vodjem obveščevalnih agencij odreja, naj IOB zagotovijo vse informacije in pomoč, ki so po ugotovitvi IOB potrebne za izvajanje njegovih funkcij, v zakonsko dovoljenem obsegu ([324]). IOB mora obveščati predsednika o obveščevalnih dejavnostih, za katere meni, da kršijo zakonodajo ZDA (vključno z odredbami) in da jih pravosodni minister DNI ali vodja obveščevalne agencije neustrezno obravnavata ([325]). Poleg tega mora IOB obveščati pravosodnega ministra o morebitnih kršitvah kazenskega prava.

(167) Četrtič, obveščevalne agencije nadzira PCLOB. V skladu z njegovim statutom o ustanovitvi so PCLOB podeljena pooblastila na področju politik boja proti terorizmu in njihovega izvajanja 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 ([326]). Prejema poročila uradnikov za varstvo zasebnosti in državljanskih svoboščin več zveznih ministrstev/agencij ([327]), lahko izdaja priporočila vladi in obveščevalnim agencijam ter redno poroča kongresnim odborom in predsedniku ([328]). Poročila odboru, vključno s poročili Kongresu, morajo biti čim bolj javno dostopna ([329]). PCLOB je izdal več poročil o nadzoru in nadaljnjih ukrepih, vključno z analizo programov, ki se izvajajo na podlagi člena 702 FISA, in varstva zasebnosti v tem okviru, izvajanja PPD-28 in Odredbe št. 12333 ([330]). PCLOB je zadolžen tudi za izvajanje posebnih nadzornih funkcij v zvezi z izvajanjem

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

([319]) Glej prav tam člene 4, 6-5.

([320]) Kar zadeva nadaljnje ukrepe, ki so določeni v zvezi s poročili in priporočili generalnega inšpektorja, glej na primer odziv na poročilo generalnega inšpektorja pri ministrstvu za pravosodje, v katerem je bilo ugotovljeno, da FBI ni ravnal dovolj pregledno do FISC v zvezi z vlogami v obdobju od leta 2014 do leta 2019, kar je povzročilo reforme za okrepitev skladnosti, nadzora in odgovornosti pri FBI (npr. direktor FBI je odredil več kot 40 popravnih ukrepov, vključno z 12 posebnimi ukrepi za postopek na podlagi FISA v zvezi z dokumentacijo, nadzorom, vzdrževanjem evidenc, usposabljanjem in revizijami) (glej https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance in https://oig.justice.gov/reports/2019/o20012.pdf). Glej na primer tudi revizijo generalnega inšpektorja pri ministrstvu za pravosodje pri Uradu FBI v zvezi z vlogami in pristojnostmi glavnega svetovalca na področju nadziranja skladnosti z veljavnimi zakoni, politikami in postopki, povezanimi z dejavnostmi FBI na področju nacionalne varnosti, in Dodatek 2, ki vsebuje dopis FBI, s katerim ta sprejema vsa priporočila. V zvezi s tem Dodatek 3 zagotavlja pregled nadaljnjih ukrepov in informacij, ki jih je generalni inšpektor zahteval od FBI, da bi lahko dokončal svoja priporočila (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Glej zakon o generalnih inšpektorjih iz leta 1978, člen 4(5) in člen 5.

([322]) Glej Odredbo št. 13462.

([323]) Glej člen 1.6(c) Odredbe št. 12333.

([324]) Člen 8(a) Odredbe št. 13462.

([325]) Člen 6(b) Odredbe št. 13462.

([326]) Člen 2000ee (g) naslova 42 zakonodajne zbirke ZDA.

([327]) Glej člen 2000ee-1 (f)(1)(A)(iii) naslova 42 zakonodajne zbirke ZDA. 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.

([328]) Člen 2000ee (e) naslova 42 zakonodajne zbirke ZDA.

([329]) Člen 2000ee (f) naslova 42 zakonodajne zbirke ZDA.

([330]) Na voljo na naslovu https://www.pclob.gov/Oversight.

Odredbe št. 14086, zlasti za pregledovanje, ali so postopki agencije skladni z Odredbo (glej uvodno izjavo 126), in ocenjevanje korektivnega delovanja mehanizma pravnih sredstev (glej uvodno izjavo 194).

(168) Petič, poleg nadzornih mehanizmov v okviru izvršilne oblasti imajo tudi določeni odbori Kongresa ZDA (obveščevalna in pravosodna odbora Predstavniškega doma oziroma Senata), pristojnosti za nadzor nad vsemi tujimi obveščevalnimi dejavnostmi v ZDA. Člani teh odborov imajo dostop do zaupnih podatkov in tudi do obveščevalnih metod in programov ([331]). Odbori izvajajo redni nadzor, zlasti z obravnavami, preiskavami, pregledi in poročili ([332]).

(169) Kongresni odbori prejemajo redna poročila o obveščevalnih dejavnostih, tudi od pravosodnega ministra, DNI, obveščevalnih agencij in drugih nadzornih organov (npr. generalnih inšpektorjev), glej uvodni izjavi 164 in 165. Zlasti v skladu z zakonom o nacionalni varnosti „[p]redsednik zagotovi, da so kongresni obveščevalni odbori v celoti in sproti obveščeni o obveščevalnih dejavnostih Združenih držav, vključno s katero koli pomembno predvideno obveščevalno dejavnostjo, kot se zahteva v skladu s tem podpoglavjem“ ([333]). Poleg tega „[p]redsednik zagotovi, da so kongresni obveščevalni odbori nemudoma obveščeni o kakršni koli nezakoniti obveščevalni dejavnosti in tudi o kakršnih koli popravnih ukrepih, sprejetih ali so načrtovanih v povezavi s tako nezakonito dejavnostjo“ ([334]).

(170) Poleg tega dodatne zahteve glede poročanja izhajajo iz posebnih zakonov. Zlasti FISA zahteva, da pravosodni minister „v celoti obvešča“ odbore spodnjega doma in senata za obveščevalno dejavnost in pravosodje o dejavnostih vlade v skladu z nekaterimi členi FISA ([335]). Zahteva tudi, da vlada kongresnim odborom predloži kopije vseh odločb, sklepov ali mnenj FISC ali FISCR, ki vključujejo pomembno formulacijo ali razlago“ določb FISA. Kar zadeva nadzor v skladu s členom 702 FISA, se parlamentarni nadzor izvaja z zakonsko določenimi poročili obveščevalnim in pravosodnim odborom in tudi s pogostim obveščanjem in zaslišanji. To vključuje polletno poročilo pravosodnega ministra, v katerem je opisana uporaba člena 702 FISA, s spremnimi dokumenti, vključno s poročili ministrstva za pravosodje in ODNI o skladnosti, z opisom morebitnih primerov neskladnosti ([336]) ter ločeno polletno oceno pravosodnega ministra in DNI, ki dokumentira skladnost s postopki izbire cilja in zmanjševanja ([337]).

([331]) Člen 3091 naslova 50 zakonodajne zbirke ZDA.

([332]) Na primer, odbori organizirajo tematske obravnave (glej npr. nedavno obravnavo odbora spodnjega doma za pravosodje o „digitalnih mrežah za prestrezanje“, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983 in obravnavo spodnjega doma za obveščevalne dejavnosti o uporabi umetne inteligence s strani obveščevalne skupnosti, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), pa tudi obravnave rednega nadzora, npr. nadzora nad FBI in oddelkom ministrstva za pravosodje za nacionalno varnost, glej https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 in https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Kot primer preiskave glej preiskavo odbora senata za obveščevalno dejavnost v zvezi z vmešavanjem Rusije v volitve ZDA leta 2016, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. V smislu poročanja glej npr. pregled dejavnosti (nadzora) odbora v poročilu odbora senata za obveščevalno dejavnost, predloženem senatu, ki zajema obdobje od 4. januarja 2019 do 3. januarja 2021, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Glej člen 3091(a)(1) naslova 50 zakonodajne zbirke ZDA. Ta določba vsebuje splošne zahteve v zvezi s kongresnim nadzorom na področju nacionalne varnosti.

([334]) Glej Člen 3091(b) naslova 50 zakonodajne zbirke ZDA.

([335]) Glej člene 1808, 1846, 1862, 1871 in 1881f naslova 50 zakonodajne zbirke ZDA.

([336]) Glej člen 1881f naslova 50 zakonodajne zbirke ZDA.

([337]) Glej člen 1881a(l)(1) naslova 50 zakonodajne zbirke ZDA.

(171) Poleg tega FISA od vlade ZDA med drugim zahteva, da Kongresu (in javnosti) vsako leto razkrije število zahtevanih in prejetih sklepov FISA in tudi oceno števila državljanov in nedržavljanov ZDA, nad katerimi se izvaja nadzor ([338]). Zakon zahteva tudi dodatno javno poročanje o številu izdanih NSL v zvezi z državljani in tudi nedržavljani ZDA (hkrati pa prejemnikom sklepov in potrdil FISA ter tudi zahtev za izdajo NSL omogoča, da pod določenimi pogoji izdajo poročila o preglednosti) ([339]).

(172) Splošneje si obveščevalna skupnost ZDA na najrazličnejše načine prizadeva zagotoviti preglednost svojih (tujih) obveščevalnih dejavnosti. na primer, leta 2015 je ODNI sprejel načela preglednosti na področju obveščevalnih dejavnosti in načrt za izvajanje preglednosti ter vsaki obveščevalni agencije odredil, naj za spodbujanje preglednosti in vodenje pobud za preglednost imenuje posebnega uradnika za preglednost obveščevalnih dejavnosti ([340]). V okviru teh prizadevanj je obveščevalna skupnost objavila in še naprej objavlja dele politik, postopkov, poročil o nadzoru, poročil o dejavnostih na podlagi člena 702 FISA in Odredbe št. 12333, odločb in drugega gradiva FISC, ki jim je bila preklicana stopnja zaupnosti, tudi na namenskem spletnem mestu „IC on the Record“, ki jo upravlja ODNI ([341]).

(173) Nazadnje, zbiranje osebnih podatkov v skladu s členom 702 FISA je poleg nadzora nadzornih organov, navedenih v uvodnih izjavah 162 do 168, predmet nadzora FISC ([342]). V skladu s pravilom 13 poslovnika FISC morajo uradniki za presojo skladnosti v obveščevalnih agencijah ZDA o vseh kršitvah člena 702 FISA v zvezi s postopki izbire cilja, zmanjševanja in poizvedovanja poročati ministrstvu za pravosodje in ODNI, ki nato o njih poročajo FISC. Poleg tega ministrstvo za pravosodje in ODNI predložita FISC polletni skupni poročili o ocenjevanju nadzora, v katerih so opredeljeni trendi na področju skladnosti z izbiro cilja; zagotovljeni statistični podatki; opisane kategorije primerov neskladnosti; podrobno opisani razlogi za pojav nekaterih primerov neskladnosti z izbiro cilja, ter navedeni ukrepi, ki so jih sprejele obveščevalne agencije za preprečitev ponovitve ([343]).

(174) Po potrebi (npr. če so ugotovljene kršitve postopkov izbire cilja) lahko sodišče ustrezni obveščevalni agenciji odredi, naj sprejme ukrepe za uveljavljanje pravnih sredstev. ([344]) Zadevni popravni ukrepi lahko zajemajo posamezne ali strukturne ukrepe, npr. od prenehanja pridobivanja podatkov in izbrisa nezakonito pridobljenih podatkov do spremembe prakse zbiranja podatkov, vključno s smernicami in usposabljanjem osebja ([345]). Poleg tega FISC med

([338]) Člen 1873(b) naslova 50 zakonodajne zbirke ZDA. Poleg tega v skladu s členom 402 „direktor nacionalne obveščevalne službe v posvetovanju z generalnim državnim tožilcem izvede pregled v zvezi z odpravo zaupnosti vsake odločbe, sklepa ali mnenja, ki ga izda FISC ali FISCR (kot je opredeljeno v členu 601(e)) in ki vključuje pomembno formulacijo 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 čim bolj zagotovi javno dostopnost vsake take odločbe, sklepa ali mnenja “.

([339]) Člena 1873(b)(7) in 1874 naslova 50 zakonodajne zbirke ZDA.

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

([341]) Glej „IC on the Record“, na voljo na naslovu https://icontherecord.tumblr.com/.

([342]) V preteklosti je FISC ugotovil, da je „Sodišču […] jasno, da izvedbene agencije ter tudi [ODNI] in [oddelek ministrstva za pravosodje za nacionalno varnosti] namenjata znatna sredstva za njune naloge na področju skladnosti in nadzora na podlagi člena 702. Primeri neskladnosti so praviloma ugotovljeni takoj in sprejeti so ukrepi za uveljavljanje pravnik sredstev, ki vključujejo odstranitev netočnih podatkov, ki so bili nepravilno pridobljeni ali drugače predmet zahtev glede uničenja na podlagi veljavnih postopkov“. Sodišče FISA, predhodno mnenje in sklep [redigirano besedilo] (2014), na voljo na naslovu https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) Glej npr. Poročilo ministrstva za pravosodje/ODNI o skladnosti s členom 702 FISA, predloženo FISC za obdobje junij 2018–november 2018, str. 21–65.

([344]) Člen 1803(h) naslova 50 zakonodajne zbirke ZDA. Glej poročilo PCLOB o členu 702, str. 76. Poleg tega glej predhodno mnenje in sklep FISC z dne 3. oktobra 2011 kot primer sklepa o pomanjkljivosti, v katerem je bilo vladi odrejeno, naj v 30 dneh odpravi ugotovljene pomanjkljivosti. Na voljo na naslovu https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Glej Waltonov dopis, oddelek 4, str. 10 in 11. Glej npr. mnenje FISC z dne 18. oktobra 2018, na voljo na naslovu https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, kakor ga je potrdilo FISCR v svojem mnenju z dne 12. julija 2019, na voljo na spletišču https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, v katerem je FISC vladi med drugim odredil izpolnjevanje nekaterih zahtev v zvezi z obveščanjem, dokumentacijo in poročanjem FISC.

([345]) Glej npr. FISC, predhodno mnenje in sklep 76 (6. december 2019) (odobren za javno objavo 4. septembra 2020), v katerem je FISC vladi naložil, naj do 28. februarja 2020 predloži pisno poročilo o korakih vlade za izboljšanje postopka opredeljevanja in odstranjevanja poročil, ki izhajajo iz informacij FISA 702, ki so bila priklicana zaradi skladnosti, ter tudi o drugih zadevah. Glej tudi Prilogo VII.

svojim letnim pregledom potrdil na podlagi člena 702 upošteva primere neskladnosti, da bi ugotovil, ali predložena potrdila izpolnjujejo zahteve FISA. Če FISC ugotovi, da vladna potrdila niso zadostovala, tudi zaradi nekaterih primerov neskladnosti, lahko podobno izda t. i. sklep o pomanjkljivosti, v katerem od vlade zahteva odpravo kršitve v 30 dneh ali prenehanje izvajanja ali neizvedbo potrjevanja na podlagi člena 702. Nazadnje, FISC oceni trende, ki jih opazi v zvezi s težavami na področju skladnosti, in lahko zahteva spremembo postopkov ali dodaten nadzor in poročanje o obravnavi trendov na področju skladnosti ([346]).

3.2.3 ***Pravna sredstva***

(175) Kot je podrobneje pojasnjeno v tem oddelku, številne možnosti v Združenih državah zagotavljajo posameznikom iz Unije, na katere se nanašajo osebni podatki, omogočajo vložitev tožbe pred neodvisnim in nepristranskim sodiščem z zavezujočimi pooblastili. Skupaj posameznikom omogočajo dostop do njihovih osebnih podatkov, pregled zakonitosti vladnega dostopa do njihovih osebnih podatkov in v primeru kršitve njeno odpravo, tudi s popravkom oziroma izbrisom takih podatkov.

(176) Prvič, na podlagi Odredbe št. 14086 je vzpostavljen poseben mehanizem pravnih sredstev, ki ga dopolnjuje uredba pravosodnega ministra o ustanovitvi DPRC za obravnavanje in reševanje pritožb posameznikov, ki se nanašajo na ameriške obveščevalne dejavnosti SIGINT. Vsak posameznik v EU ima pravico mehanizmu pravnih sredstev predložiti pritožbo, ki se nanaša na domnevno kršitev ameriškega zakona, ki ureja obveščevalne dejavnosti SIGINT (npr. Odredba št. 14086, člen 702 FISA, Odredba št. 12333), in negativno vpliva na njegove interese glede varstva zasebnosti in državljanskih svoboščin ([347]). Ta mehanizem pravnih sredstev je na voljo posameznikom iz držav ali regionalnih organizacij za gospodarsko povezovanje, ki jih je pravosodni minister ZDA opredelil kot „države, ki izpolnjujejo pogoje“ ([348]). Pravosodni minister je 30. junija 2023 Evropsko unijo in tri države Evropskega združenja za prosto trgovino, ki skupaj tvorijo Evropski gospodarski prostor, na podlagi člena 3(f) Odredbe št. 14086 opredelil kot „države, ki izpolnjujejo pogoje“ ([349]). Ta opredelitev ne posega v člen 4(2) Pogodbe o Evropski uniji.

(177) Posameznik iz Unije, na katerega se nanašajo osebni podatki in ki želi vložiti takšno pritožbo, mora le-to predložiti nadzornemu organu v državi članici EU, pristojnemu za nadzor nad obdelavo osebnih podatkov s strani javnih organov (organ za varstvo podatkov) ([350]). To zagotavlja preprost dostop do mehanizma pravnih sredstev, saj posameznikom omogoča, da se obrnejo na organ, ki je „v bližini doma“ in s katerim se lahko sporazumevajo v lastnem jeziku. Ko se zahteve za vložitev pritožbe iz uvodne izjave 178 preverijo, bo pristojni organ za varstvo podatkov prek sekretariata Evropskega odbora za varstvo podatkov pritožbo posredoval v mehanizem pravnih sredstev.

(178) Za vložitev pritožbe pri mehanizmu pravnih sredstev veljajo majhne zahteve glede dopustnosti, saj posameznikom ni treba dokazati, da so bili njihovi podatki dejansko predmet ameriških obveščevalnih dejavnosti SIGINT ([351]). Hkrati morajo biti za zagotovitev izhodišča, na podlagi katerega mehanizem pravnih sredstev izvede pregled, predložene nekatere osnovne informacije, tj. v zvezi z osebnimi podatki, za katere se utemeljeno sklepa, da so bili preneseni v ZDA, in v zvezi s sredstvi, s katerimi naj bi bili preneseni; identitetami subjektov vlade ZDA, za katere se sklepa, da so vključeni v domnevne kršitve (če je znano); podlago za domnevo, da je prišlo do kršitve zakonodaje ZDA (čeprav za to prav tako ni potreben dokaz, da so osebne podatke dejansko zbirale ameriške obveščevalne agencije) in naravo zahtevanega nadomestila.

([346]) Glej Prilogo VII.

([347]) Glej člen 4(k)(iv) Odredbe št. 14086, ki določa, da mora pritožbo pri mehanizmu pravnih sredstev vložiti pritožnik v svojem imenu (tj. ne kot predstavnik vlade, nevladne ali medvladne organizacije). Pojem „negativen vpliv“ ne zahteva, da pritožnik doseže določen prag, da bi imel dostop do mehanizma pravnih sredstev (v zvezi s tem glej uvodno izjavo 178). Pojasnjuje pa, da sta ODNI CLPO in DPRC pristojna za odpravo kršitev ameriške zakonodaje, ki ureja obveščevalne dejavnosti SIGINT, ki negativno vplivajo na pritožnikove interese zasebnosti in državljanske svoboščine. Nasprotno pa kršitve zahtev v skladu z veljavno zakonodajo ZDA, ki niso namenjene zaščiti posameznikov (npr. proračunske zahteve), ne spadajo v pristojnost ODNI CLPO in DPRC.

([348]) Člen 3(f) Odredbe št. 14086.

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

([350]) Člen 4(d)(v) Odredbe št. 14086.

([351]) Glej člen 4(k)(i)-(iv) Odredbe št. 14086.

(179) Prvotno preiskavo pritožb, predloženih temu mehanizmu pravnih sredstev, izvaja ODNI CLPO, čigar obstoječa zakonska vloga in zakonska pooblastila so bila razširjena konkretne ukrepe, sprejete v skladu z Odredbo št. 14086 ([352]). V okviru obveščevalne skupnosti je CLPO med drugim pristojen za zagotavljanje, da je varstvo zasebnosti in državljanskih svoboščin ustrezno vključeno v politike in postopke ODNI in obveščevalnih agencij; nadzor ODNI nad skladnostjo z veljavnimi zahtevami glede varstva zasebnosti in državljanskih svoboščin in izvajanje ocen učinka na varstvo zasebnosti ([353]). ODNI CLPO lahko razreši le DNI iz pomembnega razloga, tj. v primeru neustreznega ravnanja, zlorabe položaja, kršitve varnosti, zanemarjanja dolžnosti ali nesposobnosti ([354]).

(180) ODNI CLPO ima pri izvajanju pregleda dostop do informacij za njegovo ocenjevanje in se lahko opre na obvezno pomoč uradnikov za varstvo zasebnosti in državljanskih svoboščin v različnih obveščevalnih agencijah ([355]). Obveščevalne agencije imajo prepoved ovirati ali neustrezno vplivati na preglede ODNI CLPO. To vključuje DNI, ki se ne sme vmešavati v pregled ([356]). Pri pregledu pritožbe mora ODNI CLPO „uporabljati zakon nepristransko“, upoštevati interese nacionalne varnosti na področju obveščevalnih dejavnosti SIGINT in tudi varstvo zasebnosti ([357]).

(181) V okviru svojega pregleda ODNI CLPO ugotovi, ali je prišlo do kršitve veljavne zakonodaje ZDA in, če je to tako, odloči o ustrezni odpravi kršitve ([358]). Slednje se nanaša na ukrepe, ki v celoti odpravljajo ugotovljeno kršitev, kot na primer opustitev nezakonitega pridobivanja podatkov, izbris nezakonito zbranih podatkov, izbris rezultatov neustrezno izvedenih poizvedb drugače nezakonito zbranih podatkov, omejitev dostopa ustrezno usposobljenega osebja do zakonito zbranih podatkov ali priklic obveščevalnih poročil, ki vsebujejo podatke, pridobljene brez zakonitega dovoljenja ali ki so bili nezakonito razširjani ([359]). Odločitve ODNI CLPO o posameznih pritožbah (tudi o odpravi kršitve) so za zadevne obveščevalne agencije zavezujoče ([360]).

(182) ODNI CLPO mora hraniti dokumentacijo o svojem pregledu in predložiti zaupno odločbo s pojasnitvijo podlage za njegove dejanske ugotovitve, z ugotovitvijo, ali je prišlo do zajete kršitve, in določitvijo ustrezne odprave kršitve ([361]). Če je bila pri pregledu ODNI CLPO ugotovljena kršitev katerega koli pooblastila, ki je predmet nadzora FISC, mora CLPO predložiti tudi zaupno poročilo pomočniku pravosodnega ministra za nacionalno varnost, ki nato v skladu z obveznostjo poročanja sporoči neskladnost FISC, ki lahko sprejme nadaljnje izvršilne ukrepe (v skladu s postopkom, opisanim v uvodnih izjavah 173 in 174) ([362]).

(183) Ko je pregled zaključen, ODNI CLPO prek nacionalnega organa obvesti pritožnika, da „pri pregledu bodisi niso bile ugotovljene nobene zajete kršitve ali da je ODNI CLPO izdal odločitev, ki zahteva ustrezno odpravo kršitve“ ([363]). To omogoča varstvo zaupnosti dejavnosti, izvedenih za zaščito nacionalne varnosti, hkrati pa je posameznikom s tem zagotovljena odločba, ki potrjuje, da je bila njihova pritožba ustrezno preiskana, o njej pa je bilo ustrezno odločeno. Poleg tega lahko posameznik to odločbo izpodbija. V ta namen bo obveščen o možnosti vložitve pritožbe pri DPRC za presojo ugotovitev CLPO (glej uvodno izjavo 184 in naslednje) in o tem, da če se bo obrnil na sodišče, bo izbran poseben pravobranilec, ki bo zastopal pritožnikove interese ([364]).

([352]) Glej člen 3(c)(iv) Odredbe št. 14086. Glej tudi člen 103D zakona o nacionalni varnosti iz leta 1947, člen 403-3d naslova 50 zakonodajne zbirke ZDA, kar zadeva vlogo CLPO v ODNI.
([353]) Člen 3029 (b) naslova 50 zakonodajne zbirke ZDA.
([354]) Glej člen 3(c)(iv) Odredbe št. 14086.
([355]) Glej člen 3(c)(iii) Odredbe št. 14086.
([356]) Glej člen 3(c)(iv) Odredbe št. 14086.
([357]) Člena 3(c)(i)(B)(i) in (iii) Odredbe št. 14086.
([358]) Glej člen 3(c)(i) Odredbe št. 14086.
([359]) Člen 4(a) Odredbe št. 14086.
([360]) Glej člen 3(c)(d) Odredbe št. 14086.
([361]) Glej člen 3(c)(i)(F)-(G) Odredbe št. 14086.
([362]) Glej tudi člen 3(c)(i)(D) Odredbe št. 14086.
([363]) Člen 3(c)(i)(E)(1) Odredbe št. 14086.
([364]) Člena 3(c)(i)(E)(2)-(3) Odredbe št. 14086.

(184) Vsak pritožnik in tudi vsak organa obveščevalne skupnosti lahko pred DPRC zahtevajo presojo odločbe ODNI CLPO. Take vloge za presojo morajo biti vložene v 60 dneh po prejemu obvestila s strani ODNI CLPO, da je njegov pregled zaključen, vključevati pa morajo vse informacije, ki jih želi posameznik predložiti DPRC (npr. argumente o pravnih vprašanjih ali uporabi prava za dejstva zadeve) ([365]). Posamezniki iz Unije, na katere se nanašajo osebni podatki, lahko svojo vlogo ponovno vložijo pri pristojnem organu za varstvo podatkov (glej uvodno izjavo 177).

(185) DPRC je neodvisno sodišče, ki ga je pravosodni minister ustanovil na podlagi Odredbe št. 14086 ([366]). Sestavlja ga vsaj šest sodnikov, ki jih imenuje pravosodni minister po posvetovanju s PCLOB, z ministrom za trgovino in DNI za štiriletni mandat z možnostjo podaljšanja ([367]). Imenovanje sodnikov s strani pravosodnega ministra, temelji na merilih, ki jih uporablja izvršilna veja pri ocenjevanju kandidatov za zvezno pravosodje in ki dodeljujejo utež predhodnim sodniškim izkušnjam ([368]). Poleg tega morajo biti sodniki delavci v pravni stroki (tj. aktivni člani odvetniške zbornice in imeti ustrezno licenco za opravljanje odvetniške prakse) ter imeti ustrezne izkušnje s področja prava varstva zasebnosti in nacionalne varnosti. Pravosodni minister si mora prizadevati za zagotovitev, da ima vsaj polovica sodnikov vedno predhodne sodniške izkušnje, vsi sodniki pa morajo imeti varnostna potrdila, da lahko dostopajo do zaupnih podatkov o nacionalni varnosti ([369]).

(186) Za sodnike pri DPRC so lahko imenovani le posamezniki, ki izpolnjujejo kvalifikacije, navedene v uvodni izjavi 185, in ki v času svojega imenovanja ali dve leti pred tem niso oziroma niso bili zaposleni v izvršilni veji. Podobno sodniki v času svojega mandata pri DPRC ne smejo opravljati nobenih uradnih nalog ali biti zaposleni v vladi ZDA (razen kot sodniki pri DPRC) ([370]).

(187) Neodvisnost odločanja se uresničuje s številnimi jamstvi. Zlasti izvršilni veji (pravosodni minister in obveščevalne agencije) je prepovedano vmešavanje v presojo DPRC ali neustrezno vplivanje nanjo ([371]). Sam DPRC pa mora nepristransko odločati o zadevah ([372]) in deluje v skladu z lastnim poslovnikom (sprejetim z večino glasov). Poleg tega lahko sodnike pri DPRC razreši le pravosodni minister in le iz določenih razlogov (tj. neustrezno ravnanje, zloraba položaja, kršitev varnosti, zanemarjanje dolžnosti ali nesposobnost), ob ustreznem upoštevanju standardov, ki veljajo za zvezne sodnike, določene v pravilniku o ravnanju pri opravljanju sodniške službe in postopkih za ugotovitev nezmožnosti opravljanja sodniške službe ([373]).

([365]) Členi 201.6(a)-(b) uredbe pravosodnega ministra.

([366]) Člen 3(d)(i)) in uredba pravosodnega ministra. Vrhovno sodišče Združenih držav je priznalo možnost, da pravosodni minister ustanovi neodvisne organe s pooblastilom za odločanje, tudi za odločanje o posameznih zadevah, glej zlasti Združene države v imenu Accardi/Shaughnessy, 347 U.S. 260 (1954) in Združene države/Nixon, 418 U.S. 683, 695 (1974). Izpolnjevanje različnih zahtev iz Odredbe št. 14086, npr. meril in postopkov za imenovanje in razrešitev sodnikov DPRC, je namreč pod nadzorom generalnega inšpektorja ministrstva za pravosodje (glej tudi uvodno izjavo 109 o zakonskem pooblastilu generalnih inšpektorjev).

([367]) Člen 3(d)(i)(A) Odredbe št. 14086 in člen 201.3(a) uredbe pravosodnega ministra.

([368]) Členi 201.3(b) uredbe pravosodnega ministra.

([369]) Člen 3(d)(i)(B) Odredbe št. 14086.

([370]) Člen 3(d)(i)(A) Odredbe št. 14086 ter člen 201.3(a) in (c) uredbe pravosodnega ministra. Posamezniki, imenovani za sodnike pri DPRC, lahko sodelujejo v zunajsodnih dejavnostih, vključno s poslovanjem, finančnimi dejavnostmi, neprofitnimi dejavnostmi zbiranja sredstev in fiduciarnimi dejavnostmi ter tudi opravljanjem odvetniške prakse, dokler takšne dejavnosti ne vplivajo na nepristransko opravljanje njihovih dolžnosti ali na učinkovitost ali neodvisnost DPRC (člen 201.7(c) uredbe pravosodnega ministra).

([371]) Člen 3(d)(iii)-(iv) Odredbe št. 14086 in člen 201.7(d) uredbe pravosodnega ministra.

([372]) Člen 3(d)(i)(D) Odredbe št. 14086 in člen 201.9 uredbe pravosodnega ministra.

([373]) Člen 3(d)(iv) Odredbe št. 14086 in člen 201.7(d) uredbe pravosodnega ministra. Glej tudi sodbo v zadevi Bumap proti Združenim državam, 252 U.S. 512, 515 (1920), ki je potrdila dolgoletno načelo v zakonodaji ZDA, da je pristojnost razrešitve odvisna od pristojnosti za imenovanje (kot je opozoril tudi urad pravnega svetovalca ministrstva za pravosodje v mnenju Ustavna ločitev oblasti med predsednikom in kongresom, mnenje 20 O.L.C. 124, 166 (1996)).

(188) Vloge, predložene DPRC, presojajo senati treh sodnikov, vključno s predsedujočim sodnikom, ki mora ravnati v skladu s kodeksom ravnanja za sodnike ZDA ([374]). Vsakemu senatu pomaga posebni pravobranilec ([375]), ki ima dostop do vseh informacij, ki se nanašajo na zadevo, vključno z zaupnimi informacijami ([376]). Vloga posebnega pravobranilca je zagotoviti, da so pritožnikovi interesi zastopani in da je senat DPRC dobro seznanjen z vsemi ustreznimi pravnimi in dejanskimi vprašanji ([377]). Da bi se posebni pravobranilec podrobneje seznanil z vlogo za presojo, ki jo je pri DPRC vložil posameznik, lahko s pisnimi vprašanji od pritožnika zahteva informacije ([378]).

(189) DPRC presoja ugotovitve ODNI CLPO (glede kršitev veljavne zakonodaje ZDA in tudi glede ustrezne odprave kršitve) vsaj na podlagi evidence o preiskavi ODNI CLPO in tudi vseh informacij in vlog, ki so jih predložili pritožnik, posebni pravobranilec ali obveščevalna agencija ([379]). Senat DPRC ima dostop do vseh informacij, potrebnih za izvedbo presoje, ki jih lahko pridobi prek ODNI CLPO (senat lahko npr. od CLPO zahteva, naj svoje evidence dopolni z dodatnimi informacijami ali dejanskimi ugotovitvami, če je to potrebno za izvedbo presoje) ([380]).

(190) Pri izvajanju svoje presoje lahko DPRC (1) odloči, da ni dokazov o tem, da je prišlo do obveščevalnih dejavnosti SIGINT, ki vključujejo pritožnikove osebne podatke, (2) odloči, da so bile ugotovitve ODNI CLPO pravno pravilne in podprte z utemeljenimi dokazi, ali (3), če se DPRC ne strinja z ugotovitvami ODNI CLPO (o tem, ali je bila kršena veljavna zakonodaja ZDA, ali glede ustrezne odprave kršitve), izda lastne ugotovitve ([381]).

([374]) Člen 3(d)(i)(B) Odredbe št. 14086 in člen 201.7(a)-(c) uredbe pravosodnega ministra. OPCL v okviru ministrstva za pravosodje, ki je pristojno za zagotavljanje upravne podpore DPRC in posebnim pravobranilcem (glej člen 201.5 uredbe pravosodnega ministra), izbere senat s tremi sodniki po načelu rotacije, s čimer si prizadeva zagotoviti, da ima vsak senat vsaj enega sodnika s prehodnimi sodniškimi izkušnjami (če teh nima noben sodnik, bo predsedujoči sodnik tisti, ki ga bo najprej izbral OPCL).

([375]) Člen 201.4 uredbe pravosodnega ministra. Pravosodni minister imenuje vsaj dva posebna pravobranilca po posvetovanju z ministrom za trgovino, DNI in PCLOB za mandat z možnostjo dvakratnega podaljšanja. Posebni pravobranilci morajo imeti izkušnje s področja prava varstva zasebnosti in nacionalne varnosti, biti izkušen odvetniki, aktivni člani odvetniške zbornice in imeti ustrezno licenco za opravljanje odvetniške prakse. Poleg tega dve leti pred svojim prvotnim imenovanjem niso smeli biti zaposleni v izvršilni veji. Za vsako presojo vloge predsedujoči sodnik izbere posebnega pravobranilca za pomoč senatu; glej člen 201.8(a) uredbe pravosodnega ministra.

([376]) Člen 201.8(c) in člen 201.11 uredbe pravosodnega ministra.

([377]) Člen 3(d)(i)(C) Odredbe št. 14086 in člen 201.8(e) uredbe pravosodnega ministra. Posebni pravobranilec ne deluje v vlogi posrednika pritožnika in z njim ni v odnosu odvetnik-stranka.

([378]) Glej člen 201.8(d)(e) uredbe pravosodnega ministra. Taka vprašanja najprej pregleda OPLC po posvetovanju z ustreznim organom obveščevalne skupnosti, da bi opredelil in izločil morebitne zaupne ali privilegirane ali zaščitene informacije pred posredovanjem vprašanj pritožniku. Dodatne informacije, ki jih posebni pravobranilec prejme v odgovoru na taka vprašanja, vsebujejo vloge, ki jih posebni pravobranilec predloži DPRC.

([379]) Člen 3(d)(i)(D) Odredbe št. 14086.

([380]) Člen 3(d)(iii) Odredbe št. 14086 in člen 201.9(b) uredbe pravosodnega ministra.

([381]) Člen 3(d)(i)(E) Odredbe št. 14086 in člen 201.9(c)-(e) uredbe pravosodnega ministra. V skladu z opredelitvijo pojma „ustrezna odprava kršitev“ iz člena 4(a) Odredbe št. 14086 mora DPRC pri odločanju o popravnem ukrepu za popolno odpravo kršitve med drugim upoštevati „načine, na katere so se običajno obravnavale ugotovljene kršitve“, tj. DPRC bo med drugimi dejavniki preučil, kako so bile podobne težave v zvezi s skladnostjo odpravljene v preteklosti, da se zagotovi učinkovitost in ustreznost pravnega sredstva.

(191) DPRC v vseh primerih sprejme pisno odločbo z večino glasov. Če je v presoji ugotovljena kršitev veljavnih pravil, bo v odločbi navedena vsaka ustrezna odprava kršitev, ki vključuje izbris nezakonito zbranih podatkov, izbris rezultatov neustrezno izvedenih poizvedb, omejitev dostopa ustrezno usposobljenega osebja do zakonito zbranih podatkov ali priklic obveščevalnih poročil, ki vsebujejo podatke, pridobljene brez zakonitega dovoljenja ali ki so bili nezakonito razširjani ([382]). Odločba DPRC je v zvezi z obravnavano pritožbo dokončna in zavezujoča ([383]). Poleg tega, če je bila pri presoji ugotovljena kršitev katerega koli pooblastila, ki je predmet nadzora FISC, mora DPRC predložiti tudi zaupno poročilo pomočniku pravosodnega ministra za nacionalno varnost, ki nato v skladu z obveznostjo poročanja sporoči neskladnosti FISC, ki lahko sprejme nadaljnje izvršilne ukrepe (v skladu s postopkom, opisanim v uvodnih izjavah 173 in 174) ([384]).

(192) Vsaka odločba senata DPRC je posredovana ODNI CLPO ([385]). V primerih, v katerih je presojo DPRC sprožila vloga pritožnika, je pritožnik prek nacionalnega organa obveščen, da je DPRC zaključil svojo presojo in da „pri presoji bodisi niso bile ugotovljene nobene zajete kršitve bodisi je DPRC izdal ugotovitev, ki zahteva ustrezno odpravo kršitve“ ([386]). OPCL v okviru ministrstva za pravosodje hrani evidenco vseh informacij, ki jih je pregledal DPRC, in vseh izdanih odločb, ki so kot nezavezujoč precedens na voljo prihodnjim senatom DPRC za preučitev ([387]).

(193) Ministrstvo za trgovino mora hraniti tudi evidenco vsakega pritožnika, ki je vložil pritožbo ([388]). Za večjo preglednost mora ministrstvo za trgovino vsaj vsakih pet let stopiti v stik z ustreznimi obveščevalnimi agencijami, da bi preverilo, ali je bila informacijam, ki se nanašajo na presojo DPR, preklicana stopnja zaupnosti ([389]). Če je to tako, bo posameznik obveščen, da so lahko take informacije na voljo na podlagi veljavne zakonodaje (tj. da lahko zahteva dostop do njih na podlagi FOIA, glej uvodno izjavo 199).

(194) Nazadnje, pravilno delovanje tega mehanizma pravnih sredstev bo predmet rednega in neodvisnega vrednotenja. Natančneje, v skladu z Odredbo št. 14086 je delovanje mehanizma pravnih sredstev predmet letnega pregleda PCLOB, neodvisnega organa (glej uvodno izjavo 110) ([390]). V okviru svojega pregleda bo PCLOB med drugim ocenil, ali sta ODNI CLPO in DPRC pritožbe obravnavala pravočasno; ali sta pridobila popoln dostop do potrebnih informacij; ali so bili v postopku pregleda ustrezno upoštevani vsebinski zaščitni ukrepi iz Odredbe št. 14086 in ali je obveščevalna skupnost v celoti ravnala v skladu z ugotovitvami ODNI CLPO in DPRC. PCLOB bo poročilo o izidu svojega pregleda predložil predsedniku, pravosodnemu ministru, DNI, vodji obveščevalnih agencij, ODNI CLPO in kongresnim odborom za obveščevalno dejavnost, ki bo tudi objavljen v nezaupni različici, nato pa vključen v redni pregled delovanja tega sklepa, ki ga bo izvedla Komisija. Pravosodni minister, DNI, ODNI CLPO in vodje obveščevalnih agencij morajo izvajati ali drugače obravnavati vsa priporočila, ki jih vključujejo taka poročila. Poleg tega bo PCLOB izdal letno javno potrdilo o tem, ali mehanizem pravnih sredstev obravnava pritožbe v skladu z zahtevami Odredbe št. 14086.

([382]) Člen 4(a) Odredbe št. 14086.

([383]) Člen 3(d)(ii) Odredbe št. 14086 in člen 201.9(g) uredbe pravosodnega ministra. Glede na to, da je odločba DPRC dokončna in zavezujoča, nobena druga izvršilna ali upravna institucija/organ (vključno s predsednikom Združenih držav) ne more razveljaviti odločitve DPRC. To je bilo potrjeno tudi v sodni praksi vrhovnega sodišča, ki je pojasnilo, da se pravosodni minister s prenosom edinstvenega pooblastila pravosodnega ministra znotraj izvršilne veje oblasti za izdajanje zavezujočih odločitev na neodvisni organu odreka možnosti, da bi na kakršen koli način narekoval odločitev tega organa (glej sodbo v zadevi Združene države v povezavi z Accardi proti Shaughnessy, 347 U.S. 260 (1954).

([384]) Člen 3(d)(i)(F) Odredbe št. 14086 in člen 201.9(i) uredbe pravosodnega ministra.

([385]) Člen 201.9(h) uredbe pravosodnega ministra.

([386]) Člen 3(d)(i)(H) Odredbe št. 14086 in člen 201.9(h) uredbe pravosodnega ministra. Glede narave obvestila glej člen 201.9(h)(3) uredbe pravosodnega ministra.

([387]) Člen 201.9(j) uredbe pravosodnega ministra.

([388]) Člen 3(d)(v)(A) Odredbe št. 14086.

([389]) Člen 3(d)(v) Odredbe št. 14086.

([390]) Člen 3(e) Odredbe št. 14086. Glej tudi https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Poleg posebnega mehanizma pravnih sredstev, vzpostavljenega na podlagi Odredbe št. 14086, so možnosti pravnih sredstev na voljo vsem posameznikom (ne glede na državljanstvo ali prebivališče) pred rednimi sodišči ZDA ([391]).

(196) Zlasti FISA in povezan zakon določata možnost, da posamezniki vložijo civilno tožbo za denarno odškodnino proti Združenim državam, če so bile informacije o njih nezakonito in namerno uporabljene ali razkrite ([392]); da tožijo osebno uslužbence vlade ZDA za denarno odškodnino ([393]) 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 ([394]). Splošneje, če namerava vlada uporabiti informacije, pridobljene med izvajanjem obveščevalne dejavnosti, proti osumljencu v kazenski zadevi, ustavne in zakonske zahteve ([395]) nalagajo obveznost razkritja nekaterih informacij, tako da lahko obdolženec izpodbija zakonitost vladnega zbiranja in uporabe dokazov.

(197) Poleg tega obstaja več posebnih možnosti pritožbe proti vladnim uslužbencem zaradi nezakonitega vladnega dostopa do osebnih podatkov ali njihove uporabe, tudi za domnevne namene nacionalne varnosti (to so zakon o računalniških goljufijah in zlorabah ([396]), ECPA ([397]) in zakon o pravici do finančne zasebnosti ([398])). Vsa te tožbe se nanašajo na konkretne podatke, ciljne osebe 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).

(198) Splošnejšo možnost pravnega varstva zagotavlja APA ([399]), 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 sodni nadzor ([400]). To vključuje možnost, da se sodišču predlaga, naj „ugotovi, da so ukrepanje, ugotovitve in sklepi agencije, za katere je bilo ugotovljeno, da so […] samovoljni, arbitrarni, da predstavljajo zlorabo diskrecijske pravice ali so drugače neskladni s pravom, nezakoniti in jih razveljavi“ ([401]). Zvezno pritožbeno sodišče je leta 2015 o zahtevku na podlagi APA na primer odločilo, da množično zbiranje telefonskih metapodatkov s strani vlade ZDA ni bilo dovoljeno na podlagi člena 501 FISA ([402]).

([391]) Dostop do teh možnosti je predmet izkaza „pravnega interesa“. Ta standard, ki se uporablja za vsakega posameznika ne glede na njegovo državljanstvo, izhaja iz zahteve po „nasprotujočih si zahtevkih“ iz člena III ustave ZDA. V skladu z razlago vrhovnega sodišča mora zato (1) posameznik utrpeti „dejansko škodo“ (tj. oškodovan mora biti pravno varovan interes, ki je konkreten in podrobno opredeljen in dejanski ali neposreden), (2) obstajati vzročna zveza med škodo in ravnanjem, izpodbijanim pred sodiščem in (3) obstajati verjetnost in ne špekulacija, da bo s pozitivno odločbo sodišča škoda odpravljena (glej Lujan/Defenders of Wildlife, 504 U.S. 555 (1992)).

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

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

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

([395]) Glej sodbo v zadevi Brady proti Maryland, 373 U.S. 83 (1963), oziroma zakon Jencks, člen 3500 naslova 18 zakonodajne zbirke ZDA.

([396]) Člen 1030 naslova 18 zakonodajne zbirke ZDA.

([397]) Členi 2701–2712 naslova 18 zakonodajne zbirke ZDA.

([398]) Člen 3417 naslova 12 zakonodajne zbirke ZDA.

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

([400]) Na splošno se sodni nadzor opravi le za „končno“ ukrepanje agencije in ne za „predhodno, postopkovno ali vmesno“ ukrepanje agencije. Glej Člen 704 naslova 5 zakonodajne zbirke ZDA.

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

([402]) ACLU/Clapper, 785 F.3d 787 (pritožbeno sodišče drugega okrožja Združenih držav Amerike 2015). Program za množično zbiranje telefonskih podatkov, izpodbijan v teh zadevah, je bil ukinjen z zakonom ZDA o svobodi iz leta 2015 (*USA FREEDOM Act*).

(199) Nazadnje, poleg možnosti pravnih sredstev, navedenih v uvodnih izjavah 176–198, ima vsak posameznik na podlagi FOIA pravico zahtevati dostop do obstoječih evidenc zvezne agencije, tudi če te vsebujejo posameznikove osebne podatke ([403]). Pridobitev takega dostopa lahko olajša vlaganje tožb pred rednimi sodišči, tudi v podporo izkazu pravnega interesa. Agencije lahko zadržijo informacije, ki spadajo med določene navedene izjeme, vključno z dostopom do zaupnih podatkov o nacionalni varnosti in podatkov, ki se nanašajo na preiskave kazenskega pregona ([404]), vendar imajo pritožniki, ki niso zadovoljni z odzivom, možnost, da ga izpodbijajo z zahtevkom za upravni in nato sodni nadzor (pred zveznimi sodišči) ([405]).

(200) Iz zgoraj navedenega izhaja, da kadar organi ZDA za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter za nacionalno varnost izvajajo dostop do osebnih podatkov, ki spadajo na področje uporabe tega sklepa, tak dostop ureja pravni okvir, ki določa pogoje, na podlagi katerih je dostop mogoč, pri tem pa omejuje dostop in nadaljnjo uporabo podatkov na tisto, kar je potrebno in sorazmerno glede na cilj v javnem interesu. Te zaščitne ukrepe lahko uveljavljajo posamezniki, ki imajo pravice do učinkovitih pravnih sredstev.

4. **SKLEPNA UGOTOVITEV**

(201) Komisija meni, da Združene države z načeli, ki jih je izdalo ministrstvo za trgovino, zagotavljajo raven varstva osebnih podatkov, ki se prenašajo iz Unije certificiranim organizacijam v ZDA na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA, ki je v osnovi enakovredna ravni, zagotovljeni z Uredbo (EU) 2016/679.

(202) Poleg tega Komisija meni, da dejansko uporabo načel zagotavljajo obveznosti glede preglednosti in upravljanje DPF s strani ministrstva za trgovino. Gledano v celoti nadzorni mehanizmi in pravna sredstva v zakonodaji ZDA poleg tega v praksi omogočajo, da se kršitve pravil o varstvu podatkov ugotovijo in kaznujejo, ter da so posameznikom, na katere se nanašajo osebni podatki, na voljo pravna sredstva, s katerimi lahko pridobijo dostop do osebnih podatkov, ki se nanašajo nanje, in po potrebi zagotovijo popravek ali izbris takih podatkov.

(203) Nazadnje, Komisija na podlagi razpoložljivih informacij o pravnem redu ZDA, vključno z informacijami iz prilog VI in VII, meni, da bodo vsak poseg v temeljne pravice posameznikov, katerih osebne podatke javni organi ZDA prenašajo iz Unije v Združene države v javnem interesu, zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter namene nacionalne varnosti na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA, omejen na to, kar je nujno potrebno za dosego zadevnega zakonitega cilja, ter da obstaja učinkovito pravno varstvo pred takim posegom. Zato bi bilo treba glede na zgornje ugotovitve odločiti, da Združene države zagotavljajo ustrezno varstvo v smislu člena 45 Uredbe (EU) 2016/679, kot se razlaga glede na Listino Evropske unije o temeljnih pravicah, v zvezi z osebnimi podatki, ki se iz Evropske unije prenašajo organizacijam, certificiranim na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA.

(204) Glede na to, da so omejitve, zaščitni ukrepi in mehanizmi pravnega varstva, določeni v Odredbi št. 14086, bistveni elementi pravnega okvira ZDA, na katerem temelji ocena Komisije, sprejetje tega sklepa temelji na sprejetju posodobljenih politik in postopkov za izvajanje Odredbe št. 14086 s strani vseh obveščevalnih agencij ZDA in določitvi Unije kot organizacije, ki izpolnjuje pogoje za namene mehanizma pravnega sredstva, kar se je zgodilo 3. julija 2023 (glej uvodno izjavo 126) oziroma 30. junija 2023 (glej uvodno izjavo 176).

([403]) Člen 552 naslova 5 zakonodajne zbirke ZDA. Podobni zakoni obstajajo na ravni države.

([404]) V tem primeru posameznik običajno prejme standardni odgovor, s katerim agencija odkloni potrditev ali zavrnitev obstoja kakršnih koli evidenc. Glej zadevo ACLU/CIA, 710 F.3d 422 (pritožbeno sodišče Združenih držav Amerike za zvezno okrožje Kolumbije 2014). Merila in trajanje tajnosti so določena v izvršilni odredbi št. 13526, ki na splošno določa, da je treba za preklic stopnje tajnosti določiti konkreten datum ali dogodek na podlagi trajanja občutljivosti podatkov za nacionalno varnost, takrat pa se mora tajnost podatkov samodejno preklicati (glej člen 1.5 Odredbe št. 13526).

([405]) Sodišče na novo ugotovi, ali so evidence ustrezno zadržane in lahko vladi odredi, da zagotovi dostop do evidenc (člen 552(a)(4)(B) naslova 5 zakonodajne zbirke ZDA).

5. **UČINKI TEGA SKLEPA IN UKREPI ORGANOV ZA VARSTVO PODATKOV**

(205) Države članice in njihovi organi morajo sprejeti ukrepe, potrebne za zagotavljanje skladnosti z akti institucij Unije, saj se domneva, da so ti zakoniti in imajo pravne učinke, dokler niso umaknjeni, razveljavljeni na podlagi izpodbojne tožbe ali razglašeni za neveljavne na podlagi predloga za sprejetje predhodne odločbe ali sklicevanja na nezakonitost.

(206) Zato je sklep Komisije o ustreznosti varstva, sprejet na podlagi člena 45(3) Uredbe (EU) 2016/679, zavezujoč za vse organe držav članic, na katere je naslovljen, vključno z njihovimi neodvisnimi nadzornimi organi. Natančneje, prenosi od upravljavca ali obdelovalca v Uniji certificiranim organizacijam v Združenih državah lahko potekajo, ne da bi bilo treba pridobiti nadaljnje dovoljenje.

(207) V skladu s členom 58(5) Uredbe (EU) 2016/679 in glede na pojasnila Sodišča v sodbi v zadevi Schrems ([406]) je treba opozoriti, da če ima nacionalni organ za varstvo podatkov tudi po prejemu pritožbe pomisleke glede skladnosti sklepa Komisije o ustreznosti s temeljnimi pravicami posameznika do varstva zasebnosti in podatkov, mu mora nacionalno pravo zagotavljati pravno sredstvo za predložitev teh očitkov nacionalnemu sodišču, ki bi morda moralo pri Sodišču vložiti predlog za sprejetje predhodne odločbe ([407]).

6. **SPREMLJANJE IN PREGLED TEGA SKLEPA**

(208) V skladu s sodno prakso Sodišča ([408]) in kot je navedeno v členu 45(4) Uredbe (EU) 2016/679, bi morala Komisija po sprejetju sklepa o ustreznosti redno spremljati razvoj dogodkov v tretji državi, da se presodi, ali tretja država še zagotavlja v osnovi enakovredno raven varstva. Tako preverjanje je vsekakor nujno, kadar Komisija prejme kakršne koli informacije, ki zbujajo upravičen dvom o tem.

(209) Komisija bi zato morala stalno spremljati razmere v Združenih državah, kar zadeva pravni okvir in dejansko prakso obdelave osebnih podatkov, kot sta ocenjena v tem sklepu. Za olajšanje tega postopka bi morali organi ZDA Komisijo nemudoma obvestiti o bistvenem razvoju pravnega reda ZDA, ki vpliva na pravni okvir, ki je predmet tega sklepa, ter o razvoju praks v zvezi z obdelavo osebnih podatkov, ocenjenih v tem sklepu, in sicer tako glede obdelave osebnih podatkov s strani certificiranih organizacij v Združenih državah kot tudi glede omejitev in zaščitnih ukrepov, ki se uporabljajo za dostop javnih organov do osebnih podatkov.

(210) Poleg tega bi morale države članice Komisijo obveščati o vseh pomembnih ukrepih nacionalnih organov za varstvo podatkov, zlasti glede poizvedb ali pritožb posameznikov iz Unije, na katere se nanašajo osebni podatki, v zvezi s prenosom osebnih podatkov iz Unije certificiranim organizacijam v Združenih državah, da lahko Komisija učinkovito izvaja naloge spremljanja. Komisija bi morala biti obveščena tudi o kakršnih koli indicih, da ukrepi javnih organov ZDA, odgovornih za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj oziroma za nacionalno varnost, vključno z vsemi nadzornimi organi, ne zagotavljajo zahtevane ravni varnosti.

([406]) Sodba v zadevi Schrems, točka 65.

([407]) Sodba v zadevi Schrems, točka 65: „V zvezi s tem mora nacionalni zakonodajalec določiti pravna sredstva, ki zadevnemu nacionalnemu nadzornemu organu omogočajo, da očitke, ki jih šteje za utemeljene, predloži nacionalnim sodiščem, da bi ta, če bi prav tako kot ta organ dvomila o veljavnosti odločbe Komisije, sprožila postopek predhodnega odločanja za preizkus veljavnosti navedene odločbe.“

([408]) Sodba v zadevi Schrems, točka 76.

(211) Komisija bi morala po sprejetju tega sklepa na podlagi člena 45(3) Uredbe (EU) 2016/679 ([409]) redno preverjati, ali so ugotovitve, ki se nanašajo na ustreznost ravni varstva, ki jo zagotavljajo Združene države na podlagi DPF EU-ZDA, še vedno dejansko in pravno upravičene. Ker zlasti Odredba št. 14086 in uredba pravosodnega ministra zahtevata vzpostavitev novih mehanizmov in izvajanje novih zaščitnih ukrepov, bi bilo treba ta sklep prvič pregledati v enem letu po začetku njegove veljavnosti, da bi se preverilo, ali so bili vsi ustrezni elementi v celoti izvedeni in učinkovito delujejo v praksi. Komisija po tem prvem pregledu in glede na rezultate pregleda v tesnem posvetovanju z odborom, ustanovljenim v skladu s členom 93(1) Uredbe (EU) 2016/679, in Evropskim odborom za varstvo podatkov odloči o periodičnosti prihodnjih pregledov ([410]).

(212) Za izvedbo pregledov bi se morala Komisija sestati z ministrstvom za trgovino, FTC in ministrstvom za promet, po potrebi pa tudi z drugimi ministrstvi in agencijami, vključenimi v izvajanje DPF EU-ZDA, ter, glede zadev, ki se nanašajo na nacionalno varnost, s predstavniki ministrstva za pravosodje, ODNI (vključno s CLPO), drugimi organi obveščevalne skupnosti, DPRC in tudi posebnimi pravobranilci. Možnost sodelovanja na takem srečanju bi morali imeti tudi predstavniki članov Evropskega odbora za varstvo podatkov.

(213) Pregledi bi morali vključevati vse vidike učinkovanja tega sklepa glede obdelave osebnih podatkov v Združenih državah, zlasti uporabo in izvajanje načel, pri čemer bi bilo treba posebno pozornost nameniti varstvu v primeru nadaljnjih prenosov; razvoj ustrezne sodne prakse; učinkovitost uresničevanja pravic posameznikov; spremljanje in izvrševanje skladnosti z načeli; ter omejitve in zaščitne ukrepe v zvezi z vladnim dostopom, zlasti izvajanje in uporabo zaščitnih ukrepov, uvedenih z Odredbo št. 14086, vključno s politikami in postopki, ki so jih razvile obveščevalne agencije; medsebojni vpliv Odredbe št. 14086 ter člena 702 FISA in Odredbe št. 12333; ter učinkovitost nadzornih mehanizmov in pravnih sredstev (vključno z delovanjem novega mehanizma pravnih sredstev, vzpostavljenega na podlagi Odredbe št. 14086). V okviru takih pregledov bo pozornost namenjena tudi sodelovanju med organi za varstvo podatkov in pristojnimi organi Združenih držav, vključno z razvojem smernic in drugih razlagalnih orodij glede uporabe načel ter glede drugih vidikov delovanja okvira.

(214) Komisija bi morala na podlagi pregleda pripraviti javno poročilo, ki se predloži Evropskemu parlamentu in Svetu.

7. ZAČASNO ZADRŽANJE IZVAJANJA, RAZVELJAVITEV ALI SPREMEMBA TEGA SKLEPA

(215) Če se na podlagi razpoložljivih informacij, zlasti tistih, ki izhajajo iz spremljanja tega sklepa ali ki jih zagotovijo organi ZDA ali organi držav članic, ugotovi, da raven varstva, ki se zagotavlja glede osebnih podatkov, prenesenih s tem sklepom, morda ni več ustrezna, bi morala Komisija o tem takoj obvestiti pristojne organe ZDA in zahtevati, naj se v določenem razumnem roku sprejmejo ustrezni ukrepi.

(216) Če pristojni organi ZDA ob preteku tega določenega roka ne sprejmejo navedenih ukrepov ali drugače zadovoljivo dokažejo, da ta sklep še naprej temelji na ustreznem varstvu, bo Komisija začela postopek iz člena 93(2) Uredbe (EU) 2016/679 za začasno zadržanje izvajanja ali za razveljavitev dela ali celotnega tega sklepa.

(217) Druga možnost je, da bo Komisija začela navedeni postopek za spremembo tega sklepa, zlasti z uvedbo dodatnih pogojev za prenos podatkov ali z omejitvijo področja uporabe ugotovitve o ustreznosti samo na prenose podatkov, za katere je še naprej zagotovljeno ustrezno varstvo.

([409]) V skladu s členom 45(3) Uredbe (EU) 2016/679 se v „izvedbenem aktu […] določi mehanizem za redni pregled […], ki v celoti upošteva razvoj dogodkov na zadevnem področju v tretji državi ali mednarodni organizaciji".

([410]) Člen 45(3) Uredbe (EU) 2016/679 določa, da mora biti redni pregled izveden „vsaj vsaka štiri leta". Glej tudi Evropski odbor za varstvo podatkov, referenčni dokument o ustreznosti, WP 254 rev. 01.

(218) Komisija bi morala zlasti začeti postopek za začasno zadržanje izvajanja ali razveljavitev v primeru:

(a) indicev, da organizacije, ki so prejele osebne podatke iz Unije na podlagi tega sklepa, ne spoštujejo načel ter da pristojni nadzorni in izvršilni organi takega nespoštovanja ne obravnavajo učinkovito;

(b) indicev, da organi ZDA ne izpolnjujejo veljavnih pogojev in omejitev za dostop javnih organov ZDA za kazenski pregon in nacionalno varnost do osebnih podatkov, ki se prenašajo v skladu z okvirom o varstvu podatkov med EU in ZDA ali

(c) neučinkovitega obravnavanja pritožb posameznikov iz EU, na katere se nanašajo osebni podatki, tudi s strani ODNI CLPO in/ali DPRC.

(219) Prav tako bi morala Komisija razmisliti o začetku postopka za spremembo, začasno zadržanje izvajanja ali razveljavitev tega sklepa, če pristojni organi ZDA ne zagotovijo informacij ali pojasnil, potrebnih za oceno ravni varstva, ki se zagotavlja glede osebnih podatkov, prenesenih iz Unije v Združene države, ali skladnosti s tem sklepom. V tem smislu bi morala Komisija upoštevati, v kolikšni meri je mogoče zadevne informacije pridobiti iz drugih virov.

(220) Komisija bo v ustrezno utemeljenih nujnih primerih, na primer če bi bila Odredba št. 14086 ali uredba pravosodnega ministra spremenjena tako, da bi bila ogrožena raven varstva, opisana v tem sklepu, ali pa če bi pravosodni minister umaknil opredelitev Unije kot organizacije, ki izpolnjuje pogoje za namene mehanizma pravnega sredstva, uporabila možnost, da v skladu s postopkom iz člena 93(3) Uredbe (EU) 2016/679 sprejme izvedbene akte, ki se začnejo uporabljati takoj in s katerimi se začasno zadrži izvajanje tega sklepa oziroma se sklep razveljavi ali spremeni.

8. **SKLEPNE UGOTOVITVE**

(221) Evropski odbor za varstvo podatkov je objavil svoje mnenje ([411]), ki je bilo upoštevano pri pripravi tega sklepa.

(222) Evropski parlament je sprejel resolucijo o ustreznosti zaščite, ki jo zagotavlja okvir EU–ZDA za varstvo podatkov ([412]).

(223) Ukrepi iz tega sklepa so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 93(1) Uredbe (EU) 2016/679 –

SPREJELA NASLEDNJI SKLEP:

Člen 1

Za namen člena 45 Uredbe (EU) 2016/679 Združene države zagotavljajo ustrezno varstvo osebnih podatkov, ki se iz Evropske unije prenašajo organizacijam v Združenih državah, ki so vključene na „seznam okvira za varstvo zasebnosti podatkov“, ki ga vodi in objavlja Ministrstvo za trgovino ZDA v skladu s členom I.3 Priloge I.

Člen 2

Kadar pristojni organi v državah članicah z namenom varstva posameznikov v zvezi z obdelavo njihovih osebnih podatkov izvajajo svoja pooblastila na podlagi člena 58 Uredbe (EU) 2016/679 v zvezi s prenosom podatkov iz člena 1 tega sklepa, zadevna država članica o tem brez odlašanja obvesti Komisijo.

([411]) Mnenje št. 5/2023 o osnutku izvedbenega sklepa Evropske komisije o ustreznem varstvu osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA z dne 28. februarja 2023.

([412]) Resolucija Evropskega parlamenta z dne 11. maja 2023 o ustreznosti zaščite, ki jo zagotavlja okvir za varstvo zasebnosti podatkov med EU in ZDA (2023/2501(RSP)).

Člen 3

1. Komisija stalno spremlja uporabo pravnega okvira, ki je predmet tega sklepa, vključno s pogoji, pod katerimi se izvajajo nadaljnji prenosi in uveljavljajo individualne pravice ter pod katerimi imajo javni organi ZDA dostop do podatkov, prenesenih na podlagi tega sklepa, da bi ocenila, ali Združene države še naprej zagotavljajo ustrezno varstvo iz člena 1.

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

3. Države članice in Komisija se medsebojno obveščajo o vseh indicih, da posegi javnih organov ZDA, pristojnih za uresničevanje nacionalne varnosti, kazenskega pregona ali drugih javnih interesov, v pravico posameznikov do varstva osebnih podatkov presegajo to, kar je nujno potrebno, in/ali da zoper take posege ni učinkovitega pravnega varstva.

4. Komisija po enem letu od uradnega obvestila državam članicam o tem sklepu, nato pa redno na obdobje, ki bo določeno v tesnem posvetovanju z odborom, ustanovljenim v skladu s členom 93(1) Uredbe (EU) 2016/679, in Evropskim odborom za varstvo podatkov, oceni ugotovitve iz člena 1(1) na podlagi vseh razpoložljivih informacij, vključno z informacijami, pridobljenimi v okviru pregleda, ki se opravi s pristojnimi organi Združenih držav.

5. Če Komisija prejme indic, da ustrezno varstvo ni več zagotovljeno, o tem obvesti pristojne organe ZDA. Po potrebi se bo odločila, da začasno zadrži izvajanje tega sklepa, ga spremeni ali razveljavi ali pa omeji njegovo področje uporabe, v skladu s členom 45(5) Uredbe (EU) 2016/679. Komisija lahko take ukrepe sprejme tudi, če zaradi nesodelovanja vlade ZDA ne more ugotoviti, ali Združene države še naprej zagotavljajo ustrezno varstvo.

Člen 4

Ta sklep je naslovljen na države članice.

V Bruslju, 10. julija 2023

Za Komisijo
Didier REYNDERS
član Komisije

PRILOGA I

NAČELA OKVIRA ZA VARSTVO ZASEBNOSTI PODATKOV MED EU IN ZDA, KI JIH JE IZDALO MINISTRSTVO ZA TRGOVINO ZDA

I. PREGLED

1. Čeprav so Združene države (ZDA) in Evropska unija (EU) zavezane krepitvi varstva zasebnosti, pravne države in priznavanju pomena čezatlantskega pretoka podatkov za naše zadevne državljane, gospodarstva in družbe, je pristop Združenih držav do zasebnosti drugačen od pristopa EU. V Združenih državah se uporablja sektorski pristop, ki temelji na mešanici zakonodaje, predpisov in samourejanja. Ministrstvo za trgovino ZDA (*Department of Commerce*, v nadaljnjem besedilu: Ministrstvo) izdaja v okviru svoje zakonske pristojnosti, da omogoča, spodbuja in razvija mednarodno trgovino, načela okvira za varstvo zasebnosti podatkov med EU in ZDA, vključno z dopolnilnimi načeli (v nadaljnjem besedilu skupaj: načela) in s Prilogo I k načelom (v nadaljnjem besedilu: Priloga I) (člen 1512 naslova 15 zakonodajne zbirke ZDA). Načela so bila oblikovana v posvetovanju z Evropsko komisijo (v nadaljnjem besedilu: Komisija), predstavniki industrije in drugimi deležniki zaradi lajšanja trgovskih in gospodarskih stikov med Združenimi državami in EU. Načela, ključen sestavni del okvira za varstvo zasebnosti podatkov med EU in ZDA (*Data Privacy Framework*, v nadaljnjem besedilu: DPF EU-ZDA), zagotavljajo organizacijam v Združenih državah zanesljiv mehanizem za prenose osebnih podatkov iz EU v Združene države, hkrati pa, 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. Namenjena so izključno organizacijam v Združenih državah, ki prejemajo osebne podatke iz EU, z namenom izpolnjevanja pogojev DPF EU-ZDA in s tem prejemanja ugodnosti iz sklepa Evropske komisije o ustreznosti ([1]). Načela ne vplivajo na uporabo Uredbe (EU) 2016/679 (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov) ([2]), ki se uporablja za obdelavo osebnih podatkov v državah članicah EU. 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 uporabila DPF EU-ZDA, mora samocertificirati svojo zavezanost načelom pri Ministrstvu (ali njegovemu pooblaščenemu predstavniku). Medtem ko so odločitve organizacij, da tako vstopijo v DPF EU-ZDA popolnoma prostovoljne, pa je dejansko spoštovanje načel obvezno: organizacije, ki se samocertificirajo pri Ministrstvu in javno razglasijo svojo zavezanost načelom, morajo načela spoštovati v celoti. Organizacija mora za pristop k DPF EU-ZDA (a) spadati v okvir preiskovalnih in izvršilnih pooblastil Zvezne komisije za trgovino ZDA (*Federal Trade Commission*, v nadaljnjem besedilu: FTC), Ministrstva za promet ZDA (*Department of Transportation*, v nadaljnjem besedilu: ministrstvo 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 spoštovanju načel; (c) javno razkriti svoje politike zasebnosti v skladu s temi načeli in (d) jih v celoti izvajati ([3]). Če organizacija ne izpolnjuje načel, lahko postopek zoper njo začne FTC na podlagi člena 5 zakona o FTC (*Federal Trade Commission Act*), ki prepoveduje nepoštena in goljufiva dejanja v trgovini ali v zvezi z njo (člen 45 naslova 15 zakonodajne zbirke ZDA), ministrstvo za promet na podlagi člena 41712 naslova 49 zakonodajne zbirke ZDA, ki prevozniku ali agenciji za prodajo letalskih vozovnic prepoveduje nepošteno ali goljufivo ravnanje pri prodaji zračnega prevoza, ali pa se postopek začne na podlagi drugih zakonov in predpisov, ki prepovedujejo taka dejanja.

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

([2]) UREDBA (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).

([3]) Načela okvira zasebnostnega ščita EU-ZDA so bila spremenjena v „Načela okvira za varstvo zasebnosti podatkov med EU in ZDA“. (Glej dopolnilno načelo o samocertificiranju).

3. Ministrstvo bo vodilo verodostojen seznam organizacij iz ZDA, ki so se samocertificirale pri Ministrstvu in razglasile svojo zavezanost spoštovanju načel, (v nadaljnjem besedilu: seznam okvira za varstvo zasebnosti podatkov) ter javnosti omogočilo dostop do njega. Ugodnosti DPF EU-ZDA so zagotovljene od datuma, ko Ministrstvo uvrsti organizacijo na seznam okvira za varstvo zasebnosti podatkov. Ministrstvo bo s seznama okvira za varstvo zasebnosti podatkov odstranilo tiste organizacije, ki prostovoljno izstopijo iz DPF EU-ZDA ali ne opravijo svojega letnega ponovnega certificiranja pri Ministrstvu; te organizacije morajo bodisi še naprej uporabljati načela za osebne podatke, ki so jih prejele v skladu z DPF EU-ZDA, in Ministrstvu vsako leto potrditi svojo zavezanost tej uporabi (npr. dokler hranijo take informacije), zagotoviti „ustrezno“ varstvo podatkov z drugimi dovoljenimi sredstvi (na primer s sklenitvijo pogodbe, ki v celoti izraža zahteve ustreznih standardnih pogodbenih klavzul, ki jih sprejema Komisija) bodisi podatke vrniti bodisi izbrisati. Ministrstvo bo s seznama okvira za varstvo zasebnosti podatkov odstranilo tudi tiste organizacije, ki vztrajno niso spoštovale načel; te organizacije morajo vrniti ali izbrisati osebne podatke, ki so jih prejele v skladu z DPF EU-ZDA. Odstranitev organizacije s seznama okvira za varstvo zasebnosti podatkov pomeni, da ta ni več upravičena do ugodnosti, ki izhajajo iz sklepa Komisije o ustreznosti, da bi prejemala osebne podatke iz EU.

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 odstranjene s seznama okvira za varstvo zasebnosti podatkov. Ministrstvo bo navedlo jasno opozorilo, da te organizacije ne sodelujejo v DPF EU-ZDA; da odstranitev s seznama okvira za varstvo zasebnosti podatkov pomeni, da take organizacije ne morejo trditi, da izpolnjujejo načela DPF EU-ZDA , ter da se morajo vzdržati morebitnih izjav ali zavajajočih ravnanj, ki bi nakazovala, da sodelujejo v DPF EU-ZDA, in da take organizacije niso več upravičene do ugodnosti, ki izhajajo iz sklepa Komisije o ustreznosti , da bi prejemale osebne podatke iz EU. Proti organizaciji, ki še naprej trdi, da sodeluje v DPF EU-ZDA, ali daje druge lažne navedbe v zvezi z DPF EU-ZDA, potem ko je že bila odstranjena s seznama okvira za varstvo zasebnosti podatkov, lahko FTC, ministrstvo za promet ali drugih organi pregona uvedejo izvršilne ukrepe.

5. Zavezanost načelom je lahko omejena: (a) če je to potrebno za izpolnitev sodne odločbe ali izpolnjevanje zahtev javnega interesa, kazenskega pregona ali nacionalne varnosti, tudi če se z zakonom ali vladnim podzakonskim aktom ustvari nezdružljivost obveznosti; (b) z zakonom, sodno odločbo ali vladnim podzakonskim aktom, ki ustvari nezdružljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel omejeno toliko, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takšnih pooblastil; ali (c) če Splošna uredba o varstvu podatkov dovoljuje izjeme in odstopanja pod pogoji, ki so določeni v njej, če se te izjeme in odstopanja uporabljajo v primerljivih okoliščinah. V tem okviru zaščitni ukrepi iz zakonodaje ZDA o varstvu zasebnosti in državljanskih svoboščin vključujejo tiste, zahtevane v Odredbi št. 14086 ([4]) pod pogoji, določenimi v njej (vključno z zahtevami glede nujnosti in sorazmernosti). V skladu s ciljem krepitve varstva zasebnosti si morajo organizacije prizadevati, da načela uveljavijo v celoti in pregledno, vključno s prizadevanji, da v svoji politiki varstva zasebnosti navedejo, kdaj se bodo izjeme, dovoljene s točko (b) zgoraj, uporabljale. Iz istega razloga se od organizacij pričakuje, da se, kadar načela in/ali zakonodaja ZDA dopuščajo izbiro, odločijo za možnost z večjim varstvom.

6. Organizacije morajo po vstopu v DPF EU-ZDA načela uporabljati za vse osebne podatke, ki se prenašajo na podlagi uporabe DPF EU-ZDA. Organizacija, ki se odloči razširiti ugodnosti DPF EU-ZDA 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.

([4]) Odredba z dne 7. oktobra 2022 z naslovom „*Enhancing Safeguards for United States Signals Intelligence Activities*“ („Krepitev zaščitnih ukrepov za obveščevalne dejavnosti SIGINT“).

7. Zakonodaja ZDA se bo uporabljala za vprašanja glede razlage in izpolnjevanja načel ter ustreznih politik zasebnosti organizacij v DPF EU-ZDA, razen če so se takšne organizacije zavezale sodelovanju z evropskimi organi za varstvo 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 spadajo na področje uporabe Splošne uredbe o varstvu podatkov ter jih organizacije v ZDA prejmejo iz EU.

   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 in Priloge I k načelom je datum začetka veljavnosti sklepa Evropske komisije o ustreznosti.

II. **NAČELA**

1. **OBVESTILO**

a. Organizacija mora posameznike obvestiti o:

   i. svojem sodelovanju v DPF EU-ZDA in zagotoviti povezavo na seznam okvira za varstvo zasebnosti podatkov ali njegov spletni naslov;

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

   iii. svoji zavezi, da pri vseh osebnih podatkih, ki jih prejme iz EU na podlagi DPF EU-ZDA, uporabi načela;

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

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

   vi. vrsti ali identiteti tretjih strank, ki jim razkrije osebne podatke, in namene njihovega razkritja;

   vii. pravici posameznikov do dostopa do svojih osebnih podatkov;

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

   ix. neodvisnem organu za reševanje sporov, določenem za obravnavanje pritožb in brezplačno zagotavljanje ustreznega pritožbenega mehanizma posamezniku, in ali je to: (1) forum, ki ga ustanovijo organi za varstvo podatkov, (2) drug izvajalec reševanja sporov s sedežem v EU ali (3) drug izvajalec reševanja sporov s sedežem v Združenih državah;

   x. tem, da zanje veljajo preiskovalna in izvršilna pooblastila FTC, ministrstva za promet ali katerega koli drugega ameriškega zakonsko določenega organa;

   xi. možnosti posameznika, da pod določenimi pogoji uveljavi zavezujočo arbitražo ([5]);

   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.

([5]) Glej člen (c) načela pritožbenega mehanizma, izvrševanja in odgovornosti.

b. To obvestilo mora biti jasno in nedvoumno, ko organizacija posameznika prvič prosi za zagotovitev osebnih podatkov ali takoj, ko je to izvedljivo, vsekakor pa preden se podatki uporabijo za namene, ki niso tisti, za katere jih je prvotno zbrala in obdelala pošiljajoča organizacija, ali preden se prvič razkrijejo tretji stranki.

2. **MOŽNOST IZBIRE**

a. Organizacija mora posameznikom ponuditi možnost izbire (tj. zavrnitve) o tem, ali se bodo njihovi osebni podatki (i) razkrili tretji stranki ali (ii) se bodo uporabili za namen, ki je bistveno drugačen od namena/-ov, za katere/-ga so bili prvotno zbrani ali ga/jih je posameznik pozneje odobril. 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 vključujejo 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 (tj. privolitev), kadar je takšne podatke treba (i) razkriti tretji stranki ali (ii) jih uporabiti za namen, ki ni namen, 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 podatke, 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 podatkov 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 varstva 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 je 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 (vi) 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 razširjajo 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 narave osebnih podatkov.

5. **CELOVITOST PODATKOV IN OMEJITEV NAMENA**

a. V skladu z načeli je treba osebne podatke omejiti na informacije, ki ustrezajo namenu obdelave ([6]). 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 ta namen, mora organizacija z ustreznimi ukrepi zagotoviti, da so podatki zanesljivi za nameravano uporabo, točni, popolni in aktualni. Organizacija mora spoštovati načela, dokler hrani take podatke.

b. Podatki se lahko hranijo v obliki, s katero je posameznik določen ali določljiv ([7]), le dokler se uporabljajo za namen obdelave v smislu točke 5(a). Ta obveznost organizacijam ne preprečuje nadaljnje obdelave osebnih podatkov za daljša obdobja, vendar 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. V teh primerih za tako obdelavo veljajo druga načela in določbe DPF EU-ZDA. 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 v nasprotju z načeli, 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.

7. **PRITOŽBENI MEHANIZEM, IZVRŠEVANJE IN ODGOVORNOST**

a. Učinkovita zaščita zasebnosti mora vključevati trdne mehanizme, ki zagotavljajo skladnost z načeli, pritožbene mehanizme za posameznike, ki jih neizpolnjevanje načel zadeva, 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 njihovih praks varstva 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 se javno zavezale spoštovanju načel, 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 DPF EU-ZDA. 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 varstvo podatkov, vključno z organizacijami, ki obdelujejo podatke o človeških virih, morajo neposredno odgovoriti takšnim organom v zvezi s preiskovanjem in reševanjem pritožb.

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

([7]) Posameznik je v tem smislu „prepoznaven“, 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.

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 sodelujoča organizacija odgovorna za obdelavo osebnih podatkov, ki jih prejme v skladu z DPF EU-ZDA in naknadno prenese tretji stranki, ki je v vlogi posrednika v njenem imenu. Sodelujoča organizacija ostane odškodninsko odgovorna po načelih, če njen posrednik obdeluje take osebne podatke na način, ki ni skladen z načeli, razen če organizacija dokaže, da ni odgovorna za dogodek, ki je povzročil škodo.

e. Če organizacija postane predmet sodne odločbe zaradi neizpolnjevanja načel ali sklepa zakonsko določenega organa ZDA (tj. FTC ali ministrstvo za promet), navedenega v načelih ali prihodnji prilogi k načelom, zaradi neizpolnjevanja, organizacija objavi vse ustrezne dele poročila o skladnosti ali oceni v zvezi z DPF EU-ZDA, ki se predloži sodišču ali zakonsko določenemu organu ZDA, če je to skladno z zahtevami glede zaupnosti. Ministrstvo je imenovalo posebno osebo za stike z organi za varstvo podatkov v primeru težav glede izpolnjevanja načel s strani sodelujočih organizacij. FTC in ministrstvo za promet bosta prednostno obravnavala zadeve v zvezi z neizpolnjevanjem načel, ki jih bodo predložili Ministrstvo in organi držav članic EU, ter bosta 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.

3. Sekundarna odgovornost

a. Ponudniki internetnih storitev, telekomunikacijska podjetja in druge organizacije niso odgovorni v skladu z načeli, kadar v imenu druge organizacije zgolj prenašajo, usmerjajo, zamenjujejo ali pridobivajo informacije. DPF EU-ZDA ne ustvarja sekundarne odgovornosti. Če 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 bodo 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 s sodelujočimi organizacijami, so predmet rednih revizij. Takšne revizije, zlasti tiste, ki preiskujejo morebitna hudodelstva, so lahko ogrožene, če so razkrite prehitro. Podobno bo morala sodelujoča organizacija, ki je vključena 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 varstvo podatkov**

a. Organizacije bodo izvajale svojo zavezo k sodelovanju z organi EU za varstvo podatkov, kakor je opisano spodaj. V skladu z DPF EU-ZDA se morajo organizacije ZDA, ki prejemajo osebne podatke iz EU, zavezati, da bodo uporabile učinkovite mehanizme za zagotavljanje izpolnjevanja načel. 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 praks varstva zasebnosti in (a)(iii) obveznosti odpravljanja težav, ki nastanejo zaradi nespoštovanja načel, in posledice za te organizacije. Organizacija lahko izpolni točki (a)(i) in (a)(iii) načela pritožbenega mehanizma, uveljavljanja in odgovornosti, če se zaveže zahtevam, določenim tukaj, za sodelovanje z organi za varstvo podatkov.

b. Organizacija se zaveže, da bo sodelovala z organi za varstvo podatkov, tako da v vlogi za samocertificiranje v skladu z DPF EU-ZDA Ministrstvu (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 varstvo podatkov;

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

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

c. Delovanje forumov organov za varstvo podatkov

i. Sodelovanje z organi za varstvo podatkov EU bo potekalo v obliki informacij in nasvetov na naslednji način:

1. nasvete organov za varstvo 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 skladu z DPF EU-ZDA. Nasvet bo oblikovan za zagotovitev pravilne uporabe načel in bo vključeval vsa pravna sredstva za zadevne posameznike, ki jih bodo organi za varstvo 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 varstvo podatkov za namene DPF EU-ZDA, 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 varstvo 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 varstvo 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 FTC 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, da ustrezno spremeni seznam okvira za varstvo zasebnosti podatkov. Vsako neizpolnjevanje zaveze o sodelovanju z organi za varstvo podatkov, pa tudi nespoštovanje načel bo kaznovano kot goljufiva praksa v skladu s členom 5 zakona o FTC (člen 45 naslova 15 zakonodajne zbirke ZDA), člen 41712 naslova 49 zakonodajne zbirke ZDA, ali drugega podobnega zakona.

d. Organizacija, ki želi ugodnosti v skladu z DPF EU-ZDA za podatke o človeških virih, ki se prenesejo iz EU v okviru zaposlitvenega razmerja, se mora zavezati k sodelovanju z organi za varstvo 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. Znesek pristojbine bo določilo Ministrstvo po posvetovanju s Komisijo. Pristojbino lahko pobira tretja stranka, ki jo izbere Ministrstvo in je v vlogi skrbnika sredstev, zbranih za ta namen. Ministrstvo bo tesno sodelovalo s Komisijo in organi za varstvo podatkov pri določitvi ustreznih postopkov za razdelitev sredstev, zbranih s pristojbino, pa tudi pri drugih postopkovnih in upravnih vidikih foruma. Ministrstvo in Komisija se lahko dogovorita o spremembi pogostosti pobiranja pristojbine.

6. **Samocertificiranje**

a. Ugodnosti DPF EU-ZDA se zagotavljajo od datuma, na katerega Ministrstvo uvrsti organizacijo na seznam okvira za varstvo zasebnosti podatkov. Ministrstvo bo organizacijo na seznam okvira za varstvo zasebnosti podatkov uvrstilo šele po ugotovitvi, da je vloga za začetno samocertificiranje popolna, s tega seznama pa jo bo odstranilo, če ta prostovoljno izstopi, ne opravi svojega letnega ponovnega certificiranja ali če vztrajno ne spoštuje načel (glej dopolnilno načelo glede reševanja sporov in izvrševanja).

b. Če želi organizacija izvesti začetno samocertificiranje ali poznejše ponovno certificiranje za DPF EU-ZDA, mora v obeh primerih vlogo Ministrstvu predložiti vodstveni delavec v imenu organizacije, ki samocertificira ali ponovno certificira (kakor je ustrezno) lastno spoštovanje načel ([8]), vloga pa mora vsebovati vsaj naslednje podatke:

([8]) Vlogo v zvezi s spoštovanjem načel mora prek spletnega mesta okvira za varstvo zasebnosti podatkov na spletišču Ministrstva oddati posameznik v organizaciji, ki je pooblaščen za zastopanje v imenu organizacije in katerega koli od njenih vključenih subjektov.

i. ime organizacije v ZDA, ki se samocertificira ali ponovno certificira, pa tudi imena vseh njenih subjektov ali podružnic v ZDA, ki tudi spoštujejo načela, ki jih želi organizacija zajeti;

ii. opis dejavnosti organizacije v zvezi z osebnimi podatki, ki bi jih prejemala iz EU v skladu z DPF EU-ZDA;

iii. opis ustrezne/-ih politik/-e zasebnosti organizacij v zvezi s takimi osebnimi podatki, vključno s podatki:

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

2. datum začetka izvajanja;

iv. osebo za stike v organizaciji, ki se ukvarja s pritožbami, zahtevami po dostopu in drugimi vprašanji, ki izhajajo iz načel ([9]), vključno z:

1. imeni, nazivi delovnega mesta (kakor je ustrezno), elektronskimi naslovi in telefonskimi številkami ustreznih posameznikov ali ustreznih oseb za stike in

2. ustreznim ameriškim poštnim naslovom organizacije;

v. posebno zakonsko telo, ki je pristojno za obravnavanje morebitnih pritožb proti organizaciji v zvezi z morebitnimi nepoštenimi ali zavajajočimi ravnanji in kršitvami zakonov ali predpisov, ki urejajo varstvo zasebnosti (in ki je navedeno v načelih ali v prihodnji prilogi k načelom);

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

vii. metodo preverjanja (tj. samoocenjevanje; ali zunanji pregledi skladnosti, vključno s tretjo stranko, ki izvaja take preglede) ([10]); in

viii. ustrezen/-ni neodvisni pritožbeni mehanizem/-mi, ki je/so na voljo za preiskave nerešenih pritožb v zvezi z načeli ([11]).

c. Če organizacija želi, da bi ugodnosti DPF EU-ZDA zajele tudi podatke o človeških virih, prenesene iz Evropske unije za uporabo v okviru zaposlitvenih razmerij, lahko to stori, če 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 vlogi za začetno samocertificiranje in tudi v vseh vlogah za ponovno certificiranje 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 varstvo podatkov (kakor je primerno) in 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.

([9]) Glavna „oseba za stike organizacije“ ali „vodilni delavec organizacije“ ne more biti oseba zunaj organizacije (npr. zunanji pravnik ali zunanji svetovalec).

([10]) Glej dopolnilno načelo glede preverjanja.

([11]) Glej dopolnilno načelo glede reševanja sporov in izvrševanja.

d. Ministrstvo bo vodilo in objavilo seznam organizacij v okviru za varstvo zasebnosti podatkov, ki so vložile popolne vloge za začetno samocertificiranje, navedeni seznam pa bo posodabljalo na podlagi popolnih vlog za letno ponovno certificiranje in tudi uradnih obvestil, prejetih v skladu z dopolnilnim načelom glede reševanja sporov in izvrševanja. Takšne vloge za ponovno certificiranje je treba vložiti najmanj enkrat letno, sicer bo organizacija odstranjena s seznama okvira za varstvo zasebnosti podatkov in ji ugodnosti DPF EU-ZDA ne bodo več zagotovljene. Vse organizacije, ki jih Ministrstvo uvrsti na seznam okvira za varstvo zasebnosti podatkov, morajo imeti ustrezne politike zasebnosti, ki so skladne z načelom obvestila, v njih pa morajo navesti, da spoštujejo načela ([12]). Če je politika zasebnosti organizacije na voljo na spletu, mora vključevati hiperpovezavo na spletno mesto okvira za varstvo zasebnosti podatkov na spletišču Ministrstva in hiperpovezavo na spletno mesto neodvisnega pritožbenega mehanizma ali njegovega obrazca za predložitev pritožbe, ki je na voljo za preiskave nerešenih pritožb v zvezi z načeli, ki so za posameznika brezplačne.

e. Načela zasebnosti začnejo veljati takoj po samocertificiranju. Sodelujoče organizacije, ki so se prej samocertificirale za načela okvira zasebnostnega ščita EU-ZDA, bodo morale posodobiti svoje politike zasebnosti in se namesto tega sklicevati na „načela okvira za varstvo zasebnosti podatkov med EU in ZDA“. Take organizacije vključijo ta sklic čim prej, vsekakor pa najpozneje tri mesece po datumu začetka veljavnosti načel okvira za varstvo zasebnosti podatkov med EU in ZDA.

f. Organizacija mora pri vseh osebnih podatkih, ki jih prejme iz EU na podlagi DPF EU-ZDA, spoštovati načela. Za osebne podatke, ki jih organizacija prejme v času, ko uživa ugodnosti DPF EU-ZDA, zaveza načelom ni časovno omejena; njena zaveza pomeni, da bo organizacija upoštevala načela, dokler take podatke hrani, uporablja ali razkriva, čeprav bo morda pozneje iz kakršnega koli razloga izstopila iz DPF EU-ZDA. Če organizacija želi izstopiti iz DPF EU-ZDA, mora o tem vnaprej obvestiti Ministrstvo. V obvestilu mora tudi navesti, kaj bo storila z osebnimi podatki, ki jih je prejela na podlagi DPF EU-ZDA (tj. ali bo hranila, vrnila ali izbrisala podatke, in če bo podatke hranila, navede dovoljena sredstva, s katerim bo zagotavljala varstvo podatkov). Organizacija, ki izstopi iz DPF EU-ZDA, a želi hraniti takšne podatke, mora vsako leto pri Ministrstvu potrditi svojo zavezo, da bo za podatke še naprej uporabljala načela ali zagotovila „ustrezno“ varstvo podatkov z drugimi dovoljenimi sredstvi (na primer, s pogodbo, ki v celoti izraža zahteve ustreznih standardnih pogodbenih klavzul, ki jih sprejema Evropska komisija); v nasprotnem primeru mora organizacija podatke vrniti ali izbrisati ([13]). Organizacija, ki izstopi iz DPF EU-ZDA, mora iz vsake ustrezne politike zasebnosti odstraniti vse sklice na DPF EU-ZDA, ki nakazujejo, da organizacija še naprej sodeluje v DPF EU-ZDA in je upravičena do njegovih ugodnosti.

([12]) Organizacija, ki se samocertificira prvič, v svoji končni politiki zasebnosti ne sme trditi, da sodeluje v DPF EU-ZDA, dokler je Ministrstvo ne obvesti, da lahko to stori. Ko organizacija vloži vlogo za začetno samocertificiranje, mora Ministrstvu predložiti osnutek politike zasebnosti, ki je skladen z načeli. Ko Ministrstvo ugotovi, da je vloga organizacije za začetno samocertificiranje sicer popolna, jo bo obvestilo, naj dokonča (npr. objavi, če je ustrezno) svojo politiko zasebnosti, skladno z DPF EU-ZDA. Organizacija mora Ministrstvo nemudoma obvestiti, ko je politika zasebnosti dokončana, Ministrstvo pa jo bo takrat uvrstilo na seznam okvira za varstvo zasebnosti podatkov.

([13]) Če se organizacija ob izstopu odloči, da bo hranila osebne podatke, ki jih je prejela na podlagi DPF EU-ZDA, in da bo Ministrstvu vsako leto potrdila, da bo še naprej upoštevala načela pri takih podatkih, mora Ministrstvu enkrat na leto po svojem izstopu (tj. razen če in dokler organizacija zagotavlja „ustrezno“ varstvo takih podatkov z drugimi dovoljenimi sredstvi ali vse take podatke vrne ali izbriše, o tem ukrepu pa uradno obvesti Ministrstvo) dokazati, kaj je storila z navedenimi osebnimi podatki, kaj bo storila z vsemi navedenimi osebnimi podatki, ki jih še naprej hrani, in kdo v organizaciji bo imel vlogo osebe za stike za vprašanja v zvezi z načeli.

g. Organizacija, ki zaradi spremembe statusa, kot je združitev, prevzem, stečaj ali likvidacija, preneha obstajati kot ločena pravna oseba, mora o tem vnaprej uradno obvestiti Ministrstvo. V uradnem obvestilu mora tudi navesti, ali bo subjekt zaradi spremembe statusa (i) še naprej sodeloval v DPF EU-ZDA na podlagi obstoječega samocertificiranja; (ii) se bo samocertificiral kot nov udeleženec v DPF EU-ZDA (npr. če nov subjekt ali subjekt, ki še vedno posluje, še ni opravil samocertificiranja, s katerim bi lahko sodeloval v DPF EU-ZDA); ali (iii) uvedel druge zaščitne ukrepe, kot je pisni sporazum, ki bo zagotovil nadaljnjo uporabo načel za vse osebne podatke, ki jih je organizacija prejela v skladu z DPF EU-ZDA in jih bo hranil. Če se ne uporabljajo niti (i) niti (ii) niti (iii), je treba vse osebne podatke, ki so bili prejeti v skladu z DPF EU-ZDA, nemudoma vrniti ali izbrisati.

h. Če organizacija iz kakršnega koli razloga izstopi iz DPF EU-ZDA, mora odstraniti vse izjave, ki nakazujejo, da še naprej sodeluje v DPF EU-ZDA ali je upravičena do ugodnosti DPF EU-ZDA. Prav tako je treba odstraniti certifikacijsko oznako DPF EU-ZDA, če se uporablja. Vsako zavajanje širše javnosti o spoštovanju načel s strani organizacije lahko FTC, ministrstvo za promet ali drug ustrezen vladni organ kaznuje. Zavajanje Ministrstva se lahko kaznuje na podlagi zakona 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 glede svojih praks varstva zasebnosti v skladu z DPF EU-ZDA, ter izvajanja teh praks na naveden način in v skladu z načeli.

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. Če se je organizacija odločila za samoocenjevanje, mora tako preverjanje pokazati, da je njena politika zasebnosti v zvezi z osebnimi podatki, prejetimi iz EU, točna, celovita, dostopna, skladna z načeli in v celoti izvedena (tj. ravna v skladu z njo). Pokazati mora tudi, da so posamezniki obveščeni o kakršnem koli notranjem mehanizmu organizacije za obravnavo pritožb in o neodvisnem/-ih pritožbenem/-ih mehanizmu/-ih, prek katerega/-ih 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, da je bilo samoocenjevanje izvedeno, 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. Če se je organizacija odločila za zunanji pregled skladnosti z načeli, mora tako preverjanje pokazati, da je njena politika zasebnosti v zvezi z osebnimi podatki, prejetimi iz EU, natančna, celovita, dostopna, skladna z načeli in v celoti izvedena (tj. ravna v skladu z njo). Pokazati mora tudi, da so posamezniki obveščeni o mehanizmu/-ih, prek katerega/-ih se lahko pritožijo. Metode pregledovanja lahko brez omejitve vključujejo revizijo, naključne preglede, uporabo „vab“ ali tehnoloških orodij, kakor je ustrezno. Izjavo o uspešno opravljenem 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 izvajanju svojih praks varstva zasebnosti v skladu z DPF EU-ZDA 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 Ministrstva in njegove druge zahteve za informacije, povezane s spoštovanjem načel s strani organizacije.

8. **Dostop**

a. Načelo dostopa v praksi

i. V skladu z načeli 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 ([14]);

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 v nasprotju z načeli.

ii. Posameznikom ni treba obrazložiti zahtev po dostopu do njihovih osebnih podatkov. Organizacije bi morale pri odzivu na posameznikovo zahtevo po dostopu najprej preučiti težavo/-e, ki so sprožile zahtevo. 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 kateri/-e del/-e 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 osebe za stike za morebitne nadaljnje poizvedbe.

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.

ii. Na primer, če se bodo osebni podatki uporabili za odločitve, ki bodo pomembno vplivale na posameznika (npr. zavrnitev ali dodelitev pomembnih ugodnosti, kot so zavarovanje, hipoteka ali zaposlitev), potem mora organizacija v skladu z drugimi določbami teh dopolnilnih načel razkriti navedene podatke, tudi če je zagotovitev njihovega dostopa razmeroma težka ali draga. Če zahtevani osebni podatki niso občutljiv ali se ne uporabijo za odločitve, ki bodo pomembno vplivale na posameznika, temveč so dostopni in poceni, mora organizacija zagotoviti dostop do takih podatkov.

c. Zaupne poslovne 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, če bi z odobritvijo polnega dostopa razkrile svoje zaupne tržne informacije, kot so v organizaciji narejeni tržni koncepti ali klasifikacije, ali zaupne tržne informacije drugega, za katerega velja pogodbena obveznost o zaupnosti.

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

ii. Kadar je zaupno tržno informacijo mogoče zlahka ločiti od drugih osebnih podatkov, 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 podatke, za katere ni potreben dostop posameznika do podatkovne zbirke organizacije.

ii. Dostop je treba zagotoviti samo do osebnih podatkov, 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 s Splošno uredbo o varstvu podatkov lahko organizacija omeji dostop do podatkov le, če 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, če 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 tožbene zahtevke, vključno s preprečevanjem, preiskovanjem ali odkrivanjem kaznivih dejanj in pravico do poštenega sojenja;

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

3. kršitev zakonskih ali 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 skrbnim upravljanjem, ali v prihodnjih 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 osebe za stike za nadaljnje poizvedbe, ki bi jih predložili posamezniki.

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 se mu posredujejo osebni podatki, ki se nanašajo nanj. Organizacija lahko zaračuna pristojbino, ki ni previsoka.

ii. Zaračunavanje pristojbine je lahko upravičeno, na primer, če so zahteve za dostop očitno pretirane, zlasti zaradi njihove ponavljajoče se narave.

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

g. Ponavljajoče se in zlonamerne zahteve za dostop

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

h. Goljufive zahteve za dostop

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

i. Časovni okvir za odgovore

i. Organizacije bi morale 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 nanašajo osebni podatki, lahko izpolni posamezno zahtevo za dostop z rednim razkritjem, če to ne bi pomenilo nesorazmerne zamude.

9. **Podatki o človeških virih**

a. Kritje DPF EU-ZDA

i. Če organizacija v EU prenese osebne podatke o svojih zaposlenih (nekdanjih ali sedanjih), zbrane v okviru zaposlitvenega razmerja, matični družbi, povezanemu podjetju ali nepovezanemu izvajalcu storitev v Združenih državah, ki sodeluje v DPF EU-ZDA, veljajo za prenos ugodnosti DPF EU-ZDA. V takih primerih bodo za zbiranje in obdelavo podatkov pred prenosom veljali nacionalni zakoni države članice EU, v kateri so bili zbrani, pri prenosu pa bo treba spoštovati vse pogoje in omejitve v skladu z navedenimi zakoni.

ii. Načela se uporabljajo samo za prenos ali dostop do evidenc, ki so posamično določene ali določljive. Pri statističnem poročanju, ki temelji na zbirnih podatkih o zaposlenosti, in ne vsebuje osebnih podatkov ali vključuje uporabo anonimiziranih podatkov, se vprašanje varstva zasebnosti ne pojavlja.

b. Uporaba načel obvestila in možnosti izbire

i. Organizacija v ZDA, ki je prejela podatke o zaposlenih iz EU v skladu z DPF EU-ZDA, jih lahko razkrije tretji stranki ali uporabi za drugačne namene le v skladu z načeloma obvestila in možnosti izbire. Na primer, če namerava organizacija uporabiti podatke, zbrane v zaposlitvenem razmerju, za namene, ki niso povezani z zaposlitvenim razmerjem, kot so tržne komunikacije, mora organizacija v ZDA pred tem zadevnim posameznikom zagotoviti predpisano možnost izbire, razen če so že odobrili uporabo podatkov v take namene. Taka uporaba ne sme biti nezdružljiva s prvotnimi nameni, za katere so bili osebni podatki zbrani ali ki 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 opozoriti, da nekateri splošno veljavni pogoji za prenos iz nekaterih držav članic EU lahko izključijo drugačne vrste uporabe takih podatkov tudi po prenosu v države zunaj EU, in take pogoje bo treba spoštovati.

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

iv. Organizaciji ni treba zagotoviti 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

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

d. Izvrševanje

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 varstva podatkov in 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 varstvo podatkov ali delovnopravni organ, ki je pristojen tam, kjer delajo zaposleni. Sem spadajo tudi primeri, ko je za domnevno zlorabo osebnih podatkov odgovorna organizacija v ZDA, ki je prejela podatke od delodajalca, in tako vključuje domnevno kršitev načel. To bo najbolj učinkovit način za obravnavanje pogosto prekrivajočih se pravic in obveznosti, ki jih določajo lokalno delovno pravo in kolektivne pogodbe ter pravo o varstvu podatkov.

ii. Organizacija v ZDA, ki sodeluje v DPF EU-ZDA in uporablja podatke o človeških virih v EU, prenesene iz EU v okviru zaposlitvenih razmerij, ter želi, da take prenose zajema DPF EU-ZDA, 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

i. Za občasne potrebe organizacije, povezane z zaposlovanjem, v zvezi z osebnimi podatki, ki se prenesejo v skladu z DPF EU-ZDA, 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 sodelujoča organizacija izpolnila načeli obvestila in možnosti izbire.

10. **Obvezne pogodbe za prenos tretjemu**

a. Pogodbe za obdelavo podatkov

i. Če se osebni podatki prenesejo iz EU v Združene države le zaradi njihove obdelave, je potrebna pogodba ne glede na to, ali izvajalec obdelave sodeluje v DPF EU-ZDA.

ii. Od upravljavcev podatkov v EU se vedno zahteva podpis pogodbe, če se podatki prenašajo le zaradi obdelave, bodisi da se obdelujejo znotraj bodisi zunaj EU, in ne glede na to, ali izvajalec obdelave sodeluje v DPF EU-ZDA. Namen pogodbe je zagotoviti, da izvajalec obdelave:

1. deluje samo po navodilih upravljavca;

2. zagotavlja ustrezne tehnične in organizacijske ukrepe za varstvo osebnih podatkov pred naključnim ali nezakonitim uničenjem ali naključno 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 na podlagi načel.

iii. Ker sodelujoče organizacije zagotavljajo ustrezno varstvo podatkov, se za pogodbe s takimi organizacijami le zaradi obdelave podatkov, ne zahteva predhodno dovoljenje.

b. Prenosi znotraj skupine odvisnih družb ali subjektov

i. Pri prenosu osebnih podatkov 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 varstvo osebnih podatkov na podlagi načel. V primeru takih prenosov je sodelujoča organizacija še naprej odgovorna za izpolnjevanje načel.

c. Prenosi med upravljavci

i. Pri prenosih med upravljavci ni potrebno, da je upravljavec, ki prejme podatke, sodelujoča organizacija ali da ima neodvisen pritožbeni mehanizem. Sodelujoča organizacija mora skleniti pogodbo s tretjim upravljavcem, ki prejme podatke, s katero zagotovi enako raven varstva, kot je na voljo v skladu z DPF EU-ZDA, pri čemer ni nujno, da je tretji upravljavec sodelujoča organizacija ali da ima neodvisen pritožbeni mehanizem, pod pogojem, da zagotavlja enakovreden mehanizem.

11. **Reševanje sporov in izvrševanje**

a. Načelo pritožbenega mehanizma, izvrševanja in odgovornosti določa zahteve za izvrševanje DPF EU-ZDA. 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) usklajenim ravnanjem s programi varstva zasebnosti zasebnega sektorja, ki v svojih pravilih vsebujejo načela in vključujejo učinkovite mehanizme uveljavljanja, kakor so opisani v načelu pritožbenega mehanizma, uveljavljanja in odgovornosti; (ii) usklajenim ravnanjem z zakonskimi ali z drugimi predpisi predvidenimi nadzornimi organi, ki zagotavljajo obravnavo posameznikovih pritožb in reševanje sporov ali (iii) zavezo sodelovanju z organi za varstvo podatkov v Evropski uniji ali 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, izvrševanja in odgovornosti dodatek k zahtevi, da mora biti samourejanje izvršljivo v skladu s členom 5 zakona o FTC (člen 45 naslova 15 zakonodajne zbirke ZDA), ki prepoveduje nepošteno in goljufivo ravnanje, členom 41712 naslova 49 zakonodajne zbirke ZDA, ki prevozniku ali agenciji za prodajo letalskih vozovnic prepoveduje nepošteno ali goljufivo ravnanje pri prodaji zračnega prevoza, ali drugim zakonom ali predpisom, ki prepoveduje takšno ravnanje.

c. Da bi pomagale zagotoviti izpolnjevanje zavez v skladu z DPF EU-ZDA in podprle upravljanje programa, morajo organizacije in njihovi neodvisni pritožbeni mehanizmi na zahtevo Ministrstva zagotoviti informacije v zvezi z DPF EU-ZDA. Poleg tega morajo organizacije hitro odgovoriti na pritožbe v zvezi z njihovim izpolnjevanjem načel, ki so jih Ministrstvu predložili organi za varstvo podatkov. Odgovor bi moral 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. Kot zahteva načelo pritožbenega mehanizma, izvrševanja in odgovornosti, mora biti pritožbeni mehanizem za posameznika zlahka dostopen in brezplačen. Neodvisni organi za reševanje sporov morajo proučiti vse pritožbe, ki jih prejmejo od posameznikov, razen kadar so očitno neutemeljene in neresne. To ne izključuje možnosti, da neodvisen organ za reševanje sporov, ki izvaja pritožbeni mehanizem, vzpostavi izločitvene pogoje, vendar morajo biti ti pogoji pregledni in upravičeni (na primer izključitev pritožb, ki ne spadajo na področje uporabe programa ali jih mora proučiti drug forum) ter ne smejo spodkopavati zavezanosti proučevanju zakonitih pritožb. Pritožbeni mehanizmi morajo poleg tega zagotoviti, da posamezniki ob vložitvi pritožbe dobijo popolne in zlahka dostopne informacije o postopkih reševanja sporov. Takšna informacija mora v skladu z načeli vsebovati obvestilo o praksah 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 spletiščih vsebovati informacije o načelih in storitvah, ki jih zagotavljajo v skladu z DPF EU-ZDA. Te informacije morajo vsebovati: (1) informacijo o zahtevah načel ali povezavo nanje za neodvisne pritožbene mehanizme; (2) povezavo na spletno mesto okvira za varstvo zasebnosti podatkov na spletišču Ministrstva; (3) pojasnilo, da so njihove storitve v zvezi z reševanjem sporov v skladu z DPF EU-ZDA za posameznike brezplačne; (4) opis načina za vložitev pritožbe, povezane z načeli; (5) časovni okvir, v katerem se obravnavajo pritožbe, povezane z načeli 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, povezanih z načeli, 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. Kot je določeno v Prilogi I, je posamezniku na voljo možnost arbitraže, kjer se pri preostalih zahtevkih ugotovi, ali je sodelujoča organizacija kršila svoje obveznosti do posameznika na podlagi načeli 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, na primer v zvezi z izjemami pri načelih ([15]) ali v zvezi z obtožbo glede ustreznosti DPF EU-ZDA. V okviru te možnosti arbitraže je „senat DPF EU-ZDA“ (ki ga sestavljajo en ali trije arbitri, kakor se dogovorita stranki) pristojen za naložitev 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 sodelujoče organizacije bodo lahko zahtevali sodni nadzor in izvršitev arbitražnih sklepov v skladu z zakonodajo ZDA, in sicer na podlagi zveznega zakona o arbitraži (*Federal Arbitration Act*).

e. Pravna sredstva in sankcije

i. Vsako pravno sredstvo, ki ga zagotovi neodvisen organ 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

([15]) Načela, pregled, člen 5.

zahtevo za izbris podatkov v nekaterih okoliščinah ([16]). Druge sankcije lahko vključujejo tudi začasni odvzem in odstranitev pečata, odškodnine za posameznike za škodo, nastalo zaradi neizpolnjevanja načel, ter sodno prepoved. Kadar sodelujoče organizacije ne upoštevajo odločb organov, morajo neodvisni organi za reševanje sporov in samoregulativni organi iz zasebnega sektorja o tem obvestiti državni organ z veljavno pristojnostjo ali sodišča in po potrebi Ministrstvo.

f. Ukrepi FTC

i. FTC se je zavezala, da bo prednostno pregledovala predložene zadeve v zvezi z domnevnim neizpolnjevanjem načel, ki jih preme od: (i) organi 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 ali ravnanja v trgovini. Če FTC ugotovi, da obstaja razlog za sum, da je bil kršen člen 5, lahko zadevo reši tako, da izda upravni odlok o prepovedi spornega ravnanja, 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 okvira o varstvu podatkov ali se nikoli niso samocertificirale pri Ministrstvu, glede spoštovanja načel DPF EU-ZDA ali sodelovanja v njem. FTC lahko uveljavi denarne kazni za kršitev upravnega odloka o prepovedi in lahko sproži civilni ali kazenski postopek za kršitev odločbe zveznega sodišča. FTC obvesti Ministrstvo o vsakem takem ukrepu. Ministrstvo spodbuja druge vladne organe, da ga obvestijo o končnem razpletu predloženih zadev in drugih odločitev v zvezi z izpolnjevanjem načel.

g. Vztrajno neizpolnjevanje načel

i. Pri vztrajnem nespoštovanju načel organizacija ni več upravičena do ugodnosti DPF EU-ZDA. Organizacije, ki vztrajno ne spoštujejo načel, bo Ministrstvo zbrisalo s seznama okvira za varstvo zasebnosti podatkov in morajo vrniti ali izbrisati osebne podatke, ki so jih prejele v skladu z DPF EU-ZDA.

ii. Vztrajno nespoštovanje načel pomeni, da organizacija, ki se je samocertificirala pri Ministrstvu, 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, vključno z Ministrstvom, ugotovi, da organizacija tako pogosto ravna proti načelom, da njena izjava o izpolnjevanju načel ni več verodostojna. V primerih, kot to ugotovi organ, ki ni Ministrstvo, mora organizacija o takih dejstvih takoj obvestiti Ministrstvo. Če tega ne stori, se lahko kaznuje po zakonu o lažnih navedbah (člen 1001 naslova 18 zakonodajne zbirke ZDA). Izstop organizacije iz programa s samourejevalnim sistemom za varstvo zasebnosti v zasebnem sektorju ali neodvisnega mehanizma za reševanje sporov le-te ne razbremeni obveznosti do spoštovanja načel in bi pomenil vztrajno nespoštovanje načel.

iii. Ministrstvo bo s svojega seznama okvira za varstvo zasebnosti podatkov odstranilo organizacijo na podlagi vsakega uradnega obvestila o vztrajnem neizpolnjevanju načel, ki ga prejme od same organizacije, samoregulativnega organa za varstvo zasebnosti ali od vladnega organa, vendar šele po izteku 30-dnevnega roka, v katerem ima organizacija, ki ni ravnala v skladu z načeli, možnost odziva ([17]). Seznam okvira za varstvo zasebnosti podatkov, ki ga vodi Ministrstvo, bo torej jasno pokazal, katerim organizacijam so zagotovljene in katerim organizacijam niso več zagotovljene ugodnosti DPF EU-ZDA.

iv. Organizacija, ki se vloži vlogo za sodelovanje v samoregulativnem organu z namenom, da izpolni pogoje za ponovno sodelovanje v DPF EU-ZDA, mora navedeni organizaciji predložiti vse podatke o svojem prejšnjem sodelovanju v DPF EU-ZDA.

([16]) Neodvisni organi za reševanje sporov po svoji presoji odločijo, v katerih okoliščinah bodo uporabili 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.

([17]) Ministrstvo bo v obvestilu navedlo čas, ki bo nujno krajši od 30 dni, v katerem mora organizacija odgovoriti na obvestilo.

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 določi organizacija in so potrebni za učinkovito upoštevanje zavrnitve. Organizacija lahko od posameznika, ki se je odločil za „zavrnitev“, tudi zahteva, da z zadostnimi podatki potrdi svojo istovetnost. V Združenih državah lahko posamezniki uresničijo to možnost prek osrednjega programa „zavrnitve“. 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, sama pa 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. V skladu s Splošno uredbo o varstvu podatkov se lahko osebni podatki, če ni sklepa o ustreznosti, prenesejo v tretjo državo, če so zagotovljeni ustrezni zaščitni ukrepi za varstvo podatkov v skladu s členom 46 splošne uredbe o varstvu podatkov ali, v posebnih primerih, če je izpolnjen eden od pogojev iz člena 46 splošne uredbe o varstvu podatkov (npr. če je posameznik, na katerega se nanašajo osebni podatki, izrecno privolil v prenos). Organizacije v ZDA, podpisnice DPF EU-ZDA, zagotavljajo ustrezno varstvo osebnih podatkov in zato lahko prejmejo podatke, prenesene iz EU na podlagi člena 45 splošne uredbe o varstvu podatkov, ne da bi morale uvesti instrument za prenos v skladu s členom 46 Splošne uredbe o varstvu podatkov ali izpolnjevati pogoje iz člena 46 navedene uredbe. Ker DPF EU-ZDA vključuje posebna pravila za občutljive informacije, se takšne informacije (ki jih je treba zbrati na primer v zvezi z potrošnikovo potrebo po fizični pomoči) lahko prenesejo sodelujočim organizacijam. V vsakem primeru pa mora organizacija, ki prenaša podatke, spoštovati pravo države članice EU, v kateri deluje, ki lahko med drugim nalaga posebne pogoje za ravnanje z občutljivimi informacijami.

14. **Farmacevtski in medicinski izdelki**

a. Uporaba zakonov držav članic EU ali načel

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

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 v ZDA v DPF EU-ZDA, 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 redno 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

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

d. Prenosi za regulativne in nadzorne namene

i. 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

i. Podjetju za farmacevtske ali medicinske pripomočke ni treba uporabiti načel 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 organom, kot je agencija za hrano in zdravila (*Food and Drug Administration*).

g. Podatki, kodirani s šifrirnim ključem

i. 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 (npr. 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.

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

a. Organizacija mora pri osebnih podatkih iz javno dostopnih virov uporabljati načeli varnosti, celovitosti podatkov in omejitve namena ter pritožbenega mehanizma, izvrševanja in odgovornosti. Ta načela veljajo tudi za osebne podatke, zbrane iz javnih evidenc (tj. tiste evidence, ki jih hranijo vladni organi ali subjekti na kateri koli ravni in so na voljo za vpogled širše javnosti).

b. Za informacije iz javnih evidenc ni treba uporabiti načel obvestila, izbire ali odgovornosti za prenos tretjemu, če niso povezane z informacijami iz evidenc, ki niso javne, in se spoštujejo vsi pogoji glede vpogleda, ki jih je določil ustrezni pristojni organ. Prav tako na splošno ni treba uporabiti načel obvestila, izbire ali odgovornosti za prenos tretjemu za javnosti dostopne podatke, 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.

c. 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 DPF EU-ZDA.

d. Dokler informacije iz javnih evidenc niso povezane z drugimi osebnimi podatki, ni treba uporabiti načela dostopa (razen za manjše količine, ki se uporabljajo za indeksiranje in organiziranje informacij javnih evidenc); vendar je treba spoštovati vse pogoje, ki jih za vpogled določa ustrezna jurisdikcija. Kadar pa je informacija iz javnih evidenc povezana z drugimi informacijami iz evidenc, ki niso javne, (razen tistih, ki so podrobno navedene zgoraj), mora organizacija zagotoviti dostop do vseh takih informacij, če zanje ne veljajo druge dovoljene izjeme.

e. Kot pri informacijah 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. Za zagotovitev preglednosti v zvezi z zakonitimi zahtevami javnih organov za dostop do osebnih podatkov, lahko sodelujoče organizacije prostovoljno izdajo redna poročila o številu zahtev za osebne podatke, ki jih prejmejo od javnih organov za namene kazenskega pregona ali nacionalne varnosti, če so takšna razkritja dovoljena po veljavni zakonodaji.

b. Podatki, ki jih v teh poročilih zagotovijo sodelujoče organizacije, in podatki, ki jih objavi obveščevalna skupnost, in druge informacije je mogoče uporabiti kot podlago za letni skupni pregled delovanja PDF EU-ZDA v skladu z načeli.

c. Če ni obvestila v skladu s točko (a)(xii) načela obvestila, to ne preprečuje ali zmanjšuje zmožnosti organizacije, da se odzove na morebitno zakonito zahtevo.

PRILOGA I: ARBITRAŽNI MODEL

Priloga I določa pogoje, pod katerimi so organizacije, ki sodelujejo v DPF EU-ZDA 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 zajema DPF EU-ZDA. Namen te možnosti je zagotoviti takojšen neodvisen in pošten mehanizem na izbiro posameznikov za reševanje vseh zatrjevanih kršitev načel, ki niso bile razrešene v okviru katerega koli drugega mehanizma DPF EU-ZDA.

A. **Področje uporabe**

Možnost arbitraže je posamezniku na voljo, da pri preostalih zahtevkih ugotovi, ali je sodelujoča organizacija 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 na primer v zvezi z izjemami od načel ([1]) ali v zvezi z obtožbo glede ustreznosti DPF EU-ZDA.

B. **Razpoložljiva pravna sredstva**

V okviru te možnosti arbitraže je „senat okvira za varstvo zasebnosti podatkov med EU in ZDA“ (arbitražni senat, 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 senata okvira za varstvo zasebnosti podatkov med EU in ZDA v zvezi s pravnimi sredstvi. Ob upoštevanju pravnih sredstev je senat okvira za varstvo zasebnosti podatkov med EU in ZDA dolžan upoštevati druga pravna sredstva, ki so jih odredili že drugi mehanizmi v skladu DPF EU-ZDA. 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 (d)(i) dopolnilnega načela o reševanju sporov in izvrševanju; (2) uporabiti neodvisen pritožbeni mehanizem v okviru načel, brezplačen za posameznika in (3) predložiti zadevo prek posameznikovega organa za varstvo podatkov Ministrstvu 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) 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 za varstvo podatkov (1) pristojnost po dopolnilnem načelu o vlogi organov za varstvo podatkov ali dopolnilnem načelu o podatkih o človeških virih, ali (2) pristojnost za reševanje zatrjevane kršitve neposredno z organizacijo. Pooblastilo organa za varstvo 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 zavezuje pooblastilo organa za varstvo podatkov.

D. **Zavezujoča narava sklepov**

Posameznikova odločitev, da uveljavi to možnost zavezujoče arbitraže, je v celoti prostovoljna. Arbitražne odločbe 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, če nedenarno pravično nadomestilo za zatrjevano kršitev te ne odpravi v celoti, posameznikova uveljavitev arbitraže ne onemogoči zahtevka za odškodnino, ki je sicer na voljo na sodiščih.

([1]) Načela, Pregled, člen 5.

E. **Pregled in izvrševanje**

Posamezniki in sodelujoče organizacije bodo lahko zahtevali sodni nadzor in izvršitev arbitražnih odločb v skladu s pravom ZDA na podlagi zveznega zakona o arbitraži (*Federal Arbitration Act*, v nadaljnjem besedilu: FAA) ([2]). Vse take zadeve je treba vložiti pri zveznem okrožnem sodišču, ki je krajevno pristojno za primarni kraj poslovanja sodelujoče organizacije.

Ta možnost arbitraže je namenjena reševanju posameznih sporov, namen arbitražnih odločb pa ni, da so uporabljene kot prepričljiva ali zavezujoča dosedanja praksa v zadevah, ki vključujejo druge stranke, tudi v prihodnjih arbitražah ali na sodiščih v EU ali ZDA ali v postopkih Zvezne komisije za trgovino (*Federal Trade Commissio*n, v nadaljnjem besedilu: FTC).

F. **Arbitražni senat**

Stranke bodo za senat okvira za varstvo zasebnosti podatkov med EU in ZDA izbrale arbitre s seznama arbitrov, obravnavanega spodaj.

Skladno z veljavno zakonodajo bosta Ministrstvo in Komisija oblikovala seznam vsaj deset arbitrov, izbranih na podlagi neodvisnosti, integritete in strokovnosti. V zvezi s tem postopkom velja naslednje:

Arbitri:

(1) bodo ostali na seznamu tri leta, razen v izjemnih okoliščinah ali v primeru razrešitve iz pomembnega razloga, njihovo imenovanje pa lahko Ministrstvo s predhodno priglasitvijo Komisiji podaljša za dodatna triletna obdobja;

(2) ne sprejemajo navodil in niso povezani s katero koli stranko ali sodelujočo organizacijo 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 Združenih državah in strokovnjaki za pravo ZDA na področju varstva zasebnosti ter imeti strokovno znanje iz prava EU na področju varstva podatkov.

([2]) Poglavje 2 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], spada 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 „[se] [š]teje […], da arbitražni sporazum ali arbitražna odločba na podlagi takšnega razmerja, ki je v celoti med državljani Združenih držav, ne spada v okvir [newyorške] konvencije, razen če to razmerje vključuje premoženje v tujini, predvideva uspeh 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 pri katerem koli sodišču, ki je pristojno po tem poglavju, vloži predlog za izdajo sklepa, ki potrjuje arbitražno odločbo proti kateri koli drugi stranki v arbitraži. Sodišče potrdi arbitražno odločbo, razen če ugotovi obstoj enega od razlogov za zavrnitev ali odložitev priznanja ali izvrševanja arbitražne odločbe, navedene v omenjeni [newyorški] konvenciji." Id. člen 207. Poglavje 2 nadalje določa, da „[imajo] [o]krožna sodišča Združenih držav […] izvirno pristojnost za […] tožbo ali postopek [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 navedeno 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 spor, ki izhaja iz takšne pogodbe ali posla ali iz zavrnitve izvedbe celotne pogodbe ali celotnega posla ali katerega koli njunega dela, reši z arbitražo 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 izdajo sklepa, ki potrjuje arbitražno odločbo, na podlagi tega pa mora sodišče ugoditi izdaji takšnega sklepa, razen če je arbitražna odločba razveljavljena, spremenjena ali popravljena, kakor je predpisano v členih 10 in 11 [FAA]." Id. člen 9.

G. **Arbitražni postopki**

Skladno z veljavno zakonodajo sta se Ministrstvo in Komisija dogovorila o sprejetju arbitražnih pravil, ki urejajo postopke pred senatom okvira za varstvo zasebnosti podatkov med EU in ZDA ([3]). Če bo treba pravila, ki urejajo postopke, spremeniti, se bosta Ministrstvo in Komisija dogovorila o spremembi navedenih pravil ali sprejetju drugačnega sklopa obstoječih, uveljavljenih ameriških arbitražnih postopkov, kakor je ustrezno, v skladu z vsakim od naslednjih preudarkov:

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 gradiva in/ali pravno razpravo v zvezi z domnevnim zahtevkom.

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

3. Ukrep FTC 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 varstvo podatkov zagotovijo pomoč samo pri pripravi obvestila, ne smejo pa imeti dostopa do odkritja 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, ali posameznika zastopa odvetnik, se tolmačenje na arbitražni obravnavi kot tudi prevod arbitražnega gradiva posamezniku zagotovi brezplačno, razen če senat okvira za varstvo zasebnosti podatkov EU-ZDA ugotovi, da bi to glede na okoliščine posamezne arbitraže povzročilo neupravičene ali nesorazmerne stroške.

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

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

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

([3]) Mednarodno središče za reševanje sporov (*International Centre for Dispute Resolution*, v nadaljnjem besedilu: ICDR), mednarodni oddelek ameriškega združenja za arbitražo (*American Arbitration Association*, v nadaljnjem besedilu: AAA) (v nadaljnjem besedilu skupaj: ICDR-AAA) je izbralo Ministrstvo za upravljanje arbitraž v skladu s Prilogo I k načelom in arbitražnega sklada, opredeljenega v njej. Ministrstvo in Komisija sta se 15. septembra 2017 dogovorila o sprejetju sklopa arbitražnih pravil za urejanje zavezujočih arbitražnih postopkov, opisanih v Prilogi I k načelom, in tudi kodeksu ravnanja za arbitre, ki je skladen s splošno sprejetimi etičnimi standardi za trgovinske arbitre in Prilogo I k načelom. Ministrstvo in Komisija sta se dogovorila o prilagoditvi arbitražnih pravil in kodeksa ravnanja, tako da izražata posodobitve DPF EU-ZDA, Ministrstvo pa bo sodelovalo z ICDR-AAA pri pripravi navedenih posodobitev.

H. **Stroški**

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

Skladno z veljavno zakonodajo bo Ministrstvo omogočilo oblikovanje sklada, v katerega bodo morale prispevati sodelujoče organizacije, deloma glede na velikost organizacije, ki bo kril strošek arbitraže, vključno s honorarji arbitrov, do najvišjih zneskov („najvišje vrednosti“). Sklad bo upravljala tretja stranka, ki bo Ministrstvu redno poročala o delovanju sklada. Ministrstvo bo sodelovalo s tretjo stranko pri rednem pregledu delovanja sklada, vključno s potrebo po prilagoditvi zneska prispevkov ali najvišjih vrednosti stroška arbitraže, in med drugim upošteval število arbitraž ter stroške in časovni potek arbitraž ob sporazumu, da sodelujočim organizacijam ne bo naloženo čezmerno finančno breme. Ministrstvo bo Komisijo obvestilo o izidu takih pregledov s tretjo stranko in ji predhodno priglasilo morebitne prilagoditve zneska prispevkov. Ta določba ne krije stroškov odvetnikov ali morebitnih skladov.

PRILOGA II

UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

6. julij 2023

Spoštovani komisar Didier Reynders
Komisar za pravosodje
Evropska komisija
Rue de la Loi/ Wetstraat 200
1049 Bruselj
Belgija

Spoštovani komisar Reynders,

veseli me, da vam lahko v imenu Združenih držav pošljem sveženj gradiva v zvezi z okvirom za varstvo zasebnosti podatkov med EU in ZDA, ki skupaj z Odredbo št. 14086 „Krepitev zaščitnih ukrepov za obveščevalne dejavnosti SIGINT v ZDA“ in poglavjem 28, del 201, Zakonika Združenih držav (*U.S. Code of Federal Regulations*, v nadaljnjem besedilu: CFR) o spremembi predpisov Ministrstva za pravosodje ZDA (*Department of Justice*) za ustanovitev „sodišča za presojo varstva podatkov“ izraža pomembna in podrobna pogajanja za krepitev varstva zasebnosti in državljanskih svoboščin. Rezultat teh pogajanj so novi zaščitni ukrepi za zagotovitev, da so obveščevalne dejavnosti SIGINT ZDA potrebne in sorazmerne pri uresničevanju opredeljenih ciljev nacionalne varnosti , ter novi mehanizem za posameznike iz Evropske unije (EU) za uveljavljanje pravnih sredstev, če menijo, da so nezakonit cilj SIGINT, ki bodo skupaj zagotovili varstvo osebnih podatkov iz EU. Okvir za varstvo zasebnosti podatkov med EU in ZDA bo temelj vključujočega in konkurenčnega digitalnega gospodarstva. Ponosna sva lahko na izboljšave v navedenem okviru, ki bodo okrepile varstvo zasebnosti po vsem svetu. Ta sveženj, Odredba, predpisi in drugo gradivo, ki so na voljo iz javnih virov, zagotavljata trdno podlago za novo ugotovitev Evropske komisije o ustreznosti ([1]).

Priloženo je naslednje gradivo:

— Načela okvira za varstvo zasebnosti podatkov med EU in ZDA, vključno z dopolnilnimi načeli (v nadaljnjem besedilu skupaj: načela), in Priloga I k načelom (tj. priloga s pogoji, pod katerimi morajo organizacije v okviru o varstvu podatkov izpolniti nekatere preostale zahtevke glede osebnih podatkov, ki jih zajemajo načela);

— pismo Uprave za mednarodno trgovino Ministrstva za trgovino, pristojne za program okvira za varstvo zasebnosti podatkov, v katerem so opisane zaveze našega ministrstva glede zagotavljanja učinkovitega delovanja okvira za varstvo zasebnosti podatkov med EU in ZDA;

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

— pismo Ministrstva za promet, ki opisuje njegovo izvrševanje načel;

— pismo urada direktorja nacionalne obveščevalne službe (*Office of the Director of National Intelligence*) v zvezi z zaščitnimi ukrepi in omejitvami, ki veljajo za ameriške nacionalne varnostne organe 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.

([1]) Če se bo sklep Komisije o ustreznosti varstva, ki ga zagotavlja okvir za varstvo zasebnosti podatkov med EU in ZDA, uporabljal za Islandijo, Lihtenštajn in Norveško, bo sveženj o okviru o varstvu podatkov med EU in ZDA zajemal Evropsko unijo in tudi te tri države.

Celoten sveženj okvira za varstvo zasebnosti podatkov med EU in ZDA bo objavljen na spletnem mestu okvira za varstvo zasebnosti podatkov na spletišču Ministrstva, načela in Priloga I k načelom pa bodo začeli veljati na datum začetka veljavnosti sklepa Evropske komisije o ustreznosti.

Zagotavljam vam, da Združene države te zaveze jemljejo resno. Veselimo se sodelovanja z vami pri uvajanju okvira za varstvo zasebnosti podatkov EU-ZDA in pri skupnem delu v naslednji fazi tega procesa.

S spoštovanjem,

Gina M. RAIMONDO

PRILOGA III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12. december 2022

Spoštovani komisar Didier Reynders
Komisar za pravosodje
Evropska komisija
Rue de la Loi/Wetstraat 200
1049 Bruselj
Belgija

Spoštovani komisar Reynders,

veseli me, da lahko v imenu Uprave za mednarodno trgovino (ITA) opišem zaveze, ki jih je Ministrstvo za trgovino ZDA (*Department of Commerce*, v nadaljnjem besedilu: Ministrstvo) sprejelo za zagotavljanje učinkovitega varstva osebnih podatkov s svojim upravljanjem in nadzorom programa okvira za varstvo zasebnosti podatkov. Dokončanje okvira za varstvo zasebnosti podatkov med EU in ZDA (v nadaljnjem besedilu: DPF EU-ZDA) je velik dosežek za zasebnost in podjetja na obeh straneh Atlantika, saj posameznikom v EU omogoča zaupanje, da bodo njihovi podatki varovani in da bodo imeli na voljo pravna sredstva za obravnavo pomislekov v zvezi z njihovimi podatki, na tisoče podjetjem pa bo omogočil nadaljnje naložbe v trgovino in poslovanje ter siceršnje sodelovanje na teh področjih prek Atlantika v korist naših gospodarstev in državljanov. DPF EU-ZDA je plod dolgoletnega trdega dela in sodelovanja z vami in našimi kolegi iz Evropske komisije (v nadaljnjem besedilu: Komisija). Veselimo se nadaljnjega sodelovanja s Komisijo, s katerim bomo zagotovili učinkovitost skupnih prizadevanj.

DPF EU-ZDA bo prinesel pomembne ugodnosti posameznikom in podjetjem. Prvič, zagotavlja pomemben sklop varstva podatkov posameznikov iz EU, ki se prenašajo v Združene države. Od sodelujočih ameriških organizacij zahteva, da oblikujejo skladno politiko zasebnosti; se javno zavežejo upoštevanju „načel okvira za varstvo zasebnosti podatkov med EU in ZDA“, vključno z dopolnilnimi načeli (v nadaljnjem besedilu skupaj: načela), in Priloge I k tem načelom (tj. priloga s pogoji, pod katerimi morajo organizacije v DPF EU-ZDA izpolniti nekatere preostale zahtevke glede osebnih podatkov, ki jih zajemajo načela), tako da postane zaveza izvršljiva na podlagi prava ZDA ([1]); vsako leto ponovno certificirajo svoje izpolnjevanje načel pri Ministrstvu; posameznikom iz EU zagotovijo brezplačno neodvisno reševanje sporov in da so pod preiskovalno in izvršilno pristojnostjo zakonsko določenega organa ZDA, navedenega v načelih (tj. Zvezne komisije za trgovino ZDA (*Federal Trade Commission*, v nadaljnjem besedilu: FTC)) in Ministrstva za promet ZDA (*Department of Transportation*, v nadaljnjem besedilu: ministrstvo za promet), ali zakonsko določenega organa, navedenega v prihodnji prilogi k načelom. Čeprav je odločitev organizacije za samocertificiranje prostovoljna, pa je, potem ko se organizacija javno zaveže DPF EU-ZDA, njena zaveza izvršljiva na podlagi prava ZDA s strani FTC, ministrstva za promet ali drugega zakonsko določenega organa ZDA, odvisno od tega, kateri organ je pristojen za sodelujočo organizacijo. Drugič, DPF EU-ZDA bo podjetjem v Združenih državah, vključno s podružnicami evropskih podjetij v Združenih državah omogočil, da prejmejo osebne podatke iz Evropske unije in tako pospešijo pretok podatkov v podporo čezatlantski trgovini. Pretok

([1]) Organizacije, ki so samocertificirale svojo zavezo izpolnjevanju načel okvira zasebnostnega ščita EU-ZDA in želijo uživati ugodnosti sodelovanja v DPF EU-ZDA, morajo izpolnjevati „načela okvira za varstvo zasebnosti podatkov med EU in ZDA“. To zavezo izpolnjevanju „načel okvira za varstvo zasebnosti podatkov med EU in ZDA“ izražajo politike zasebnosti takih sodelujočih organizacij čim prej, v vsakem primeru pa najpozneje tri mesece po datumu začetka veljavnosti „načel okvira za varstvo zasebnosti podatkov med EU in ZDA“ (Glej člen (e) dopolnilnega načela o samocertificiranju).

podatkov med Združenimi državami in Evropsko unijo je najobsežnejši na svetu, na njem pa temeljijo gospodarski odnosi v vrednosti 7,1 bilijona USD, 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 največja podjetja s seznama Fortune 500 ter tudi mala in srednja podjetja. Čezatlantski pretok podatkov ameriškim organizacijam omogoča, da obdelajo podatke, potrebne za zagotavljanje blaga, storitev in zaposlitvenih možnosti posameznikom iz Evrope.

Ministrstvo je zavezano tesnemu in plodnemu sodelovanju z našimi sorodnimi organi v EU pri učinkovitem upravljanju in nadzoru programa okvira za varstvo zasebnosti podatkov. Ta zaveza je izražena v oblikovanju in stalnem izpopolnjevanju najrazličnejših virov Ministrstva za pomoč organizacijam pri postopku samocertificiranja, vzpostavitvi spletišča za zagotavljanje ciljno usmerjenih informacij deležnikom, sodelovanju s Komisijo in evropskimi organi za varstvo podatkov pri razvoju smernic, ki pojasnjujejo pomembne elemente DPF EU-ZDA, ozaveščanju za omogočanje čedalje večjega razumevanja obveznosti organizacij glede varstva podatkov ter nadzoru in spremljanju njihovega izpolnjevanja programskih zahtev.

Naše stalno sodelovanje s cenjenimi sorodnimi organi v EU bo Ministrstvu omogočilo, da zagotovi učinkovito delovanje DPF EU-ZDA. Vlada Združenih držav ima dolgo zgodovino sodelovanja s Komisijo pri spodbujanju skupnih načel varstva podatkov, premagovanja razlik v naših zadevnih pravnih pristopih, hkrati pa spodbuja trgovino in gospodarsko rast Evropske unije in Združenih držav. Prepričani smo, da bo DPF EU-ZDA, ki je primer takega sodelovanja, Komisiji omogočil izdajo novega sklepa o ustreznosti, s katerim bo organizacijam dovoljena uporaba DPF EU-ZDA za prenos osebnih podatkov iz Evropske unije v Združene države v skladu s pravom Unije.

Upravljanje in nadzor programa okvira za varstvo zasebnosti podatkov s strani Ministrstva za trgovino ZDA

Ministrstvo je trdno zavezano učinkovitemu upravljanju in nadzoru programa okvira za varstvo zasebnosti podatkov ter si bo ustrezno prizadevalo za zagotovitev navedenega izida, čemur bo tudi namenilo ustrezna sredstva. Ministrstvo bo vodilo verodostojen seznam organizacij iz ZDA, ki so se samocertificirale pri Ministrstvu in se zavezale spoštovanju načel (v nadaljnjem besedilu: seznam okvira za varstvo zasebnosti podatkov), ki ga bo posodabljalo na podlagi letnih vlog za samocertificiranje, ki jih vložijo sodelujoče organizacije, in z odstranitvijo organizacij, ki prostovoljno izstopijo, ne opravijo letnega ponovnega certificiranja v skladu s postopki Ministrstva, ali pri katerih ugotovi, da vztrajno ne spoštujejo načel, ter javnosti omogočilo dostop do njega. Vodilo bo tudi verodostojno evidenco organizacij iz ZDA, ki so bile odstranjene s seznama okvira za varstvo zasebnosti podatkov, in javnosti omogočalo dostop do nje, pri čemer bo navedlo razloge za odstranitev vsake posamezne organizacije. Zgoraj navedena verodostojna seznam in evidenca bosta javnosti na voljo na spletnem mestu okvira za varstvo zasebnosti podatkov na spletišču Ministrstva. Na tem spletnem mestu okvira za varstvo zasebnosti podatkov bo vidno objavljeno pojasnilo, da mora vsaka organizacija, odstranjena s seznama okvira za varstvo zasebnosti podatkov prenehati navajati, da sodeluje v DPF EU-ZDA ali ga izpolnjuje ter da lahko prejema osebne informacije v skladu z DPF EU-ZDA. Taka organizacija pa mora kljub temu še naprej uporabljati načela za osebne informacije, ki jih je prejela med sodelovanjem DPF EU-ZDA, dokler hrani take informacije. Ministrstvo se v podporo svoji krovni, stalni zavezanosti učinkovitemu upravljanju in nadzoru programa okvira za varstvo zasebnosti podatkov zlasti zavezuje, da bo:

Preverilo zahteve za samocertificiranje

— Ministrstvo bo pred dokončanjem začetnega samocertificiranja ali vsakoletnega ponovnega certificiranja (v nadaljnjem besedilu skupaj: samocertificiranje) in uvrstitvijo organizacije na seznam okvira za varstvo zasebnosti podatkov ali njeno ohranitvijo na njem preverilo, ali je organizacija izpolnila vsaj ustrezne zahteve, ki so določene v dopolnilnem načelu o samocertificiranju in se nanašajo na informacije, ki jih mora organizacija navesti v svoji vlogi za samocertificiranje, vloženi pri Ministrstvu, in ali je pravočasno zagotovila ustrezno politiko zasebnosti, v kateri posameznike seznanja z vsemi 13 izrecno navedenimi elementi, določenimi v načelu obvestila. Ministrstvo bo preverilo, ali je organizacija:

— opredelila organizacijo, ki vlaga vlogo za samocertificiranje, in tudi morebitne subjekte v ZDA ali podružnice organizacije, ki se samocertificira, v ZDA, ki prav tako spoštujejo načela, ki jih organizacija želi zajeti v svojem samocertificiranju;

— zagotovila potrebne podatke za stik z organizacijo (tj. kontaktne podatke določenega/-ih posameznika/-ov in/ali služb/-e znotraj organizacije, ki se samocertificira, odgovorne/-ih za obravnavanje pritožb, dostop do zahtevkov in morebitna druga vprašanja, ki izhajajo iz DPF EU-ZDA);

— opisala namen/-i, za katere/-ga bi organizacija zbirala in uporabljala osebne podatke, prejete iz Evropske unije;

— navedla, kakšne osebne podatke bi prejemala iz Evropske unije na podlagi DPF EU-ZDA in bi bile zato zajete v njeni vlogi za samocertificiranje;

— če ima organizacija javno spletno stran, zagotovila spletni naslov, kjer je na voljo ustrezna politika zasebnosti, in razpoložljivost slednje na navedeni spletni strani ali, če organizacija nima javne spletne strani, predložila Ministrstvu izvod ustrezne politike zasebnosti in navedla, kje je zadevnim posameznikom na voljo politika zasebnosti (tj. zadevnim zaposlenim, če gre pri ustrezni politiki zasebnosti za politiko zasebnosti človeških virov ali javnosti, če pri ustrezni politiki zasebnosti ne gre za politiko zasebnosti človeških virov);

— v svojo ustrezno politiko zasebnosti v ustreznem roku (tj. na začetku le v osnutek politike zasebnosti, skupaj z vlogo, če je navedena vloga za začetno samocertificiranje, sicer pa v končno in, če je ustrezno, objavljeno politiko zasebnosti) vključila izjavo, da se zavezuje k spoštovanju načel, in hiperpovezavo na ali spletno mesto okvira za varstvo zasebnosti podatkov na spletišču Ministrstva (npr. domača stran ali spletno mesto seznama okvira za varstvo zasebnosti podatkov);

— v svojo ustrezno politiko zasebnosti v ustreznem roku vključila vseh 12 drugih izrecno navedenih elementov, določenih v načelu obvestila (tj. možnost, da zadevni posameznik iz EU pod določenimi pogoji uveljavlja zavezujočo arbitražo; zahtevo po razkritju osebnih informacij na podlagi zakonitih zahtev javnih organov, tudi z namenom izpolnjevanja zahtev nacionalne varnosti ali kazenskega pregona in svojo odgovornost v primerih prenosa tretjemu);

— 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 varstvo zasebnosti (in ki je navedeno v načelih ali v prihodnji prilogi k načelom);

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

— opredelila, ali je ustrezna metoda (tj. postopke, ki jih mora zagotoviti) preverjanja njenega izpolnjevanja načel samoocenjevanje (tj. notranje preverjanje) ali „zunanji pregled skladnosti“ (tj. preverjanje s strani tretjih strank), in ali če je kot ustrezno metodo opredelila zunanji pregled skladnosti, tudi navedla tretjo stranko, ki je opravila navedeni pregled;

— opredelila ustrezni neodvisni pritožbeni mehanizem, ki je na voljo za obravnavanje pritožb, vloženih na podlagi načel, in zadevnemu posamezniku brezplačno zagotovila ustrezna pravna sredstva.

— Če je organizacija izbrala neodvisen pritožbeni mehanizem, ki ga zagotavlja organ za alternativno reševanje sporov v zasebnem sektorju, je v svojo ustrezno politiko zasebnosti vključila hiperpovezavo na ali spletno mesto ustreznega spletišča mehanizma ali njegovega obrazca za predložitev pritožbe, ki je na voljo za preiskave nerešenih pritožb, vloženih na podlagi načel.

— Če se od organizacije bodisi zahteva (tj. v zvezi s podatki o človeških virih, ki se prenašajo iz Evropske unije v okviru zaposlitvenega razmerja) bodisi se je sama odločila, da pri preiskavi in reševanju pritožb, vloženih na podlagi načel, sodeluje oziroma bo sodelovala z ustreznimi organi za varstvo podatkov, se je zavezala takemu sodelovanju z organi za varstvo podatkov in upoštevanju njihovega povezanega nasveta, da bo sprejela posebne ukrepe za spoštovanje načel.

— Ministrstvo bo prav tako preverilo, ali je vloga organizacije za samocertificiranje skladna z njeno/-imi zadevno/-imi politiko/-ami zasebnosti. Če želi organizacija, ki se samocertificira, vključiti katerega koli svojih subjektov ali podružnic v ZDA, ki imajo ločene ustrezne politike zasebnosti, bo Ministrstvo pregledalo tudi ustrezne politike zasebnosti takih vključenih subjektov ali podružnic, da bi zagotovilo, da vključujejo vse zahtevane elemente, določene v načelu obvestila.

— Ministrstvo bo sodelovalo z zakonsko določenimi organi (npr. FTC ali ministrstvo za promet), da bi preverilo, ali je za organizacije pristojen ustrezen zakonsko določen organ, naveden v njihovih vlogah za samocertificiranje, če Ministrstvo upravičeno dvomi o taki pristojnosti.

— Ministrstvo bo sodelovalo z organi za alternativno reševanje sporov v zasebnem sektorju, da bi preverilo, ali so organizacije aktivno registrirane pri neodvisnem pritožbenem mehanizmu, navedenem v njihovih vlogah za samocertificiranje, in sodelovalo z navedenimi organi, da bi preverilo, ali so organizacije aktivno registrirane za zunanji pregled skladnosti, naveden v njihovih vlogah za samocertificiranje, kadar lahko navedeni organi zagotavljajo obe vrsti storitev.

— Ministrstvo bo sodelovalo s tretjo stranko po svoji izbiri, ki bo v vlogi skrbnika sredstev, zbranih s pristojbino foruma organov za varstvo podatkov (tj. letne pristojbine za pokrivanje stroškov delovanja foruma organov za varstvo podatkov), da bi preverilo, ali so organizacije plačale navedeno pristojbino za ustrezno leto, če so organizacije navedle organe za varstvo podatkov kot neodvisen pritožbeni mehanizem.

— Ministrstvo bo sodelovalo s tretjo stranko po svoji izbiri pri upravljanju arbitraž v skladu s Prilogo I k načelom in arbitražnega sklada, opredeljenega v njej, da bi preverilo, ali so organizacije plačale prispevek v arbitražni sklad.

— Če Ministrstvo med svojim pregledom vlog organizacij za samocertificiranje odkrije kakršne koli težave, jih bo obvestilo, da morajo odpraviti vse take težave v ustreznem roku, ki ga določi Ministrstvo ([2]). Ministrstvo jih bo tudi obvestilo, da če se ne bodo odzvale v rokih, ki jih določi Ministrstvo, ali če ne bodo opravile svojega samocertificiranja v skladu s postopki Ministrstva, se bo štelo, da so odstopile od navedenih vlog za samocertificiranje, in da je lahko vsako zavajanje o sodelovanju organizacije v DPF EU-ZDA ali v skladu z njim predmet izvršilnih ukrepov FTC, ministrstva za promet ali drugega ustreznega vladnega organa. Ministrstvo bo o tem organizacije obvestilo prek osebe za stike, ki jo je organizacija navedla Ministrstvu.

Olajšalo sodelovanje z organi za alternativno reševanje sporov, ki zagotavljajo storitve, povezane z načeli

— Ministrstvo bo sodelovalo z neodvisnimi organi za alternativno reševanje sporov v zasebnem sektorju, ki zagotavljajo neodvisne pritožbene mehanizme, ki so na voljo za preiskave nerešenih pritožb, vloženih na podlagi načel, da bi preverilo, ali izpolnjujejo vsaj zahteve, določene v dopolnilnem načelu o reševanju sporov in izvrševanju. Ministrstvo bo preverilo, ali:

  — na svojih javnih spletiščih vključujejo informacije v zvezi z načeli in storitvami, ki jih zagotavljajo v skladu z DPF EU-ZDA, ki morajo vključevati: (1) informacije o zahtevah načel za neodvisne pritožbene mehanizme ali povezavo nanje; (2) hiperpovezavo na spletno mesto okvira za varstvo zasebnosti podatkov na spletišču Ministrstva; (3) pojasnilo, da so njihove storitve v zvezi z reševanjem sporov v skladu z DPF EU-ZDA za posameznike brezplačne; (4) opis načina za vložitev pritožbe, povezane z načeli; (5) časovni okvir, v katerem se obravnavajo pritožbe, povezane z načeli in (6) opis možnih pravnih sredstev. Ministrstvo bo organe pravočasno obvestilo o bistvenih spremembah svojega nadzora in upravljanja programa okvira za varstvo zasebnosti podatkov, če so take spremembe neizbežne ali so se že zgodile in so pomembne za vlogo organov v skladu z DPF EU-ZDA;

([2]) Npr. kar zadeva ponovno certificiranje, bi se pričakovalo, da organizacije vse take težave obravnavajo v 45 dneh; Ministrstvo pa lahko določi drugačen ustrezen časovni okvir.

— objavljajo letno poročilo s skupnimi statističnimi podatki v zvezi s svojimi storitvami reševanja sporov, ki mora vključevati: (1) skupno število pritožb, povezanih z načeli, 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. Ministrstvo bo organom zagotovilo posebne, dopolnilne smernice o tem, katere informacije naj zagotovijo v navedenih letnih poročilih, o obravnavi navedenih zahtev (npr. navedba posebnih meril, ki jih mora pritožba izpolnjevati, da se šteje za pritožbo na podlagi načel za namene letnega poročila) in tudi o drugih vrstah informacij, ki bi jih morali organi zagotoviti (npr. če organ zagotavlja tudi storitev preverjanja v zvezi z izpolnjevanjem načel, opis načina, kako organ preprečuje morebitna dejanska ali potencialna navzkrižja interesov v primerih, kadar organizaciji zagotavlja storitve preverjanja in storitve reševanja sporov. V dodatnih smernicah, ki jih bo zagotovilo Ministrstvo, bo naveden tudi datum, do katerega bi morala biti objavljena letna poročila organov za ustrezno obdobje poročanja.

Nadalje spremljajo organizacije, ki želijo biti ali so bile odstranjene s seznama okvira za varstvo zasebnosti podatkov

— Če organizacija želi izstopiti iz DPF EU-ZDA, bo Ministrstvo zahtevalo, da organizacija iz vsake ustrezne politike zasebnosti odstrani vse sklice na DPF EU-ZDA, ki nakazujejo, da še naprej sodeluje v DPF EU-ZDA in da lahko prejema osebne podatke v skladu z DPF EU-ZDA (glej opis zaveze Ministrstva iskanju lažnih navedb o sodelovanju). Ministrstvo bo tudi zahtevalo, da organizacija izpolni in mu predloži ustrezen vprašalnik , da bi preverilo:

  — njene želje po izstopu;

  — kaj od naslednjega bo storila z osebnimi podatki, ki jih je prejela na podlagi DPF EU-ZDA, medtem ko je sodelovala v DPF EU-ZDA: (a) hranila take podatke, zanje še naprej uporabljala načela in vsako leto Ministrstvu potrdila svojo zavezo uporabi načel za take podatke; (b) hranila take podatke in zagotavljala „ustrezno“ varstvo zanje z drugimi dovoljenimi sredstvi ali (c) vrnila ali izbrisala take podatke do navedenega datuma, ter

  — kdo v organizaciji bo imel vlogo osebe za stike za vprašanja, povezana z načeli.

— Če se je organizacija odločila tako, (a) kot je navedeno v predhodni alinei, bo Ministrstvo tudi zahtevalo, da vsako leto po svojem izstopu (tj. do prve obletnice svojega izstopa ter tudi do vsake naslednje obletnice, razen če in dokler organizacija bodisi zagotavlja „ustrezno“ varstvo takih podatkov z drugimi dovoljenimi sredstvi, ali vrne ali izbriše take podatke, o tem ukrepu pa obvesti Ministrstvo) izpolni in mu predloži ustrezen vprašalnik za preverjanje, kaj je storila z osebnimi podatki, kaj bo storila s katerimi koli od navedenih osebnih podatkov, ki jih še naprej hrani, in kdo v organizaciji bo imel vlogo osebe za stike za vprašanja, povezana z načeli.

— Če je samocertificiranje organizacije poteklo (tj. niti ni opravila letnega ponovnega certificiranja spoštovanja načel niti iz kakega drugega razloga, kot je izstop, ni bila odstranjena s seznama okvira za varstvo zasebnosti podatkov), ji bo Ministrstvo odredilo, naj ga opravi ter mu predloži ustrezen vprašalnik za preverjanje, ali želi izstopiti ali opraviti ponovno certificiranje:

  — in če želi izstopiti, za nadaljnje preverjanje, kaj bo storila z osebnimi podatki, ki jih je prejela na podlagi DPF EU-ZDA, medtem ko je sodelovala v DPF EU-ZDA (glej prejšnji opis, kaj mora organizacija preveriti, če želi izstopiti);

  — in če se namerava ponovno certificirati, za nadaljnje preverjanje, ali je med potekom njenega statusa ceritificiranja uporabljala načela za osebne podatke, ki jih je prejela v skladu z DPF EU-ZDA, in pojasni, katere ukrepe bo sprejela za obravnavanje nerešenih težav, zaradi katerih je zamudila svoje ponovno certificiranje.

— Če je organizacija odstranjena s seznama okvira za varstvo zasebnosti podatkov iz katerega koli od naslednjih razlogov: (a) izstop iz DPF EU-ZDA, (b) zaradi neopravljenega letnega ponovnega certificiranja spoštovanja načel (tj. ga je bodisi začela, vendar ni opravila postopka letnega ponovnega certificiranja ni pravočasno zaključila, bodisi postopka letnega ponovnega certificiranja ni niti začela) ali (c) „vztrajno nespoštovanje načel“, bo Ministrstvo osebi/-am za stike, navedeni/-m v vlogi organizacije za samocertificiranje, poslalo obvestilo, v katerem bo navedlo razlog za odstranitev in pojasnilo, da mora prenehati izrecno ali implicitno navajati, da sodeluje v DPF EU-ZDA ali da izpolnjuje njegova načela, in da lahko prejema osebne podatke v skladu s DPF EU-ZDA. V obvestilu, ki lahko vključuje tudi drugo vsebino, prilagojeno razlogu za odstranitev, bo navedeno, da so lahko organizacije, ki zavajajo o svojem sodelovanju v DPF EU-ZDA ali izpolnjevanju njegovih načel, vključno z navajanjem, da sodelujejo v DPF EU-ZDA, potem ko so bile odstranjene s seznama okvira za varstvo zasebnosti podatkov, predmet izvršilnih ukrepov FTC, ministrstva za promet ali drugega ustreznega vladnega organa.

Sproti poiskalo in obravnavalo lažne navedbe o sodelovanju,

— če organizacija: (a) izstopi iz sodelovanja v DPF EU-ZDA, (b) ne opravi letnega ponovnega certificiranja spoštovanja načel (tj. postopek letnega ponovnega certificiranja je bodisi začela, vendar ga ni pravočasno opravila, bodisi postopka letnega ponovnega certificiranja sploh ni začela), (c) je izločena kot udeleženec iz DPF EU-ZDA, zlasti zaradi „vztrajnega neizpolnjevanja načel“ ali (d) ne opravi začetnega samocertificiranja spoštovanja načel (tj. postopek letnega ponovnega certificiranja je sicer začela, vendar ga ni pravočasno opravila), bo Ministrstvo po uradni dolžnosti sproti sprejemalo ukrepe za preverjanje, da nobena ustrezna objavljena politika zasebnosti organizacije ne vsebuje sklicev na DPF EU-ZDA, ki nakazujejo, da organizacija še naprej sodeluje v DPF EU-ZDA in da lahko prejema osebne podatke v skladu z DPF EU-ZDA. Če Ministrstvo najde take sklice, bo organizacijo obvestilo, da bo po potrebi zadevo odstopilo ustrezni agenciji za morebitno uvedbo pregona, če bo ta še naprej zavajala o svojem sodelovanju DPF EU-ZDA. Ministrstvo bo organizacijo o tem obvestilo prek osebe za stike, ki jo je organizacija navedla Ministrstvu, ali po potrebi na druge ustrezne načine. Če organizacija niti ne odstrani sklicev niti ne opravi samocertificiranja svoje skladnosti na podlagi DPF EU-ZDA v skladu s postopki Ministrstva, bo Ministrstvo po uradni dolžnosti zadevo odstopilo FTC, ministrstvu za promet ali drugemu ustreznemu organu pregona ali pa sprejelo ustrezne ukrepe za zagotovitev pravilne uporabe certifikacijske oznake DPF EU-ZDA;

— Ministrstvo si bo drugače prizadevalo za prepoznavanje lažnih navedb o sodelovanju v DPF EU-ZDA in nepravilne uporabe certifikacijske oznake DPF EU-ZDA, tudi s strani organizacij, ki za razliko od organizacij, navedenih v predhodni alinei, nikoli niso začele postopka samocertificiranja (npr. z iskanjem ustreznih strani po internetu za odkrivanje sklicev na certifikacijske oznake DPF EU-ZDA v politikah zasebnosti organizacij). Če Ministrstvo s takimi prizadevanji ugotovi lažne navedbe o sodelovanju v DPF EU-ZDA in nepravilno uporabe certifikacijske oznake DPF EU-ZDA, bo Ministrstvo organizacijo obvestilo, da bo po potrebi zadevo odstopilo ustrezni agenciji za morebitno uvedbo pregona, če bo ta še naprej zavajala o svojem sodelovanju v DPF EU-ZDA. Ministrstvo bo o tem obvestilo organizacijo prek morebitne osebe za stike, ki jo je organizacija navedla Ministrstvu, ali po potrebi na druge ustrezne načine. Če organizacija niti ne odstrani sklicev nisi ne opravi samocertificiranja svoje skladnosti na podlagi DPF EU-ZDA v skladu s postopki Ministrstva, bo Ministrstvo po uradni dolžnosti zadevo odstopilo FTC, ministrstvu za promet ali drugemu ustreznemu organu pregona ali pa sprejelo ustrezne ukrepe za zagotovitev pravilne uporabe certifikacijske oznake DPF EU-ZDA;

— Ministrstvo bo sproti pregledovalo in obravnavalo konkretne resne pritožbe o lažnih navedbah o sodelovanju v DPF EU-ZDA, ki jih prejme (npr. pritožbe, ki jih prejme od organov za varstvo podatkov, neodvisnih pritožbenih mehanizmov, ki jih zagotavljajo organi za alternativno reševanje sporov v zasebnem sektorju, posameznikov, na katere se nanašajo osebni podatki, podjetij v EU in ZDA ter drugih vrst tretjih strank) in

— Ministrstvo lahko sprejme druge ustrezne popravne ukrepe. Zavajanje Ministrstva se lahko kaznuje na podlagi zakona o lažnih navedbah (člen 1001 naslova 18 zakonodajne zbirke ZDA.

Po uradi dolžnosti opravljalo redne preglede skladnosti z načeli in ocene programa okvira za varstvo zasebnosti podatkov

— Ministrstvo si bo sproti prizadevalo za spremljanje dejanske skladnosti organizacij v DPF EU-ZDA, da bi odkrilo težave, ki lahko zahtevajo nadaljnje ukrepe. Ministrstvo bo zlasti po uradni dolžnosti izvajalo preglede naključno izbranih organizacij v DPF EU-ZDA na kraju samem ter tudi *ad hoc* preglede nekaterih organizacij v DPF EU-ZDA na kraju samem, če so ugotovljene morebitne pomanjkljivosti na področju skladnosti (npr. morebitne pomanjkljivosti na področju skladnosti, na katere so Ministrstvo opozorile tretje stranke), da bi preverilo: (a) ali je/so na voljo oseba/-e za stike, odgovorna/-e za obravnavanje pritožb, zahtev za dostop in drugih vprašanj, ki se pojavijo v skladu z DPF EU-ZDA; (b) če je ustrezno, ali je javno dostopna politika zasebnosti organizacije dostopna javnosti na javnem spletnem mestu organizacije ali prek hiperpovezave na seznam okvira za varstvo zasebnosti podatkov; (c) ali je politika zasebnosti organizacije še vedno skladna z zahtevami za samocertificiranje, navedenimi v načelih, in (d) ali je na voljo neodvisen pritožbeni mehanizem, ki ga je opredelila organizacija, za obravnavanje pritožb, vloženih v skladu z DPF EU-ZDA. Ministrstvo bo prav tako dejavno spremljalo nove objave poročil, ki zagotavljajo verodostojne dokaze o neskladnosti organizacij v DPF EU-ZDA;

— v okviru svojega pregleda skladnosti bo Ministrstvo zahtevalo, da organizacija v DPF EU-ZDA izpolni in Ministrstvu predloži izčrpen vprašalnik, če: (a) je Ministrstvo prejelo kakršne koli konkretne resne pritožbe v zvezi z upoštevanjem načel s strani organizacije, (b) organizacija ne odgovori zadovoljivo na poizvedbe Ministrstva po informacijah v zvezi z DPF EU-ZDA ali (c) če obstajajo verodostojni dokazi, da organizacija ne izpolnjuje svojih zavez v skladu z DPF EU-ZDA. Če je Ministrstvo organizaciji poslalo tak izčrpen vprašalnik in ta nanj ne odgovori zadovoljivo, bo Ministrstvo organizacijo obvestilo, da bo po potrebi zadevo odstopilo ustrezni agenciji za morebitno uvedbo pregona, če od nje ne bo prejelo pravočasnega in zadovoljivega odgovora. Ministrstvo bo organizacijo o tem obvestilo prek osebe za stike, ki jo je organizacija navedla Ministrstvu, ali po potrebi na druge ustrezne načine. Če organizacija ne odgovori pravočasno in zadovoljivo, bo Ministrstvo po uradni dolžnosti predalo zadevo FTC, ministrstvu za promet ali drugemu organu pregona ali sprejelo druge ustrezne ukrepe za zagotavljanje skladnosti. Ministrstvo se o takšnih pregledih skladnosti z načeli po potrebi posvetuje s pristojnimi organi za varstvo podatkov in

— Ministrstvo bo redno ocenjevalo upravljanje in nadzor programa okvira za varstvo zasebnosti podatkov, da bi zagotovilo, da so njegova prizadevanja za spremljanje, vključno z vsemi prizadevanji za uporabo iskalnih orodij (npr. za pregled prekinjenih povezav na politike zasebnosti organizacij v DPF EU-ZDA), primerna za obravnavanje obstoječih vprašanj in morebitnih novih vprašanj, ko se pojavijo.

Prilagodilo spletno mesto okvira za varstvo zasebnosti podatkov ciljnim skupinam

Ministrstvo bo prilagodilo spletno mesto okvira za varstvo zasebnosti podatkov naslednjim ciljnim skupinam: posameznikom iz EU, podjetjem iz EU, podjetjem iz ZDA in organom za varstvo podatkov. Vključitev gradiva, namenjenega neposredno posameznikom in podjetjem iz EU, bo na več načinov omogočila preglednost. Spletno mesto bo posameznikom iz EU natančno pojasnilo: (1) pravice, zagotovljene posameznikom iz EU v skladu z DPF EU-ZDA; (2) pritožbene mehanizme, ki so na voljo posameznikom iz EU, če menijo, da je organizacija kršila svojo zavezanost spoštovanju načel in (3) kako poiskati informacije v zvezi s samocertificiranjem organizacije v DPF EU-ZDA. Podjetjem iz EU bo omogočila preverjanje: (1) ali je organizacija član DPF EU-ZDA; (2) vrsto informacij, ki jih zajema samocertificiranje organizacije v DPF EU-ZDA; (3) politiko zasebnosti, ki velja za zajete informacije, in (4) metodo, ki jo organizacija uporablja za preverjanje spoštovanja načel. Podjetjem iz ZDA bo pojasnila: (1) koristi sodelovanja v DPF EU-ZDA; (2) kako se pridružiti DPF EU-ZDA ter tudi, kako se ponovno certificirati za DPF EU-ZDA ali izstopiti iz njega in (3) kako Združene države upravljajo in izvršujejo DPF EU-ZDA. Vključitev gradiva, namenjenega neposredno organom za varstvo podatkov (npr. informacij o namenski kontaktni točki Ministrstva za organe za varstvo podatkov in hiperpovezava na vsebino na spletišču FTC v zvezi z načeli) bo olajšala sodelovanje in preglednost. Ministrstvo bo tudi *ad hoc* sodelovalo s Komisijo in Evropskim odborom za varstvo podatkov (EOVP) za pripravo dodatnega, tematskega gradiva (npr. odgovorov na pogosto zastavljena vprašanja) za uporabo na spletnem mestu okvira za varstvo zasebnosti podatkov, kjer bi take informacije olajšale učinkovito upravljanje in nadzor programa okvira za varstvo zasebnosti podatkov.

Povečalo sodelovanje z organi za varstvo podatkov

Za krepitev priložnosti za sodelovanje z organi za varstvo podatkov bo Ministrstvo zagotavljalo posebno osebo za stike pri Ministrstvu, ki bo imela vlogo uradnika za zvezo z organi za varstvo podatkov. V primerih, ko organ za varstvo podatkov meni, da organizacija v DPF EU-ZDA ne izpolnjuje načel, tudi po pritožbi posameznika iz EU, se bo lahko organ za varstvo podatkov obrnil na posebno osebo za stike pri Ministrstvu in zahteval nadaljnji pregled organizacije. Ministrstvo si bo čim bolj prizadevalo olajšati reševanje pritožbe z organizacijo v DPF EU-ZDA. Ministrstvo bo v 90 dneh po prejemu pritožbe obvestilo organ za varstvo podatkov. Posebna oseba za stike bo prejela tudi predložene zadeve v zvezi z organizacijami, ki lažno navajajo, da sodelujejo v DPF EU-ZDA. Posebna oseba za stike bo spremljala vse predložene zadeve organov za varstvo podatkov, ki jih prejme Ministrstvo, slednje pa bo v skupnem pregledu, opisanem spodaj, predložilo poročilo z zbirno analizo pritožb, ki jih prejme vsako leto. Posebna oseba za stike bo organom za varstvo podatkov pomagala pri iskanju informacij v zvezi s samocertificiranjem posamezne organizacije ali njenem prejšnjem sodelovanju v DPF EU-ZDA ter odgovarjala na poizvedbe organa za varstvo podatkov v zvezi z izvajanjem posebnih zahtev DPF EU-ZDA. Ministrstvo bo sodelovalo tudi s Komisijo in EOVP pri postopkovnih in upravnih vidikih foruma organov za varstvo podatkov, tudi pri določitvi ustreznih postopkov za razdelitev sredstev, zbranih s pristojbino foruma organov za varstvo podatkov. Kot smo seznanjeni, bo Komisija sodelovala z Ministrstvom za lažje reševanje vseh vprašanj, ki se lahko pojavijo v zvezi z navedenimi postopki. Poleg tega bo Ministrstvo organom za varstvo podatkov zagotovilo gradivo v zvezi z DPF EU-ZDA, ki ga vključijo na lastna spletišča in s tem povečajo preglednost za posameznike in podjetja iz EU. Večja ozaveščenost v zvezi z DPF EU-ZDA ter pravicami in odgovornostmi, ki jih prinaša, bi morala olajšati odkrivanje vprašanj, ko se ta pojavijo, tako da jih je mogoče ustrezno obravnavati.

Izpolnilo svoje zaveze v skladu s Prilogo I k načelom

Ministrstvo bo izpolnilo svoje zaveze v skladu s Prilogo I k načelom, vključno z vodenjem seznama arbitrov, ki jih izbere Komisija na podlagi njihove neodvisnosti, integritete in strokovnosti, in po potrebi z zagotavljanjem podpore tretji stranki, ki jo izbere Ministrstvo za upravljanje arbitraž v skladu s Prilogo I k načelom in arbitražnega sklada, opredeljenega v njej ([3]). Ministrstvo bo sodelovalo s tretjo stranko med drugim pri preverjanju, ali tretja stranka vzdržuje spletno mesto s smernicami o arbitražnemm postopku, vključno: (1) z načinom uvedbe postopkov in predložitvijo dokumentov; (2) s seznamom arbitrov, ki ga vodi Ministrstvo, in načinom izbire arbitrov z navedenega seznama; (3) z urejanjem arbitražnega postopka in s kodeksom ravnanja za arbitre, ki sta ga sprejela Ministrstvo in Komisija ([4]), in (4) s pobiranjem in plačilom honorarjev arbitrov. Poleg tega bo Ministrstvo sodelovalo s tretjo stranko pri rednem pregledu delovanja arbitražnega sklada, vključno s potrebo po prilagoditvi zneska prispevkov ali najvišjih vrednosti (tj. najvišjih zneskov) stroška arbitraže, in med drugim upoštevalo število arbitraž ter stroške in časovni potek arbitraž ob sporazumu, da organizacijam v DPF EU-ZDA ne bo naloženo čezmerno finančno breme. Ministrstvo bo Komisijo obvestilo o izidu takih pregledov s tretjo stranko in jo predhodno obvestilo o morebitnih prilagoditvah zneska prispevkov.

Izvajalo skupne preglede delovanja DPF EU-ZDA

Ministrstvo in drugi organi, kot je primerno, se bodo redno sestajali s Komisijo, zainteresiranimi organi za varstvo podatkov in ustreznimi predstavniki EOVP, Ministrstvo pa jim bo zagotovilo najnovejše podatke o DPF EU-ZDA. Na srečanjih bodo obravnavana aktualna vprašanja v zvezi z delovanjem, izvajanjem, nadzorom in uveljavljanjem programa okvira za varstvo zasebnosti podatkov. Srečanja lahko po potrebi vključujejo razprave o povezanih temah, kot so drugi mehanizmi za prenos podatkov, ki jim koristijo zaščitni ukrepi v skladu z DPF EU-ZDA.

([3]) ICDR, mednarodni oddelek AAA (v nadaljnjem besedilu skupaj: ICDR-AAA) je izbralo Ministrstvo za upravljanje arbitraž v skladu s Prilogo I k načelom in arbitražnega sklada, opredeljenega v njej.

([4]) Ministrstvo in Komisija sta se 15. septembra 2017 dogovorila o sprejetju sklopa arbitražnih pravil za urejanje zavezujočih arbitražnih postopkov, opisanih v Prilogi I k načelom, in tudi o kodeksu ravnanja za arbitre, ki je skladen s splošno sprejetimi etičnimi standardi za trgovinske arbitre in Prilogo I k načelom. Ministrstvo in Komisija sta se dogovorila o prilagoditvi arbitražnih pravil in kodeksa ravnanja, tako da izražata posodobitve DPF EU-ZDA, Ministrstvo pa bo sodelovalo z ICDR-AAA pri pripravi navedenih posodobitev.

Posodabljalo zakonodajo

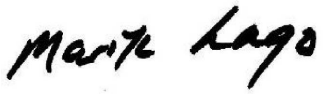
Ministrstvo si bo čim bolj prizadevalo obveščati Komisijo o vsebinskem razvoju prava v Združenih državah, kolikor bo ta upošteven za DPF EU-ZDA na področju varstva zasebnosti podatkov, ter omejitvah in zaščitnih ukrepih, ki se uporabljajo za omejitev dostopa do osebnih podatkov s strani organov ZDA.

Dostop ameriške vlade do osebnih podatkov

Združene države so izdale Odredbo št. 14086 z naslovom „Krepitev zaščitnih ukrepov za obveščevalne dejavnosti SIGINT ZDA“ in poglavje 28, del 201, zakonika Združenih držav (*U.S. Code of Federal Regulations*, v nadaljnjem besedilu: CFR), s katerim so bili spremenjeni predpisi Ministrstva za pravosodje ZDA za ustanovitev sodišča za presojo varstva podatkov (*Data Protection Review Court*, v nadaljnjem besedilu: DPRC), ki zagotavljata močno varstvo osebnih podatkov v zvezi z vladnim dostopom do podatkov za namene nacionalne varnosti. Zagotovljeno varstvo vključuje: krepitev zaščitnih ukrepov na področju varstva zasebnosti in državljanskih svoboščin za zagotovitev, da so obveščevalne dejavnosti SIGINT ZDA potrebne in sorazmerne pri uresničevanju opredeljenih ciljev nacionalne varnosti; vzpostavitev novega mehanizma pravnih sredstev z neodvisnim in zavezujočim pooblastilom ter krepitev obstoječega strogega in večplastnega nadzora nad obveščevalnimi dejavnostmi SIGINT ZDA. S tem varstvom lahko posamezniki iz EU zahtevajo odškodnino od novega večplastnega mehanizma pravnih sredstev, ki vključuje neodvisen DPRC, ki bi ga sestavljali izbrani posamezniki, ki niso v vladi ZDA, in bi imeli polno pooblastilo za odločanje o zahtevkih in po potrebi usmerjali popravne ukrepe. Ministrstvo bo vodilo evidenco posameznikov iz EU, ki vložijo upravičeno pritožbo v skladu z Odredbo št. 14086 in poglavjem 28, del 201, CFR. Ministrstvo bo pet let po datumu tega dopisa, nato pa vsakih pet let, vzpostavilo stik z ustreznimi organi v zvezi z vprašanjem, ali je bila informacijam v zvezi s pregledom upravičenih pritožb ali morebitnih vlog za pregled, ki so bile predložene DPRC, preklicana stopnja zaupnosti. Če je bila takim informacijam preklicana stopnja zaupnosti, bo Ministrstvo sodelovalo z ustreznim organom za varstvo podatkov pri obveščanju posameznika iz EU. Te izboljšave potrjujejo, da bodo osebni podatki, preneseni v Združene države, obravnavani na način, ki je skladen s pravnimi zahtevami EU glede vladnega dostopa do podatkov.

Na podlagi načel, Odredbe št. 14086, poglavja 28, del 201, CFR in priloženih dopisov in gradiva, vključno z zavezami Ministrstva v zvezi z upravljanjem in nadzorom programa okvira za varstvo zasebnosti podatkov, pričakujemo, da bo Komisija ugotovila, da DPF EU-ZDA zagotavlja ustrezno varstvo za namene prava EU in da se bodo podatki še naprej prenašali iz Evropske unije organizacijam, ki sodelujejo v DPF EU-ZDA. Prav tako pričakujemo, da bodo pogoji navedenih ureditev še olajšali prenose organizacijam v ZDA na podlagi standardnih pogodbenih klavzul EU ali zavezujočih poslovnih pravil EU.

S spoštovanjem,



Marisa LAGO

PRILOGA IV

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

9. junij 2023

Didier Reynders
Komisar za pravosodje
Evropska komisija
Rue de la Loi / Wetstraat 200
1049 Bruselj
Belgija

Spoštovani komisar Reynders,

Zvezna komisija za trgovino ZDA (Federal Trade Commission, v nadaljnjem besedilu: FTC) se zahvaljuje za priložnost za obravnavo svoje izvršilne vloge v zvezi z načeli okvira za varstvo zasebnosti podatkov med EU in ZDA (DPF EU-ZDA). FTC je že dlje časa zavezan varstvu potrošnikov in zasebnosti prek meja, in zavezani smo uveljavljanju vidikov trgovinskega sektorja v tem okviru. FTC tako vlogo opravlja od leta 2000 v zvezi z okvirom varnega pristana med ZDA in EU, nedavno, od leta 2016 pa v zvezi z okvirom zasebnostnega ščita EU-ZDA ([1]). Dne 16. julija 2020 je Sodišče Evropske unije (SEU) razveljavilo sklep Evropske komisije o ustreznosti, na kateri temelji okvir zasebnostnega ščita EU-ZDA, zaradi težav, ki niso trgovinska načela, ki jih je FTC uveljavil. ZDA in Evropska komisija sta se od takrat pogajali o okviru za varstvo zasebnosti podatkov med EU in ZDA, da bi obravnavali navedeno sodbo SEU.

V svojem pismu potrjujem zavezo FTC odločnemu uveljavljanju načel DPF EU-ZDA. Zlasti potrjujemo svojo zavezo na treh ključnih področjih: (1) prednostna obravnava in preiskovanje predloženih zadev; (2) uveljavljanje in spremljanje sklepov ter 3) izvrševanje sodelovanja z organi za varstvo podatkov EU.

I. **Uvod**

a. **Izvrševanje in politika FTC na področju varstva zasebnosti**

FTC ima široka pooblastila za izvrševanje civilnega prava z namenom spodbujanja varstva potrošnikov in konkurenčnosti v trgovini. V okviru svojega pooblastila za zaščito potrošnikov FTC izvaja široko paleto zakonov za varstvo zasebnosti in

([1]) Pismo predsednice Edith Ramirez komisarki Evropske unije za pravosodje, potrošnike in enakost spolov Věri Jourovi z naslovom „*Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework*“ (Opis uveljavitve novega zasebnostnega ščita EU-ZDA s strani Zvezne komisije za trgovino) (29. februar 2016), na voljo na naslovu https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. FTC se je v preteklosti zavezala tudi uveljavitvi programa varnega pristana ZDA-EU. Pismo predsednika FTC Roberta Pitofskyja direktorju GD Evropske komisije za notranji trg, Johnu Moggu (14. julij 2000), na voljo na naslovu https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. To pismo nadomešča navedene prejšnje zaveze.

varnosti potrošnikov in njihovih podatkov. Glavni zakon, ki ga izvaja FTC, tj. zakon o FTC (*FTC Act*), prepoveduje „nepoštena“ ali „goljufiva“ dejanja ali ravnanje v trgovini ali v zvezi z njo ([2]). FTC 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 ([3]).

FTC je nedavno uresničil številne pobude za krepitev našega dela na področju varstva zasebnosti. Avgusta 2022 je FTC napovedal, da proučuje pravila za preprečevanje škodljivega trgovinskega nazora in ohlapne varnosti podatkov ([4]). Cilj projekta je vzpostaviti zanesljivo javno evidenco za obveščanje, ali bi moral FTC izdati pravila za obravnavo praks na področju trgovinskega nazora in varnosti podatkov, ter kakšna bi ta pravila morala biti. Pozdravili smo pripombe deležnikov o tem in drugih pobudah.

Na naših konferencah o zasebnosti „PrivacyCon“ se še naprej zbirajo vodilni raziskovalci, da bi razpravljali o najnovejših raziskavah in trendih v zvezi z varstvom zasebnosti potrošnikov in varnostjo podatkov. Prav tako smo povečali zmogljivosti naše agencije, da bi sledili tehnološkemu razvoju, ki je v veliki meri v središču našega dela na področju varstva zasebnosti, ter oblikovali skupino tehnologov in interdisciplinarnih raziskovalcev, ki še naprej raste. Kot veste, smo napovedali tudi skupni dialog z vami in vašimi kolegi pri Evropski komisiji, kar vključuje obravnavo tem v zvezi z varstvom zasebnosti, kot so temni vzorci in poslovni modeli, za katere je značilno vseprisotno zbiranje podatkov ([5]). Nedavno smo prav tako izdali poročilo Kongresu, v katerem opozarjamo na škodo, povezano z uporabo umetne inteligence (UI), da bi obravnavali škodo v spletu, ki jo je ugotovil Kongres. To poročilo je vzbudilo pomisleke v zvezi z netočnostjo, pristranskostjo, diskriminacijo in širjenjem trgovinskega nadzora ([6]).

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

DPF EU-ZDA deluje v sklopu širšega področja zasebnosti v ZDA, ki na več načinov ščiti potrošnike iz EU. Prepoved nepoštenih ali goljufivih dejanji ali ravnanja v zakonu o FTC 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 FTC pri zaščiti tujih potrošnikov uporabi vsa pravna sredstva, ki so na voljo za zaščito domačih potrošnikov ([7]).

FTC uveljavlja tudi druge ciljne zakone, ki varujejo tudi potrošnike zunaj ZDA, kot je zakon o varstvu zasebnosti otrok na spletu (*Children's Online Privacy Protection Act*, v nadaljnjem besedilu: 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

([2]) Člen 45(a) naslova 15 zakonodajne zbirke ZDA. FTC ni pristojen za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali zadeve nacionalne varnosti. FTC prav tako ne more doseči večino drugih vladnih ukrepov. Poleg tega obstajajo izjeme v pristojnosti FTC za trgovinske dejavnosti, tudi v zvezi z bankami, letalskimi prevozniki, zavarovalništvom in dejavnostmi splošnih telekomunikacijskih operaterjev. FTC prav tako ni pristojen za večino neprofitnih organizacij, je pa pristojen za lažne dobrodelne in druge neprofitne organizacije, ki dejansko poslujejo za dobiček. FTC je pristojen tudi za neprofitne organizacije, ki poslujejo za dobiček svojih članov, usmerjenih v dobiček, vključno tako, da zagotavljajo precejšnje gospodarske koristi tem članom. V nekaterih primerih pristojnost FTC 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.

([3]) Glej FTC, poglavje „*Privacy and Security*“ (Zasebnost in varnost), https://www.ftc.gov/business-guidance/privacy-security.

([4]) Glej sporočilo za javnost Zvezne komisije za trgovino „*FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices*“ (FTC proučuje pravila za preprečevanje škodljivih praks na področju trgovinskega nadzora in ohlapne varnosti podatkov) (11. avgust 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) Glej skupno izjavo za javnost Didierja Reyndersa, komisarja Evropske unije za pravosodje, in Line Khan, predsednice FCA ZDA (30. marec 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) Glej sporočilo za javnost Zvezne komisije za trgovino „*FTC Report Warns About Using Artificial Intelligence to Combat Online Problems*“ (Opozorila FTC o uporabi umetne inteligence za odpravo težav na spletu) (16. junij 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) Člen 45(a)(4)(B) zakonodajne zbirke ZDA. Poleg tega pojem „nepoštena ali goljufiva dejanja ali ravnanja“ vključuje taka dejanja ali ravnanja, ki vključujejo zunanjo trgovino, ki (i) povzročijo ali je verjetno, da bodo povzročili, razumno predvidljivo škodo v Združenih državah ali (ii) vključujejo bistveno ravnanje v Združenih državah. Člen 45(a)(4)(A) naslova 15 zakonodajne zbirke ZDA.

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. Še več, poleg ameriških zveznih zakonov, ki jih uveljavlja FTC, lahko potrošnikom iz EU prinesejo dodatne ugodnosti tudi drugi zvezni in državni zakoni na področju varstva potrošnikov, kršitev varstva podatkov in varstva zasebnosti.

c. **Dejavnost uveljavljanja FTC**

FTC je vložil tožbe v skladu z okvirom varnega pristana ZDA-EU in tudi okvirom zasebnostnega ščita EU-ZDA ter še naprej uveljavljala zasebnostni ščit EU-ZDA, tudi po razveljavitvi sklepa o ustreznosti s strani SEU, na katerem temelji okvir zasebnostnega ščita EU-ZDA ([8]). Več nedavnih pritožb FTC je vsebovalo obtožbe, da so podjetja kršila določbe zasebnostnega ščita EU-ZDA, tudi v postopkih zoper Twitter, ([9]) CafePress, ([10]) in Flo ([11]). Pri uvedbi pregona v zadevi zoper Twitter je FTC od Twitterja pridobil 150 milijonov USD zaradi njegove kršitve prejšnjega sklepa FTC z ravnanji, ki so vplivala na več kot 140 milijonov potrošnikov, vključno s kršitvijo načela 5 zasebnostnega ščita EU-ZDA (celovitost podatkov in omejitev namena). Nadalje, sklep organa zahteva, da Twitter uporabnikom omogoči uporabo varnih metod večfaktorske avtentikacije, ki od uporabnikov ne zahtevajo, da zagotovijo svoje telefonske številke.

V zadevi CafePress je FTC trdil, da podjetje ni zaščitilo občutljivih podatkov potrošnikov, pri čemer je prikrilo veliko kršitev podatkov in kršilo načela 2 (izbira), 4 (varnost) in 6 (dostop) zasebnostnega ščita EU-ZDA. V skladu s sklepom FTC mora podjetje nadomestiti neustrezne ukrepe na področju avtentikacije z večfaktorsko avtentikacijo, znatno omejiti količino podatkov, ki jih zbira in hrani, šifrirati številke socialnega zavarovanja in dati tretji stranki oceniti svoje programe na področju informacijske varnosti, FTC pa predloži kopijo, ki jo je mogoče objaviti.

V zadevi Flo je FTC trdil, da je aplikacija za spremljanje plodnosti razkrila zdravstvene informacije uporabnikov tretjim ponudnikom storitev podatkovne analitike po tem, ko se je zavezala varovanju zaupnosti takih podatkov. V pritožbi FTC je izrecno navedeno sodelovanje podjetja s potrošniki iz EU in da je Flo kršila načela 1 (obvestilo), 2 (izbira), 3 (odgovornosti za prenos tretjemu) in 5 (celovitost podatkov in omejitev namena) zasebnostnega ščita EU-ZDA. Med drugim mora Flo v skladu s sklepom organa obvestiti zadevne uporabnike o razkritju njihovih osebnih podatkov ter vsaki tretji stranki, ki je prejela zdravstvene informacije uporabnikov, naročiti, naj uniči navedene podatke. Pomembno je, da sklepi FTC varujejo vse potrošnike po svetu, ki sodelujejo s podjetjem iz ZDA, ne le tiste potrošnike, ki so vložili pritožbe.

Številni pretekli primeri pregona na podlagi varnega pristana ZDA-EU in zasebnostnega ščita EU-ZDA so vključevali organizacije, ki so opravile začetno samocertificiranje prek Ministrstva za trgovino ZDA (*Department of Commerce*), vendar niso samocertificiranja niso opravljale letno, hkrati pa se še naprej predstavljale kot aktualni udeleženci. Druge zadeve so vključevale lažne navedbe o sodelovanju organizacij, ki nikoli niso opravile začetnega samocertificiranja prek Ministrstva za trgovino ZDA. V prihodnje pričakujemo, da bomo naša proaktivna prizadevanja na področju izvrševanja usmerili v vrste domnevnih bistvenih kršitev načel DPF EU-ZDA v zadevah, kot so Twitter, CafePress in Flo. Medtem bo Ministrstvo za trgovino ZDA upravljalo in nadziralo postopek samocertificiranja, vodilo verodostojen seznam udeležencev v DPF EU-ZDA in obravnavalo vprašanja navedb o sodelovanju v drugih programih ([12]). Pomembno je, da so lahko organizacije, ki navajajo, da sodelujejo v DPF EU-ZDA, predmet vsebinskega uveljavljanja načel DPF EU-ZDA, tudi če ne opravijo ali ne opravljajo redno samocertificiranja prek Ministrstva za trgovino ZDA.

([8]) Za seznam zadev FTC v zvezi z varnim pristanom in zasebnostnim ščitom glej Dodatek A.

([9]) Glej sporočilo za javnost Zvezne komisije za trgovino „*FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads*“ (FTC toži Twitter zaradi goljufive uporabe varnostnih podatkov o računu za prodajo ciljno usmerjenih oglasov) (25. maj 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) Glej sporočilo za javnost Zvezne komisije za trgovino „*FTC Takes Action Against CafePress for Data Breach Cover Up*“ (FTC toži CafePress zaradi prikrivanja kršitve podatkov) (15. marec 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) Glej sporočilo za javnost Zvezne komisije za trgovino „*FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*“ (FTC dokončuje poravnavo s Flo Health, aplikacijo za spremljanje plodnosti, ki je delila občutljive zdravstvene podatke s Facebookom, Googlom in drugimi) (22. junij 2021),https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Pismo Marise Lago, namestnice ministra za mednarodno trgovino, spoštovanemu Didierju Reyndersu, komisarju Evropske komisije za pravosodje (12. december 2022).

II. **Prednostna obravnava in preiskave predloženih zadev**

Zvezna komisija za trgovino se tako kot v okviru varnega pristana EU-ZDA in v okviru zasebnostnega ščita EU-ZDA zavezuje, da bo dala prednost zadevam, ki jih Ministrstvo za trgovino ZDA in države članice EU predložijo v zvezi z načeli DPF EU-ZDA. Prav tako bomo dali prednost zadevam neizpolnjevanja načel DPF EU-ZDA, ki jih predložijo organizacije s samourejevalnim sistemom za varstvo zasebnosti in drugi neodvisni organi za reševanje sporov.

Za lažjo predložitev zadev držav članic EU v skladu z DPF EU-ZDA je FTC pripravil poenoten postopek za predložitev in daje državam članicam EU navodila glede vrste informacij, ki bi najbolj pomagale FTC v njegovi preiskavi predložene zadeve. V okviru teh prizadevanj je FTC v agenciji imenoval 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 s FTC v preiskavi.

Ob prejemu take predložitve Ministrstva za trgovino ZDA, države članice EU ali organizacije s samourejevalnim sistemom ali drugih neodvisnih organov za reševanje sporov lahko FTC sprejme vrsto različnih ukrepov za obravnavo sproženih vprašanj. Na primer, pregledamo lahko politike zasebnosti organizacije, pridobimo dodatne informacije neposredno od organizacije 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 ZDA, ocenimo, ali bi bila koristna dodatna prizadevanja za opozarjanje udeležencev na trgu, in po potrebi sprožimo izvršilni postopek.

Poleg prednostne obravnave zadev, ki jih v zvezi z načeli DPF EU-ZDA predložijo Ministrstvo za trgovino ZDA, države članice EU in organizacije s samourejevalnim sistemom ali drugi organi za reševanje sporov ([13]), bo FTC še naprej preiskoval pomembne kršitve načel DPF EU-ZDA na lastno pobudo, kjer je primerno, z različnimi orodji. V okviru svojega programa preiskovanja zadev glede varstva zasebnosti in varnosti, ki vključujejo trgovinske organizacije, je organ redno pregledoval, ali se zadevni subjekti predstavljajo v okviru zasebnostnega ščita EU-ZDA. Če se je subjekt tako predstavljal in je preiskava razkrila očitne kršitve načel zasebnostnega ščita EU-ZDA, je FTC v uvedbo pregona vključil obtožbe kršitev zasebnostnega ščita EU-ZDA. Ta dejavni pristop bomo nadaljevali tudi zdaj v zvezi z načeli DPF EU-ZDA.

III. **Uveljavljanje in spremljanje sklepov**

FTC potrjuje tudi zavezo, da bo uveljavljal in spremljal izvršilne odloke in tako zagotovil skladnost z načeli DPF EU-ZDA. Skladnost z načeli DPF EU-ZDA bomo zahtevali z vrsto ustreznih prepovednih določb v prihodnjih sklepih FTC v zvezi z načeli DPF EU-ZDA. Kršitve upravnih sklepov FTC lahko privedejo do denarnih kazni v višini do 50 120 USD za posamezno kršitev ali 50 120 USD na dan za nadaljnje kršenje ([14]), kar lahko v primeru ravnanja, ki zadeva veliko potrošnikov, znaša tudi več milijonov USD. Vsak sklep za pridobivanje soglasij vsebuje tudi določbe v zvezi s poročanjem in skladnostjo. Subjekti, na katere se nanaša sklep, morajo hraniti dokumente, ki dokazujejo njihovo izpolnjevanje načel, določeno število let. Sklepe je treba poslati tudi zaposlenim, ki so odgovorni za zagotavljanje izpolnjevanja sklepa.

FTC sistematično spremlja izpolnjevanje obstoječih sklepov v zvezi z načeli zasebnostnega ščita EU-ZDA kot pri vseh svojih sklepih ter po potrebi vlaga tožbe za njihovo uveljavitev ([15]). Pomembno je, da bodo sklepi FTC še naprej varovali vse potrošnike po svetu, ki sodelujejo s podjetjem, ne le tiste potrošnike, ki so vložili pritožbe. Nazadnje, FTC bo vodil spletni seznam podjetij, za katere veljajo sklepi, pridobljeni v zvezi z uveljavljanjem načel DPF EU-ZDA ([16]).

([13]) Čeprav FTC ne razrešuje ali izvaja mediacije pri posameznih pritožbah potrošnikov, pa potrjuje, da bo prednostno obravnaval zadeve v zvezi z načeli DPF EU-ZDA, ki jih bodo predložili organi EU za varstvo podatkov. Poleg tega FTC uporablja pritožbe v svoji podatkovni zbirki Consumer Sentinel, dostop do katere imajo mnogi drugi organi kazenskega pregona, da bi odkril gibanja ter določil prednostne naloge pri pregonu in morebitne preiskovalne cilje. Posamezniki iz EU lahko za predložitev pritožbe FTC uporabijo enak pritožbeni sistem, kakor je na voljo potrošnikom iz ZDA, in sicer na spletišču https://reportfraud.ftc.gov/. Za posamezne pritožbe v zvezi z načeli DPF EU-ZDA pa je morda najpriročnejše, da posamezniki iz EU predložijo pritožbe organu za varstvo podatkov v svoji državi članici ali drugemu neodvisnemu organu za reševanje sporov.

([14]) Člen 45(m) naslova 15 zakonodajne zbirke ZDA; člen 1.98 zbirke zveznih predpisov št. 16. Ta znesek se redno prilagaja glede na inflacijo.

([15]) Lani je FTC glasoval za poenostavitev postopka preiskovanja večkratnih storilcev. Glej sporočilo za medije „*FTC Authorizes Investigations into Key Enforcement Priorities*“ (FTC dovoljuje preiskave ključnih prednostnih nalog na področju kazenskega pregona) (1. julij 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) Glej *FTC, Privacy Shield* (FTC, zasebnostni ščit), https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Sodelovanje z organi EU za varstvo podatkov na področju kazenskega pregona**

FTC priznava pomembno vlogo, ki jo imajo organi EU za varstvo podatkov glede skladnosti z načeli DPF EU-ZDA, in spodbuja okrepljeno posvetovanje in sodelovanje na področju kazenskega pregona. Usklajen pristop k izzivom, ki jih predstavljajo trenuten razvoj na digitalnem trgu in podatkovno intenzivni poslovni modeli, je dejansko čedalje bolj ključen. FTC bo izmenjevala 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 FTC. FTC bo organu, ki predloži zadevo, zagotovil tudi povratne informacije o vrstah predložitev, ki jih prejme, da bi povečal učinkovitost prizadevanj za obravnavo nezakonitega ravnanja. Če organ pregona, ki predloži zadevo, zahteva informacije o statusu posamezne predložene zadeve za namene izvajanja lastnega izvršilnega postopka, bo FTC odgovoril, pri tem pa upošteval število predloženih zadev v obravnavi, zaupnost in druge zakonske zahteve.

FTC bo prav tako tesno sodeloval z organi EU za varstvo podatkov, da bi zagotovil pomoč pri kazenskem pregonu. 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 FTC dovoljuje, da tujim organom kazenskega pregona nudi pomoč, kadar tuji organ izvršuje zakone, ki prepovedujejo ravnanje, ki je po vsebini precej podobno ravnanju, prepovedanemu z zakoni, ki jih izvaja FTC ([17]). V okviru te pomoči lahko FTC izmenjuje informacije, pridobljene v zvezi z lastno preiskavo, izda prisilni postopek v imenu organa EU za varstvo podatkov, ki izvaja lastno preiskavo, in poišče ustna pričevanja prič ali obtoženih v zvezi z izvršilnim postopkom organa za varstvo podatkov v skladu z zahtevami ameriškega zakona o spletni varnosti. FTC redno uporablja to pooblastilo za pomoč drugim organom po svetu v zadevah glede varstva zasebnosti in potrošnikov.

Poleg morebitnih posvetov z organi EU za varstvo podatkov v zvezi s posameznimi zadevami, ki jih predložijo ti organi, bo FTC sodeloval na rednih srečanjih z imenovanimi predstavniki EOVP, kjer bodo na splošno obravnavani načini za izboljšanje sodelovanja. FTC bo skupaj s predstavniki Ministrstva za trgovino ZDA, Evropske komisije in predstavniki EOVP sodeloval tudi pri rednem pregledu DPF EU-ZDA, kjer bo obravnavano njegovo izvajanje. FTC spodbuja tudi razvoj orodij, ki bodo okrepila sodelovanje pri kazenskem pregonu z organi EU za varstvo podatkov in drugimi organi za uveljavljanje varstva zasebnosti po svetu. FTC z veseljem potrjuje svojo zavezo uveljavljanju vidikov trgovinskega sektorja v DPF EU-ZDA. Naše partnerstvo s kolegi iz EU je po našem mnenju ključen del zagotavljanja varstva zasebnosti naših in vaših državljanov.

S spoštovanjem,

Lina M. KHAN
predsedujoča Zvezni komisiji za trgovino

([17]) Pri ugotavljanju, ali uveljaviti svoje pooblastilo na podlagi ameriškega zakona o spletni varnosti, FTC 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 izvrševanje zakonov o konkurenci.

Dodatek A

Uveljavljanje zasebnostnega ščita in varnega pristana

	Opravilna št./Št. spisa Zvezne komisije za trgovino ZDA (*Federal Trade Commission*, v nadaljnjem besedilu: FTC)	**Zadeva**	**Povezava**
1	Št. spisa FTC 2023062 Št. zadeve 3:22-cv-03070 (severno okrožje Kalifornije)	ZDA/**Twitter, Inc.**	Twitter
2	Št. spisa FTC 192 3209	v zadevi Residual Pumpkin Entity, LLC, subjekt prej posloval kot **CafePress**, in PlanetArt, LLC, posluje kot **CafePress**	CafePress
3	Št. spisa FTC 192 3133 Opravilna št. C-4747	v zadevi **Flo Health, Inc.**	Flo Health
4	Št. spisa FTC 192 3050 Opravilna št. C-4723	v zadevi **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	Št. spisa FTC 192 3092 Opravilna št. C-4709	v zadevi **T&M Protection, LLC**	T&M Protection
6	Št. spisa FTC 192 3084 Opravilna št. C-4704	v zadevi **TDARX, Inc.**	TDARX
7	Št. spisa FTC 192 3093 Opravilna št. C-4706	v zadevi **Global Data Vault, LLC**	Global Data
8	Št. spisa FTC 192 3078 Opravilna št. C-4703	v zadevi **Incentive Services, Inc.**	Incentive Services
9	Št. spisa FTC 192 3090 Opravilna št. C-4705	v zadevi **Click Labs, Inc.**	Click Labs
10	Št. spisa FTC 182 3192 Opravilna št. C-4697	v zadevi **Medable, Inc.**	Medable
11	Št. spisa FTC 182 3189 Opravilna št. 9386	v zadevi NTT Global Data Centers Americas, Inc., kot naslednica pravnega interesa **RagingWire Data Centers, Inc.**	RagingWire
12	Št. spisa FTC 182 3196 Opravilna št. C-4702	v zadevi **Thru, Inc.**	Thru
13	Št. spisa FTC 182 3188 Opravilna št. C-4698	v zadevi **DCR Workforce, Inc.**	DCR Workforce
14	Št. spisa FTC 182 3194 Opravilna št. C-4700	v zadevi **LotaData, Inc.**	LotaData
15	Št. spisa FTC 182 3195 Opravilna št. C-4701	v zadevi **EmpiriStat, Inc.**	EmpiriStat

16	Št. spisa FTC 182 3193 Opravilna št. C-4699	v zadevi 214 Technologies, Inc., ki posluje tudi kot **Trueface.ai**	Trueface.ai
17	Št. spisa FTC 182 3107 Opravilna št. 9383	v zadevi **Cambridge Analytica, LLC**	Cambridge Analytica
18	Št. spisa FTC 182 3152 Opravilna št. C-4685	v zadevi **SecureTest, Inc.**	SecurTest
19	Št. spisa FTC 182 3144 Opravilna št. C-4664	v zadevi **VenPath, Inc.**	VenPath
20	Št. spisa FTC 182 3154 Opravilna št. C-4666	v zadevi **SmartStart Employment Screening, Inc.**	SmartStart
21	Št. spisa FTC 182 3143 Opravilna št. C-4663	v zadevi **mResourceLLC,** posluje kot Loop Works LLC	mResource
22	Št. spisa FTC 182 3150 Opravilna št. C-4665	v zadevi **Idmission LLC**	IDmission
23	Št. spisa FTC 182 3100 Opravilna št. C-4659	v zadevi **ReadyTech Corporation**	ReadyTech
24	Št. spisa FTC 172 3173 Opravilna št. C-4630	v zadevi **Decusoft, LLC**	Decusoft
25	Št. spisa FTC 172 3171 Opravilna št. C-4628	v zadevi **Tru Communication, Inc.**	Tru
26	Št. spisa FTC 172 3172 Opravilna št. C-4629	v zadevi **Md7, LLC**	Md7
30	Št. spisa FTC 152 3198 Opravilna št. C-4543	v zadevi **Jhayrmaine Daniels (posluje kot California Skate-Line)**	Jhayrmaine Daniels
31	Št. spisa FTC 152 3190 Opravilna št. C-4545	v zadevi **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32	Št. spisa FTC 152 3141 Opravilna št. C-4540	v zadevi **Golf Connect, LLC**	Golf Connect
33	Št. spisa FTC 152 3202 Opravilna št. C-4546	v zadevi **Inbox Group, LLC**	Inbox Group
34	Št. spisa 152 3187 Opravilna št. C-4542	v zadevi **IOActive, Inc.**	IOActive
35	Št. spisa FTC 152 3140 Opravilna št. C-4549	v zadevi **Jubilant Clinsys, Inc.**	Jubilant
36	Št. spisa FTC 152 3199 Opravilna št. C-4547	v zadevi **Just Bagels Manufacturing, Inc.**	Just Bagels

37	Št. spisa FTC 152 3138 Opravilna št. C-4548	v zadevi **NAICS Association, LLC**	NAICS
38	Št. spisa FTC 152 3201 Opravilna št. C-4544	v zadevi **One Industries Corp.**	One Industries
39	Št. spisa FTC 152 3137 Opravilna št. C-4550	v zadevi **Pinger, Inc.**	Pinger
40	Št. spisa FTC 152 3193 Opravilna št. C-4552	v zadevi **SteriMed Medical Waste Solutions**	SteriMed
41	Št. spisa FTC 152 3184 Opravilna št. C-4541	v zadevi **Contract Logix, LLC**	Contract Logix
42	Št. spisa FTC 152 3185 Opravilna št. C-4551	v zadevi **Forensics Consulting Solutions, LLC**	Forensics Consulting
43	Št. spisa FTC 152 3051 Opravilna št. C-4526	v zadevi **American Int'l Mailing, Inc.**	AIM
44	Št. spisa FTC 152 3015 Opravilna št. C-4525	v zadevi **TES Franchising, LLC**	TES
45	Št. spisa FTC 142 3036 Opravilna št. C-4459	v zadevi **American Apparel, Inc.**	American Apparel
46	Št. spisa FTC 142 3026 Opravilna št. C-4469	v zadevi **Fantage.com, Inc.**	Fantage
47	Št. spisa FTC 142 3017 Opravilna št. C-4461	v zadevi **Apperian, Inc.**	Apperian
48	Št. spisa FTC 142 3018 Opravilna št. C-4462	v zadevi **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49	Št. spisa FTC 142 3019 Opravilna št. C-4463	v zadevi **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50	Št. spisa FTC 142 3020 Opravilna št. C-4464	v zadevi **BitTorrent, Inc.**	BitTorrent
51	Št. spisa FTC 142 3022 Opravilna št. C-4465	v zadevi **Charles River Laboratories, Int'l**	Charles River
52	Št. spisa FTC 142 3023 Opravilna št. C-4466	v zadevi **DataMotion, Inc.**	DataMotion
53	Št. spisa FTC 142 3024 Opravilna št. C-4467	v zadevi **DDC Laboratories, Inc.**, posluje kot DNA Diagnostics Center	DDC
54	Št. spisa FTC 142 3028 Opravilna št. C-4470	v zadevi **Level 3 Communications, LLC**	Level 3

55	Št. spisa FTC 142 3025 Opravilna št. C-4468	v zadevi **PDB Sports, Ltd.**, posluje kot Denver Broncos Football Club, LLP	Broncos
56	Št. spisa FTC 142 3030 Opravilna št. C-4471	v zadevi **Reynolds Consumer Products, Inc.**	Reynolds
57	Št. spisa FTC 142 3031 Opravilna št. C-4472	v zadevi **Receivable Management Services Corporation**	Receivable Mgmt
58	Št. spisa FTC 142 3032 Opravilna št. C-4473	v zadevi **Tennessee Football, Inc.**	Tennessee Football
59	Št. spisa FTC 102 3058 Opravilna št. C-4369	v zadevi **Myspace LLC**	Myspace
60	Št. spisa FTC 092 3184 Opravilna št. C-4365	v zadevi **Facebook, Inc.**	Facebook
61	Št. spisa FTC 092 3081 Civilna tožba št. 09-CV-5276 (C.D. Cal.)	FTC/Javian Karnani, in **Balls of Kryptonite, LLC**, posluje kot Bite Size Deals, LLC, in Best Priced Brands, LLC	Balls of Kryptonite
62	Št. spisa FTC 102 3136 Opravilna št. C-4336	v zadevi **Google, Inc.**	Google
63	Št. spisa FTC 092 3137 Opravilna št. C-4282	v zadevi **World Innovators, Inc.**	World Innovators
64	Št. spisa FTC 092 3141 Opravilna št. C-4271	v zadevi **Progressive Gaitways LLC**	Progressive Gaitways
65	Št. spisa FTC 092 3139 Opravilna št. C-4270	v zadevi **Onyx Graphics, Inc.**	Onyx Graphics
66	Št. spisa FTC 092 3138 Opravilna št. C-4269	v zadevi **ExpatEdge Partners, LLC**	ExpatEdge
67	Št. spisa FTC 092 3140 Opravilna št. C-4281	v zadevi **Directors Desk LLC**	Directors Desk
68	Št. spisa FTC 092 3142 Opravilna št. C-4272	v zadevi **Collectify LLC**	Collectify

PRILOGA V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6. julij 2023

Komisar Didier Reynders
Evropska komisija
Rue de la Loi / Wetstraat 200
1049 Bruselj
Belgija

Spoštovani komisar Reynders,

Ministrstvo za promet ZDA (*Department of Transportation*, v nadaljnjem besedilu: ministrstvo za promet ali Ministrstvo) se zahvaljuje za priložnost, da opiše svojo vlogo pri uveljavljanju načel okvira za varstvo zasebnosti podatkov EU-ZDA. med EU in ZDA (v nadaljnjem besedilu DPF EU-ZDA). DPF EU-ZDA bo igral ključno vlogo pri varstvu osebnih podatkov, pridobljenih med trgovinskim poslovanjem v vedno bolj povezanem svetu. Podjetjem bo omogočil izvajanje pomembnih operacij v svetovnem gospodarstvu, obenem pa bo zagotovil, da potrošniki iz EU ohranijo pomembno varstvo zasebnosti.

Ministrstvo za promet je prvič javno izrazilo svojo zavezo uveljavljanju okvira varnega pristana med ZDA in EU v pismu, poslanem Evropski komisiji pred 22 leti, tj. zaveze, ponovljene in razširjene v pismu iz leta 2016 v zvezi z okvirom zasebnostnega ščita EU-ZDA. Ministrstvo za promet se je v teh dveh pismih zavezalo, da bo odločno uveljavljalo načela zasebnosti varnega pristana med ZDA in EU, nato pa načel zasebnostnega ščita EU-ZDA. Ministrstvo za promet razširja svojo zavezo na načela DPF EU-ZDA in jo zapisuje v tem pismu.

Ministrstvo za promet zlasti potrjuje svojo zavezo na naslednjih ključnih področjih: (1) prednostna obravnava preiskav domnevnih kršitev načel DPF EU-ZDA; (2) ustrezen kazenski pregon proti subjektom, ki lažno ali goljufivo navajajo, da sodelujejo v DPF EU-ZDA ter (3) spremljanje in javna objava izvršilnih odlokov v zvezi s kršitvami načel DPF EU-ZDA. Zagotavljamo informacije o vsaki od teh zavez in za potreben kontekst tudi ustrezno ozadje vloge ministrstva za promet pri varstvu zasebnosti potrošnikov in uveljavljanju načel DPF EU-ZDA.

1. **Ozadje**

A. Pooblastilo ministrstva za promet glede varstva zasebnosti

Ministrstvo je trdno zavezano zagotavljanju zasebnosti informacij, ki jih potrošniki dajo letalskim prevoznikom in agencijam za prodajo letalskih vozovnic.

Pooblastilo ministrstva za promet 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“ pri prodaji zračnega prevoza. Člen 41712 je oblikovan po členu 5 zakona o Zvezni komisiji za trgovino ZDA (Federal Trade Commission, v nadaljnjem besedilu FTC) (člen 45 naslova 15 zakonodajne zbirke ZDA).

Ministrstvo za promet je nedavno izdalo predpise, ki opredeljujejo nepošteno in goljufivo ravnanje ter so skladni z dosedanjo prakso ministrstva za promet in FTC (člen 399.79 poglavja 14 zakonika Združenih držav). Natančneje, ravnanje je „nepošteno“, če povzroči ali je verjetno, da bo povzročilo, bistveno škodo, ki se ji ni mogoče razumno izogniti in je ne odtehtajo ugodnosti za potrošnike ali konkurenco.

Ravnanje je „goljufivo“, če je verjetno, da bo zavedlo potrošnika, ki se vede razumno v danih okoliščinah v zvezi s pomembno zadevo. Zadeva je pomembna, če je verjetno, da je vplivala na potrošnikovo vedenje ali odločitev v zvezi s proizvodom ali storitvijo. Ministrstvo za promet poleg teh splošnih načel natančneje razlaga člen 41712 kot prepoved letalskim prevoznikom in agencijam za prodajo letalskih vozovnic, da: (1) kršijo pogoje svoje politike zasebnosti; (2) kršijo katero koli pravilo, ki ga izda Ministrstvo in ki določa posamezno ravnanje v zvezi varstvom zasebnosti kot nepošteno ali goljufivo ali (3) kršijo zakon COPPA ali pravila FTC, ki izvajajo zakon COPPA ali (4) kot udeleženec v DPF EU-ZDA ne izpolnjujejo načel DPF EU-ZDA ([1]).

Kot je bilo že navedeno, ima v skladu z zveznim zakonom ministrstvo za promet 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 s FTC.

Ko se prevoznik ali prodajalec zračnega prevoza javno zaveže načelom DPF EU-ZDA, lahko Ministrstvo kot tako uporabi zakonske pristojnosti iz člena 41712 za zagotovitev skladnosti z navedenimi načeli. Ko torej potnik zagotovi podatke letalskemu prevozniku ali agenciji za prodajo letalskih vozovnic, ki se je zavezal/-a načelom DPF EU-ZDA, vsako neizpolnjevanje teh načel letalskega prevoznika ali agencije za prodajo letalskih vozovnic pomeni kršitev člena 41712.

B. Prakse izvrševanja

Urad za varstvo potrošnikov v letalstvu (*Office of Aviation Consumer Protection*, v nadaljnjem besedilu: OACP) ([2]) v okviru Ministrstva opravlja preiskave in pregon po členu 41712 naslova 49 zakonodajne zbirke ZDA zakonodajne zbirke ZDA zakonodajne zbirke ZDA 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 spletišču ministrstva za promet ([3]).

Če v zadevi ni dosežena razumna in ustrezna rešitev, ima OACP pristojnost, da uvede izvršilni postopek, ki vključuje predhodno obravnavo pred upravnim sodnikom ministrstva za promet. Upravni sodnik je pooblaščen za izdajo odlokov o prepovedi in naložitev. Posledica kršitev člena 41712 je lahko izdaja odloka o prepovedi ter naložitev denarne kazni v višini do 37 377 USD 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 OACP in ki neposredno koristijo potrošnikom (npr. gotovina, dobropisi), 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 DPF EU-ZDA, 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 dejavnosti, in torej z izgubo pooblastila za opravljanje gospodarske dejavnosti.

Do danes je ministrstvo za promet 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 med zagotavljanjem 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.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Prej znan kot Urad za izvrševanje in postopke v letalstvu (Office of Aviation Enforcement and Proceedings).
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

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 načel DPF EU-ZDA**

Če se letalski prevoznik ali agencija za prodajo letalskih vozovnic odloči sodelovati v DPF EU-ZDA in Ministrstvo prejme pritožbo, da je tak letalski prevoznik ali taka agencija za prodajo letalskih vozovnic domnevno kršil/-a načela DPF EU-ZDA, Ministrstvo sprejme naslednje ukrepe za odločno uveljavljanje načel DPF EU-ZDA.

A. Prednostna obravnava preiskave domnevnih kršitev

OACP v okviru Ministrstva bo preiskal vsako pritožbo glede domnevnih kršitev DPF EU-ZDA, vključno s pritožbami, prejetimi od organov za varstvo podatkov EU, in uvedel pregon, kjer obstajajo dokazi o kršitvi.

Poleg tega bo OACP sodeloval s FTC in Ministrstvom za trgovino ZDA (*Department of Commerce*) ter prednostno obravnaval obtožbe, da regulirani subjekti ne izpolnjujejo zavez v zvezi z varstvom zasebnosti, ki so jih sprejeli v skladu z DPF. EU-ZDA.

Ob prejemu obtožbe glede kršitve načel DPF EU-ZDA lahko OACP sprejme različne ukrepe v sklopu svoje preiskave. Na primer, pregleda lahko politike 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 mu 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 ZDA ali FTC, in ocenilo, ali bi bilo izobraževanje potrošnikov in podjetij koristno, ter po potrebi uvedlo pregon.

Če Ministrstvo izve za morebitne kršitve načel DPF EU-ZDA s strani agencij za prodajo letalskih vozovnic, bo zadevo uskladilo s FTC. O izidu morebitnega pregona v zvezi z načeli DPF EU-ZDA bomo obvestili FTC in Ministrstvo za trgovino ZDA.

B. Obravnavanje lažnih ali goljufivih navedb o sodelovanju

Ministrstvo ostaja zavezano preiskovanju kršitev načel DPF EU-ZDA, vključno z lažnimi ali goljufivimi navedbami o članstvu v DPF EU-ZDA. Prednostno bomo obravnavali zadeve, ki jih predloži Ministrstvo za trgovino ZDA v zvezi z organizacijami, za katere je ugotovilo, da se neustrezno predstavljajo kot člani DPF EU-ZDA ali brez dovoljenja uporabljajo certifikacijsko oznako DPF EU-ZDA.

Poleg tega opozarjamo, da če politika zasebnosti organizacije obljublja, da spoštuje načela DPF EU-ZDA, in organizacija ne opravi (ponovnega) samocertificiranja pri Ministrstvu za trgovino ZDA, to samo po sebi verjetno ne odvezuje organizacije od uveljavljanja teh zavez s strani ministrstva za promet.

C. Spremljanje in javna objava izvršilnih odlokov v zvezi s kršitvami načel DPF EU-ZDA

OACP v okviru Ministrstva se še naprej zavezuje, da bo spremljal izvršilne odloke, kakor so potrebni za zagotavljanje skladnosti z načeli DPF EU-ZDA. Zlasti, če urad izda odlok, ki letalskemu prevozniku ali agenciji za prodajo letalskih vozovnic prepoveduje nadaljnje kršitve načel DPF EU-ZDA in člena 41712, bo spremljal subjektovo izpolnjevanje določbe o prepovedi v odloku. Poleg tega bo urad zagotovil, da bodo odloki, ki izhajajo iz zadev v zvezi z načeli DPF EU-ZDA, na voljo na njegovem spletišču.

Veselimo se nadaljnjega dela z našimi zveznimi partnerji in deležniki iz EU v zadevah DPF EU-ZDA.

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,

Pete BUTTIGIEG

ANNEX VI

U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General Washington, D.C. 20530

23. junija 2023

Ana Gallego Torres
generalna direktorica za pravosodje in potrošnike
Evropska komisija
Rue Montoyer/Montoyerstraat 59
1049 Bruselj
Belgija

Spoštovana generalna direktorica Gallego Torres:

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]). Vsi pravni procesi, opisani v tem pismu, so nediskriminatorni, saj so uporabljeni za pridobivanje informacij od korporacij v Združenih državah, vključno s podjetji, ki se bodo samocertificirala prek okvira za varstvo zasebnosti podatkov med EU in ZDA, ne glede na narodnost posameznika, na katerega se nanašajo podatki, ali njegov prebivališče. 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 „[p]ravica 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/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/United States, 389 U.S. str. 347 in 357 (1967). Standardi za izdajo naloga, kot so utemeljeni sum in zahteve po določnosti, se uporabljajo za naloge za fizične preiskave in zasege ter tudi za naloge za shranjene vsebine elektronskih komunikacij, izdane na podlagi zakona o shranjenih komunikacijah (*Stored Communications Act*), kakor je navedeno spodaj. Kadar zahteva naloga ne velja, je vladna dejavnost še vedno

([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, 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; člen 3162 naslova 50 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 (*Foreign Intelligence Surveillance Act*), člen 1801 naslova 50 zakonodajne zbirke ZDA in naslednji.

([2]) To pismo 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 dodatno varstvo, ki ga zagotavljajo ustave držav ali zakoni in ki presega določbe v Ustavi ZDA. Varstvo državnih zakonov mora biti vsaj enakovredno varstvu Ustave ZDA, med drugim tudi četrtemu amandmaju.

podvržena preskusu „razumnosti“ v skladu s četrtim amandmajem. Sama Ustava torej zagotavlja, da vlada ZDA nima neomejene ali samovoljne moči, da zaseže zasebne informacije ([3]).

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 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 preiskovalni organ sodišča, ki ga sodnik ali sodnik nižjega sodišča vključi v poroto. V sodnem pozivu se lahko od osebe zahteva, da priča v postopku ali predloži ali zagotovi poslovne evidence, elektronsko shranjene informacije ali druge stvarne 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. str. 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 upravnih 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 stvarnih predmetov, pomembnih za preiskave 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 tekočo kazensko preiskavo. Glej člene 3121 do 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*, v nadaljnjem besedilu: ECPA): vladni dostop do informacij o naročnikih, podatkov o prometu in shranjenih vsebin komunikacij, ki jih hranijo ponudniki internetnih storitev (znani tudi kot ISP), telefonska podjetja in drugi tretji ponudniki storitev, urejajo dodatna pravila v skladu z naslovom II ECPA, imenovanem tudi zakon o shranjenih komunikacijah (*Stored Communications Act*, v nadaljnjem besedilu: 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 internetnega protokola (IP) in povezane časovne žige ter izpolnjene podatke za obračunavanje morajo organi kazenskega pregona pridobiti sodni poziv. Za večino drugih

([3]) V zvezi z načeli četrtega amandmaja o zaščiti interesov za varstvo zasebnosti in varnosti, navedenih zgoraj, sodišča ZDA redno uporabljajo navedena načela za nove vrste preiskovalnih orodij kazenskega pregona, ki jih omogočata razvoj in tehnologija. Leta 2018 je vrhovno sodišče na primer odločilo, da je pridobitev informacij o historičnih lokacijskih podatkih baznih postaj za daljše časovno obdobje s strani vlade od podjetja mobilne telefonije v kazenski preiskavi „iskanje“, ki je predmet zahteve naloga na podlagi četrtega amandmaja. Carpenter proti ZDA, 138 S. Ct. 2206 (2018).

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 komunikacijorgani kazenskega pregona na splošno pridobijo nalog od sodnika na podlagi utemeljenega suma, da zadevni račun vsebuje dokaze o kaznivem dejanju. SCA določa tudi civilno odgovornost in kazenske sankcije ([4]).

Sodni nalogi 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 do 2523 naslova 18 zakonodajne zbirke ZDA. To pooblastilo je na voljo le v skladu s sodnim nalogom, v katerem 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 določa civilno odgovornost in kazenske sankcije za kršitve določb glede prisluškovanja telefonskim pogovorom.

Nalog za preiskavo – zvezna pravila o kazenskem postopku, 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. Oseba, ki se preišče ali katere lastnina se preišče, lahko poskuša doseči, da se dokazi, predloženi zoper njo med kazenskim postopkom, ki so bili pridobljeni ali izhajajo iz nezakonite preiskave, izločijo. Glej Mapp/Ohio, 367 U.S. 643 (1961). Če se od imetnika podatkov zahteva, naj v skladu z nalogom razkrije podatke, lahko stranka, od katere se zahteva sodelovanje, zahtevo po razkritju izpodbija kot neupravičeno obremenitev. Glej zadevo Vloga Združenih držav, 610 F.2d 1148, 1157 (pritožbeno sodišče tretjega okrožja Združenih držav Amerike 1979) (z odločitvijo, da „dolžno pravno postopanje zahteva obravnavo vprašanja o obremenjenosti, preden se telefonskemu podjetju z nalogom za preiskavo naloži obveznost zagotavljanja“ pomoči); zadevo Vloga Združenih držav, 616 F.2d 1122 (pritožbeno sodišče devetega okrožja Združenih držav Amerike 1980) (z enako ugotovitvijo na podlagi nadzornega organa sodišča).

Smernice in politike Ministrstva za pravosodje ZDA: poleg teh ustavnih in zakonskih omejitev na podlagi pravil glede vladnega dostopa do podatkov je pravosodni minister 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 pravosodnega ministra za domače operacije FBI (september 2008) (*Attorney General's Guidelines for Domestic FBI Operations*, v nadaljnjem besedilu: smernice AG FBI), na voljo na naslovu 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*, v nadaljnjem besedilu: DIOG), na voljo na naslovu https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29, 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 pravosodje (*Justice Manual*), prav tako na voljo na naslovu https://www.justice.gov/jm/justicemanual.

Civilni in regulativni organi (javni interes):

([4]) Poleg tega člen 2705(b) SCA na vlado prenaša pooblastilo, da na podlagi dokazane potrebe po zaščiti pred razkritjem pridobi sodno odločbo, ki ponudniku komunikacijskih storitev prepoveduje, da bi svoje uporabnike prostovoljno obveščal o vročitvi sodnega postopka na podlagi SCA. Oktobra 2017 je namestnik pravosodnega ministra Rod Rosenstein pravobranilcem in agentom pri Ministrstvu za pravosodje ZDA izdal memorandum, ki določa smernice za zagotovitev, da so vloge za take odredbe o zaščiti prilagojene konkretnim dejstvom in zadevam preiskave, ter splošno enoletno zgornjo mejo trajanja odloga obvestila, ki ga je mogoče zahtevati z vlogo. Maja 2022 je namestnica pravosodnega ministra Lisa Monaco izdala dopolnilne smernice o tej temi, ki med drugim zadeva vzpostavljene notranje zahteve Ministrstva za pravosodje ZDA glede odobritve vlog za podaljšanje odredbe o zaščiti za več kot prvotno enoletno obdobje, in zahtevala prenehanje odredb o zaščiti ob zaključku preiskave.

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 stvarne 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 zvezna pravila o civilnem postopku 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. Člen 5318 naslova 31 zakonodajne zbirke ZDA; zbirka zveznih predpisov št. 31, poglavje 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 do 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 na podlagi četrtega amandmaja. Glej See/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 pravosodnega ministra, 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.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

PRILOGA VII

URAD GLAVNE SVETOVALKE URADA DIREKTORJA NACIONALNE OBVEŠČEVALNE SLUŽBE

WASHINGTON, D.C. 20511

9. december 2022

Leslie B. Kiernan,
glavna svetovalka
Ministrstva za trgovino ZDA
(*Department of Commerce*), 1401 Constitution Ave.,
NW Washington, D.C. 20230

Spoštovana gospa Kiernan,

dne 7. oktobra 2022 je predsednik Joe Biden podpisal Odredbo št. 14086 z naslovom „Enhancing Safeguards for United States Signals Intelligence Activities“ (Krepitev zaščitnih ukrepov za obveščevalne dejavnosti SIGINT ZDA), ki spodbuja niz strogih zaščitnih ukrepov za varstvo zasebnosti in državljanskih svoboščin, ki veljajo za obveščevalne dejavnosti SIGINT ZDA. Ti zaščitni ukrepi vključujejo: zahtevo, da obveščevalne dejavnosti SIGINT izpolnjujejo izrecno navedene zakonite cilje; izrecno prepoved izvajanja takih dejavnosti za namene posebnih prepovedanih ciljev; uvedbo novih postopkov za zagotovitev, da obveščevalne dejavnosti SIGINT podpirajo te zakonite cilje in ne podpirajo prepovedanih ciljev; zahtevo, da se obveščevalne dejavnosti SIGINT izvajajo le po odločitvi, ki temelji na razumni presoji vseh ustreznih dejavnikov, da so dejavnosti potrebne za izboljšanje potrjenih prednostnih nalog obveščevalnih služb, in le v obsegu in na način, ki je sorazmeren s potrjenimi prednostnimi nalogami obveščevalnih služb, za katere so bile dovoljene, in navodilo organom obveščevalne skupnosti, da posodobijo svoje politike in postopke tako, da bodo izražali zaščitne ukrepe za obveščevalne dejavnosti SIGINT, ki jih zahteva Odredba. Najpomembneje, Odredba uvaja tudi neodvisen in zavezujoč mehanizem, ki posameznikom iz „držav, ki izpolnjujejo pogoje“, kot jih opredeljuje Odredba, omogoča, da uveljavljajo pravna sredstva, če menijo, da so bili predmet nezakonitih ameriških obveščevalnih dejavnosti SIGINT, vključno z dejavnostmi, ki kršijo varstvo, ki ga zagotavlja Odredba.

Izdaja Odredbe št. 14086 predsednika Joeja Bidena je predstavljala vrhunec več kot leto dni trajajočih izčrpnih pogajanj med predstavniki iz Evropske komisije (EK) in Združenih držav ter usmerja ukrepe, ki jih bodo Združene države sprejele za izvajanje svojih zavez na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA. V duhu sodelovanja, ki je rezultat okvira, ste, če sem prav obveščen, od EK prejeli dva sklopa vprašanj o tem, kako bo obveščevalna skupnost izvajala Odredbo. Na ta vprašanja z veseljem odgovarjam v tem pismu.

Člen 702 zakona o nadzoru tujih obveščevalnih podatkov iz leta 1978 (Foreign Intelligence Surveillance Act of 1978, v nadaljnjem besedilu: člen 702 FISA)

Prvi sklop vprašanj se nanaša na člen 702 FISA, ki omogoča zbiranje tujih obveščevalnih podatkov s ciljnim osredotočanjem na nedržavljane ZDA, za katere se utemeljeno sklepa, da se nahajajo zunaj Združenih držav, ob zavezujoči pomoči ameriških ponudnikov storitev elektronskih komunikacij. Natančneje, vprašanja se nanašajo na medsebojni vpliv navedene določbe in Odredbe št. 14086, pa tudi drugih zaščitnih ukrepov, ki veljajo za dejavnosti, ki se izvajajo v skladu s členom 702 FISA.

Za začetek lahko potrdimo, da bo obveščevalna skupnost zaščitne ukrepe iz Odredbe št. 14086 uporabljala za dejavnosti, ki se izvajajo v skladu s členom 702 FISA.

Poleg tega se številni drugi zaščitni ukrepi uporabljajo za vladno uporabo člena 702 FISA. Vsa potrdila na podlagi člena 702 FISA morata na primer podpisati pravosodni minister in direktor nacionalne obveščevalne službe (*Director of National Intelligence*, v nadaljnjem besedilu: DNI), vlada pa mora vsa taka potrdila predložiti v odobritev sodišču za nadzor tujih obveščevalnih podatkov (*Foreign Intelligence Surveillance Court*, v nadaljnjem besedilu: FISC), ki ga sestavljajo neodvisni sodniki s trajnimi, neobnovljivimi mandati za obdobja, razporejena čez sedem let. V potrdilih so opredeljene kategorije tujih obveščevalnih podatkov, ki se zbirajo s ciljnim osredotočanjem na nedržavljane ZDA, za katere se utemeljeno sklepa, da se nahajajo zunaj Združenih držav, in morajo izpolnjevati zakonsko opredelitev tujih obveščevalnih podatkov. Potrdila morajo vključevati informacije, ki se nanašajo na mednarodni terorizem in druge teme, kot je pridobivanje informacij v zvezi z orožjem za množično uničevanje. Vsako letno potrdilo mora biti predloženo FISC v odobritev v svežnju vlog za izdajo potrdil, ki vključuje potrdili pravosodnega ministra in DNI, izjave vodij obveščevalnih agencij in postopke izbire cilja, zmanjševanja in poizvedovanja, ki so za vlado zavezujoči. Postopki izbire cilja med drugih zahtevajo, da obveščevalna skupnost na podlagi vseh okoliščin razumno oceni, ali obstaja verjetnost, da bo bodo z izbiro cilja zbrani tuji obveščevalni podatki, opredeljeni v potrdilu na podlagi člena 702 FISA.

Poleg tega mora obveščevalna skupnost pri zbiranju informacij v skladu s členom 702 FISA: na podlagi svoje ocene v času izbire cilja predložiti pisno pojasnitev, da se pričakuje, da bo ciljna oseba posedovala, prejela ali verjetno sporočala tuje obveščevalne podatke, opredeljene v potrdilu iz člena 702 FISA; potrditi, da je standardu izbire cilja, kakor je določen v postopkih izbire cilja na podlagi člena 702 FISA, še vedno zadoščeno in končati zbiranje, če standardu ni več zadoščeno. Glej vlogo vlade ZDA, predloženo FISC, „*2015 Summary of Notable Section 702 Requirements*“ (Povzetek pomembnejših zahtev na podlagi člena 702 iz leta 2015), na str. 2 in 3 (15. julij 2015).

Zahteva, da obveščevalna skupnost pisno evidentira svojo oceno, da cilji na podlagi člena 702 FISA zadoščajo veljavnim standardom izbire cilja, in redno potrjuje njeno veljavnost, olajšuje nadzor obveščevalnih dejavnosti obveščevalne skupnosti s strani FISA. Vsako evidentirano oceno izbire cilja in razloge vsaka dva meseca pregledajo državni tožilci pri Ministrstvu za pravosodje ZDA (*Department of Justice*, v nadaljnjem besedilu: ministrstvo za pravosodje) za nadzor obveščevalnih dejavnosti, ki izvaja to nadzorno funkcijo neodvisno od tujih obveščevalnih dejavnosti. Oddelek ministrstva za pravosodje, ki izvaja to funkcijo, je nato na podlagi že dolgo določenega pravila FISC, pristojen za poročanje FISC o vseh kršitvah veljavnih postopkov. Skupaj z rednimi srečanji med FISC in tem oddelkom ministrstva za pravosodje v zvezi z nadzorom izbire cilja na podlagi člena 702 to poročanje FISC omogoča, da uveljavi skladnost s postopki izbire cilja in drugimi postopki na podlagi člena 702 FISA ter zagotovi zakonitost vladnih dejavnosti. Zlasti lahko FISC to stori na številne načine, tudi z izdajo zavezujočih sklepov o odpravi kršitve za odvzem vladnega pooblastila za zbiranje podatkov določene ciljne osebe ali za spremembo ali odlog zbiranja podatkov na podlagi člena 702 FISA. FISC lahko od vlade tudi zahteva, naj predloži nadaljnja poročila ali obvestila o svojem spoštovanju postopkov izbire cilja in drugih postopkov, ali zahteva spremembo navedenih postopkov.

„Množično“ zbiranje obveščevalnih podatkov v okviru SIGINT

Drugi sklop vprašanj se nanaša na „množično“ zbiranje obveščevalnih podatkov v okviru SIGINT, ki je v Odredbi št. 14086 opredeljeno kot „pooblaščeno zbiranje velikih količin obveščevalnih podatkov v okviru SIGINT, ki se iz tehničnih ali operativnih razlogov pridobivajo brez uporabe diskriminant (npr. brez uporabe posebnih identifikatorjev ali izbirnih izrazov)“.

V zvezi s temi vprašanji najprej opozarjamo, da niti FISA niti sodni pozivi v zvezi z nacionalno varnostjo ne dovoljujejo množičnega zbiranja. V zvezi s FISA:

— naslova I in III FISA, ki dovoljujeta elektronski nadzor oziroma fizične preiskave, zahtevata sodno odločbo (z omejenimi izjemami, kot so izredne razmere) in vedno zahtevata utemeljen sum, da je cilj tuja sila ali agent tuje sile. Glej člen 1805 in člen 1824 naslova 50 zakonodajne zbirke ZDA.

— Z zakonom ZDA o svobodi iz leta 2015 (*USA FREEDOM Act of 2015*) je bil spremenjen naslov IV FISA, ki dovoljuje uporabo snemalnikov klicev ter naprav za pasti in sledenje v skladu s sodno odločbo (razen v izrednih razmerah), da bi se od vlade zahtevala utemeljitev zahtev na podlagi „posebnega izbirnega izraza“. Glej člen 1842(c)(3) naslova 50 zakonodajne zbirke ZDA.

— Naslov V FISA, ki FBI dovoljuje pridobivanje nekaterih vrst poslovnih evidenc, zahteva sodno odločbo na podlagi vloge, v kateri je navedeno, da „obstajajo konkretna in utemeljena dejstva, ki upravičujejo razlog za sum, da je oseba, na katero se nanašajo evidence, tuja sila ali agent tuje sile.“ Glej tudi člen 1862(b)(2)(B) naslova 50 zakonodajne zbirke ZDA ([1]).

— Nazadnje, člen 702 FISA dovoljuje „ciljno osredotočanje na osebe, za katere se utemeljeno sklepa, da se nahajajo zunaj ZDA, za pridobitev tujih obveščevalnih podatkov“. Glej člen 1881a(a) naslova 50 zakonodajne zbirke ZDA. Kot je opozoril odbor za nadzor zasebnosti in državljanskih svoboščin (*Privacy and Civil Liberties Oversight Board*), vladno zbiranje podatkov na podlagi člena 702 FISA torej „v celoti sestavljata izbira posameznih ciljni oseb in pridobivanje komunikacij v zvezi s tistimi osebami, od katerih si vlada utemeljeno obeta pridobitev nekaterih vrst tujih obveščevalnih podatkov“ tako, da se „program ne izvaja z množičnim zbiranjem komunikacij“. Odbor za nadzor zasebnosti in državljanskih svoboščin, „*Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*“ (Poročilo o programu nadzora, ki se izvaja v skladu s členom 702 zakona o nadzoru tujih obveščevalnih podatkov), na str. 103 (2. julij 2014) ([2]).

Kar zadeva sodne pozive v zvezi z nacionalno varnostjo, zakon ZDA o svobodi iz leta 2015 za uporabo takih pozivov nalaga obveznost „posebnega izbirnega izraza“. Glej člen 3414(a)(2) naslova 12 zakonodajne zbirke ZDA; člen 1681u naslova 15 zakonodajne zbirke ZDA; člen1681v(a) naslova 15 zakonodajne zbirke ZDA; člen 2709(b) naslova 18 zakonodajne zbirke ZDA.

Poleg tega Odredba št. 14086 določa, da je „[ciljno] usmerjeno zbiranje prednostna naloga“, in da če obveščevalna skupnost izvaja množično zbiranje, je „množično zbiranje obveščevalnih podatkov v okviru SIGINT dovoljeno le na podlagi ugotovitve […], da informacij, potrebnih za izboljšanje potrjenih prednostnih nalog obveščevalnih služb, ni mogoče pod razumnimi pogoji pridobiti s ciljno usmerjenim zbiranjem“. Glej člen 2(c)(ii)(A) Odredbe št. 14086.

Poleg tega, ko obveščevalna skupnost ugotovi, da množično zbiranje zadošča standardom, Odredba št. 14086 določa dodatne zaščitne ukrepe. Natančneje, v skladu z Odredbo se od obveščevalne skupnosti zahteva, da pri izvajanju množičnega zbiranja „uporablja razumne metode in tehnične ukrepe za omejitev zbranih podatkov le na tisto, kar je potrebno za izboljšanje potrjenih prednostnih nalog obveščevalnih služb.“ Glej prav tam. Odredba prav tako določa, da se „obveščevalne dejavnosti SIGINT“, ki vključujejo poizvedovanje po obveščevalnih podatkih v okviru SIGINT, pridobljene z množičnim zbiranjem, izvajajo le po ugotovitvi, ki temelji na razumni presoji vseh ustreznih dejavnikov, da so dejavnosti potrebne za izboljšanje potrjenih prednostnih nalog obveščevalnih služb.“ Glej prav tam, člen 2(a)(ii)(A). Odredba poleg tega to načelo izvaja z določbo, da lahko obveščevalna skupnost poizveduje le po nezmanjšani količini obveščevalnih podatkov v okviru SIGINT, ki so množično pridobljeni v skladu s šestimi dopustnimi cilji, in da je treba take poizvedbe opravljati v skladu s politikami in postopki, pri katerih se „ustrezno upošteva vpliv [poizvedb] na varstvo zasebnosti in državljanskih svoboščin vseh oseb ne glede na njihovo državljanstvo ali prebivališče“. Glej prav tam, člen 2(c)(iii)(D). Nazadnje, Odredba določa nadzor nad ravnanjem z zbranimi podatki, njihovo varnostjo in dostopom do njih. Glej prav tam, člen 2(c)(iii)(A) in člen 2(c)(iii)(B).

* * * * *

Upamo, da so ta pojasnila v pomoč. Če imate dodatna vprašanja, kako namerava obveščevalna skupnost ZDA izvajati Odredbo št. 14086, se brez oklevanja obrnite na nas.

([1]) Od leta 2001 do leta 2020 je naslov V FISA FBI dovoljeval, da od FISC zahteva dovoljenje za pridobitev „oprijemljivih predmetov“, pomembnih za nekatere odobrene preiskave. Glej člen 215 zakona o domovinski varnosti ZDA (*USA Patriot Act*), javno pravo, št. 107–56, 115 zakon 272 (2001). Ta ubeseditev, ki ji je potekla veljavnost in torej ni več zakon, je določala pooblastilo, v skladu s katerim je vlada nekoč množično zbirala telefonske metapodatke. Celo pred potekom veljavnosti določbe pa je bila z zakonom ZDA o svobodi spremenjena tako, da je od vlade zahtevala utemeljitev vloge FISC na podlagi „posebnega izbirnega izraza“. Glej člen I 03 zakona ZDA o svobodi, javno pravo, št. 114–23, 129 zakon 268 (2015).

([2]) Člen 703 in člen 704, ki obveščevalni skupnosti dovoljujeta izbiro ciljnih oseb, ki so državljani ZDA in se nahajajo v tujini, zahtevata sodno odločbo (razen v izrednih razmerah) in vedno zahtevata utemeljen sum, da je cilj tuja sila, agent tuje sile ali uradnik ali zaposleni tuje sile. Glej člen 1881b in člen 1881c naslova 50 zakonodajne zbirke ZDA.

Sincerely,

Christopher C. FONZONE,
Glavni svetovalec

PRILOGA VIII

Seznam okrajšav

V tem sklepu se uporabljajo naslednje okrajšave:

AAA	Ameriško združenje za arbitražo
Uredba pravosodnega ministra	Uredba pravosodnega ministra o ustanovitvi sodišča za presojo varstva podatkov
AGG-DOM	Smernice pravosodnega ministra za domače operacije FBI
APA	Zakon o upravnem postopku
CIA	Centralna obveščevalna agencija
CNSS	Odbor za sisteme nacionalne varnosti
Sodišče	Sodišče Evropske unije
Sklep	Izvedbeni sklep Komisije v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA
DHS	Ministrstvo za domovinsko varnost
DNI	direktor nacionalne obveščevalne službe
DoC	Ministrstvo za trgovino ZDA
DoJ	Ministrstvo za pravosodje ZDA
DoT	Ministrstvo za promet ZDA
DPA	Organ za varstvo podatkov
Seznam DPF	Seznam okvira o varstvu podatkov
DPRC	Sodišče za presojo varstva podatkov
ECOA	Zakon o enakih možnostih pridobitve posojila
ECPA	Zakon o zasebnosti elektronskih komunikacij
EGP	Evropski gospodarski prostor
Odredba št. 12333	Odredba št. 12333 „Obveščevalne dejavnosti ZDA“
Odredba št. 14086, Odredba	Odredba št. 14086 „Krepitev zaščitnih ukrepov za obveščevalne dejavnosti SIGINT ZDA“
DPF ali DPF EU-ZDA	Okvir za varstvo zasebnosti podatkov med EU in ZDA
Senat DPF EU-ZDA	Senat Okvira za varstvo zasebnosti podatkov med EU in ZDA
FBI	Zvezni preiskovalni urad
FCRA	Zakon o pravičnem poročanju o kreditni sposobnosti
FISA	Zakon o nadzoru tujih obveščevalnih podatkov
FISC	Sodišče za nadzor tujih obveščevalnih podatkov
FISCR	Prizivno sodišče za nadzor tujih obveščevalnih podatkov
FOIA	Zakon o dostopu do informacij javnega značaja
FRA	Zakon o evidencah zveznih agencij

FTC	Zvezna komisija ZDA za trgovino
HIPAA	Zakon o prenosu zdravstvenih podatkov in s tem povezani odgovornosti
ICDR	Mednarodno središče za reševanje sporov
IOB	Odbor za nadzor obveščevalnih podatkov
NIST	Nacionalni institut za standarde in tehnologijo
NSA	Agencija za nacionalno varnost
NSL	Sodni poziv(i) v zvezi z nacionalno varnostjo
ODNI	Urad direktorja nacionalne obveščevalne službe
ODNI CLPO, CLPO	Uradnik za varstvo zasebnosti in državljanskih svoboščin v okviru Urada direktorja nacionalne obveščevalne službe
OMB	Urad za upravljanje in proračun
OPCL	Urad za varstvo zasebnosti in državljanskih svoboščin Ministrstva za pravosodje
PCLOB	Odbor za nadzor zasebnosti in državljanskih svoboščin
PIAB	Predsedniški obveščevalni svetovalni odbor
PPD 28	Predsedniška politična direktiva št. 28
Uredba (EU) 2016/679	Uredba (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
SAOP	Višji uradnik agencije za področje zasebnosti
Načela	Načela okvira za varstvo zasebnosti podatkov med EU in ZDA
ZDA	Združene države
Unija	Evropska unija