EUROPSKA
KOMISIJA

Bruxelles, 9.10.2024.
COM(2024) 451 final

IZVJEŠĆE KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

o prvom periodičnom preispitivanju funkcioniranja odluke o primjerenosti okvira EU-a i SAD-a za privatnost podataka

1. PRVO PERIODIČNO PREISPITIVANJE – KONTEKST, PRIPREMA I POSTUPAK

U odluci od 10. srpnja 2023. („odluka o primjerenosti”) Komisija je utvrdila da okvir EU-a i SAD-a za privatnost podataka osigurava primjerenu razinu zaštite osobnih podataka koji se iz Europske unije prenose organizacijama u Sjedinjenim Američkim Državama[1]. Odlukom o primjerenosti propisano je da Komisija mora provoditi periodična preispitivanja, a prvo bi trebala provesti godinu dana od datuma dostave odluke o primjerenosti državama članicama. Ovo izvješće zaključuje prvo preispitivanje.

U skladu s uvodnom izjavom 211. odluke o primjerenosti ovo prvo preispitivanje, provedeno nakon prve godine primjene novog okvira, bilo je usmjereno na provjeru jesu li svi elementi predviđeni okvirom provedeni i funkcioniraju li učinkovito u praksi. Preispitivanje je obuhvatilo sve aspekte funkcioniranja okvira, među ostalim s obzirom na pravne promjene od donošenja odluke o primjerenosti.

U okviru priprema za preispitivanje Komisija je prikupila informacije od relevantnih dionika, posebno od nevladinih organizacija sa stručnim znanjem u području digitalnih prava i privatnosti[2], organizacija koje su certificirane u skladu s okvirom za privatnost podataka preko njihovih trgovinskih udruženja[3] i od američkih tijela uključenih u provedbu okvira. Nadalje, Komisija je prikupila i povratne informacije od šire javnosti u okviru posebnog poziva na očitovanje na portalu „Iznesite svoje mišljenje”[4].

Sastanak za preispitivanje održan je u Washingtonu 18. i 19. srpnja 2024. Otvorili su ga povjerenik EU-a za pravosuđe i zaštitu potrošača Didier Reynders i američka ministrica trgovine Gina Raimondo.[5]

Kad je riječ o EU-u, preispitivanje su proveli predstavnici Glavne uprave Europske komisije za pravosuđe i zaštitu potrošača te pet predstavnika koje je imenovao Europski odbor za zaštitu

[1] Provedbena odluka Komisije EU 2023/1795 od 10. srpnja 2023. u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenoj razini zaštite osobnih podataka u skladu s okvirom EU-a i SAD-a za privatnost podataka.

[2] Komisija je poslala upitnik devet nevladinih organizacija (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology) koji se prvenstveno odnosio na relevantne promjene pravnog okvira SAD-a, mehanizme nadzora i provedbe te funkcioniranje mehanizama pravne zaštite. Službe Komisije i predstavnici Europskog odbora za zaštitu podataka 9. srpnja 2024. održali su i internetski sastanak s tim nevladinim organizacijama.

[3] Komisija je poslala upitnik devet trgovinskih udruženja (Software & Information Industry Association, Gospodarska komora SAD-a, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine) koji se prvenstveno odnosio na iskustvo poduzeća certificiranih u skladu s okvirom EU-a i SAD-a za privatnost podataka, posebno na postupak certificiranja, radnje poduzete za usklađivanje s Načelima okvira za privatnost podataka, mehanizme za rješavanje zahtjeva i pritužbi pojedinaca itd.

[4] Primljene povratne informacije dostupne su na sljedećoj poveznici: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_hr

[5] Sastanak je organiziran je po temama, pri čemu je uvod u svaku posebnu točku dnevnog reda bilo kratko izlaganje nadležnog tijela SAD-a te predstavnika ili organizacije EU-a, nakon čega je uslijedio blok s detaljnim pitanjima i odgovorima. Prvi dan tema su bili „komercijalni aspekti” okvira (tj. primjena i provedba zahtjeva koji se odnose na poduzeća certificirana u skladu s okvirom za privatnost podataka), a drugi dan raspravljalo se o pitanjima povezanima s vladinim pristupom osobnim podacima.

podataka (EDPB), iz različitih nacionalnih tijela za zaštitu podataka i Europskog nadzornika za zaštitu podataka[6]. SAD su na preispitivanju zastupali predstavnici Ministarstva trgovine, Ministarstva vanjskih poslova, Savezne trgovinske komisije (FTC), Ministarstva prometa, Ureda direktora za nacionalna obavještajna pitanja (ODNI), Ministarstva pravosuđa, glavnog inspektora obavještajne zajednice te članovi Odbora za nadzor privatnosti i građanskih sloboda (PCLOB). Osim toga, predstavnici organizacija koje nude usluge neovisnog rješavanja sporova i Američko udruženje za arbitražu dostavili su informacije na relevantnim sastancima za preispitivanje. Nadalje, preispitivanje je dopunjeno informacijama iz izlaganja organizacija certificiranih u skladu s okvirom za privatnost podataka o tome kako se poduzeća usklađuju s obvezama definiranima okvirom.

Zaključci Komisije dodatno su dopunjeni informacijama iz javno dostupnih materijala, kao što su sudske odluke, provedbena pravila i postupci relevantnih američkih tijela, izvješća i studije nevladinih organizacija, izvješća o transparentnosti koja su izradila poduzeća certificirana u skladu s okvirom privatnost podataka, godišnja izvješća nadzornih tijela i medijska izvješća.

2. NALAZI

2.1. Komercijalni aspekti

2.1.1. Postupak certificiranja

Kako bi poduzeće iz SAD-a moglo primati osobne podatke iz EU-a na temelju okvira za privatnost podataka, mora se certificirati, a zatim svake godine ponovno certificirati, u skladu s posebnim zahtjevima zaštite podataka („načela okvira za privatnost podataka”). Da bi se poduzeće certificiralo, mora se podvrgnuti istražnim i provedbenim ovlastima FTC-a ili Ministarstva prometa, javno izjaviti da se obvezuje na usklađenost s Načelima okvira za privatnost podataka, objaviti svoju politiku zaštite privatnosti i u potpunosti provoditi te zahtjeve[7]. Prije dovršetka certificiranja Ministarstvo trgovine provjerava je li poduzeće ispunilo sve zahtjeve za certificiranje[8].

Na sastanku za preispitivanje Ministarstvo trgovine objasnilo je da je u prvoj godini primjene okvira za privatnost podataka u prvom planu bila uspostava postupka certificiranja, uključujući razvoj namjenskih informatičkih alata, ažuriranje postupaka, suradnju s poduzećima i provedbu drugih aktivnosti informiranja / upoznavanja javnosti s okvirom. Do dana sastanka za preispitivanje više od 2800 poduzeća certificirano je u skladu s okvirom za privatnost podataka. To znači da je više poduzeća certificirano u skladu s okvirom za privatnost podataka nego u skladu s prethodnim okvirom, sustavom zaštite privatnosti, u prvoj godini primjene[9]. Prema informacijama Ministarstva trgovine, 70 % sudionika su MSP-ovi, a velik broj poduzeća uključenih u okvir za privatnost podataka (47 %) pripada sektoru informacijskih i komunikacijskih tehnologija (IKT). Nadalje, 60 % poduzeća certificirano je isključivo za podatke koji nisu povezani s ljudskim resursima, 2,5 % poduzeća certificirano je isključivo za

[6] Predstavnici Komisije i EDPB-a sastali su se 12. lipnja i 10. srpnja 2024. kako bi se pripremili za preispitivanje, raspravili o primljenim doprinosima i utvrdili za koje je aspekte potrebno prikupiti dodatne informacije i pojašnjenja.
[7] Odjeljak I.2 Priloga I. odluci o primjerenosti.
[8] Prilog III. odluci o primjerenosti.
[9] U okviru sustava zaštite privatnosti u istovjetnom je razdoblju certificirano 2400 poduzeća.

podatke povezane s ljudskim resursima, a 37,5 % certificirano je i za podatke povezane s ljudskim resursima i za one koji nisu povezani s ljudskim resursima.

Ministarstvo trgovine donijelo je postupke potrebne za obradu prijave poduzeća. Poduzeća moraju podnijeti prijave za certificiranje na internetskim stranicama Ministarstva trgovine o okviru za privatnost podataka (https://www.dataprivacyframework.gov/). Sadržava informacije o tome kako se uključiti u okvir za privatnost podataka[10] i o obvezama poduzeća na temelju okvira[11]. Poseban tim u Ministarstvu trgovine, pod vodstvom posebnog direktora za okvir za privatnost podataka, zadužen je za sve aspekte upravljanja okvirom za privatnost podataka, uključujući postupak certificiranja i praćenje usklađenosti. Svaka se prijava dodjeljuje određenom članu osoblja koji je odgovoran za predmetno poduzeće tijekom cijelog postupka certificiranja.

Poduzeća koja se žele certificirati u skladu s okvirom podnose prijavu s priloženim nacrtom politike zaštite privatnosti. Ministarstvo trgovine provjerava je li u skladu sa zahtjevima okvira za privatnost podataka. Ako organizacije žele certificirati više subjekata u grupi poduzeća (npr. više podružnica), Ministarstvo trgovine traži da dostave i preispituje jednu sveobuhvatnu politiku zaštite privatnosti u kojoj su jasno navedeni svi subjekti na koje se odnosi ili zasebne politike za svaki subjekt. Ministarstvo trgovine provjerava s neovisnim mehanizmom pravne zaštite[12] koji je naveden u prijavi je li organizacija uistinu registrirana za njega. Kad je riječ o poduzećima koja odaberu odbor tijela za zaštitu podataka (npr. jer obrađuju podatke o ljudskim resursima), Ministarstvo trgovine provjerava je li poduzeće platilo potrebnu naknadu za taj odbor. Ministarstvo trgovine prema potrebi provjerava je li podnositelj prijave u nadležnosti FTC-a ili Ministarstva prometa (što znači da ispunjava uvjete za uključivanje u okvir za privatnost podataka).

Ako su ispunjeni svi uvjeti, Ministarstvo trgovine obavještava organizaciju da na svojim internetskim stranicama može objaviti svoju politiku zaštite privatnosti u kojoj se upućuje na okvir za privatnost podataka. Nakon što politika zaštite privatnosti postane javna, Ministarstvo trgovine potvrđuje certifikate i uvrštava poduzeće na popis organizacija uključenih u okvir za privatnost podataka. Okvir za privatnost podataka može se primjenjivati za primanje osobnih podataka iz EU-a od datuma kad Ministarstvo trgovine uvrsti organizaciju na taj popis[13].

Kako je objašnjeno na sastanku za preispitivanje, u dosadašnjim provjerama Ministarstvo trgovine odbilo je 33 prijave jer nisu ispunjavale zahtjeve okvira za privatnost podataka. Ministarstvo trgovine uglavnom surađuje s poduzećem da bi uklonilo sve nedostatke. Ako Ministarstvo trgovine utvrdi nedostatke, obavješćuje poduzeće da ih mora ukloniti i da će, ako ne odgovori u određenom roku ili ne dovrši samocertificiranje u skladu s postupcima Ministarstva trgovine, smatrati da je odustalo od prijave. Ako se početno certificiranje ne provede/izmijeni u roku od 12 mjeseci, Ministarstvo trgovine smatra da je poduzeće odustalo od prijave.

Rok za godišnje ponovno certificiranje naveden je u popisu organizacija uključenih u okvir za privatnost podataka za svako poduzeće. Kako bi podsjetilo poduzeća da trebaju podnijeti

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(dio%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Mehanizmi za rješavanje sporova iz privatnog sektora u okviru kojih se pritužbe i sporovi svakog pojedinca istražuju i brzo rješavaju bez troškova za tog pojedinca.

[13] Odjeljak I. stavak 3. Priloga I. odluci o primjerenosti.

prijavu za ponovno certificiranje, Ministarstvo trgovine izradilo je sustav podsjetnika o skorašnjem isteku certifikata. Organizacije dobivaju podsjetnik mjesec dana, dva tjedna i jedan dan prije datuma isteka. One kojima certifikat istekne uklanjaju se s popisa organizacija uključenih u okvir za privatnost podataka. Kako je opisano u Prilogu III. odluci o primjerenosti, Ministarstvo trgovine na svojim internetskim stranicama ima poseban odjeljak u kojem se navode organizacije iz SAD-a koje više nisu aktivni sudionici i razlozi zbog kojih su predmetna poduzeća uklonjena s popisa (npr. istek certifikata ili povlačenje) („popis neaktivnih organizacija"). Ako organizacije budu uklonjene s popisa organizacija uključenih u okvir za privatnost podataka jer je njihov certifikat istekao, Ministarstvo trgovine stupit će u kontakt s njima kako bi provjerilo žele li se povući ili se namjeravaju ponovno certificirati. Ako se namjeravaju ponovno certificirati, trebaju dodatno potvrditi da su u razdoblju od isteka certifikata primjenjivale Načela okvira za privatnost podataka na osobne podatke primljene u skladu s tim okvirom i pojasniti koje će radnje poduzeti da riješe otvorena pitanja zbog kojih su odgodile ponovno certificiranje. Kad poduzeća obavijeste Ministarstvo trgovine da se žele povući iz okvira za privatnost podataka, ono od njih traži da potvrde hoće li vratiti ili izbrisati podatke primljene u skladu s okvirom za privatnost podataka, zadržati takve podatke i nastaviti primjenjivati Načela na njih (što moraju potvrditi svake godine) ili ih zadržati i osigurati njihovu zaštitu drugim sredstvima (kao što su standardne ugovorne klauzule koje je donijela Europska komisija).

Povratne informacije trgovinskih udruženja i poduzeća upućuju na to da su poduzeća certificirana u skladu s okvirom za privatnost podataka poduzela niz radnji kako bi osigurala usklađenost s Načelima okvira. Na primjer, kako bi postupale u skladu s *načelom pravne zaštite, provedbe i odgovornosti*, organizacije su provele interne provjere u okviru samoprocjene ili vanjskog preispitivanja usklađenosti. Dva neovisna mehanizma pravne zaštite iz privatnog sektora koja su sudjelovala na sastanku za preispitivanje objasnila su da pružaju uslugu vanjskog preispitivanja usklađenosti u okviru koje preispituju politiku zaštite privatnosti, a jedan je naveo da pruža i usluge revizije i nasumične provjere, s posebnim težištem na, na primjer, načela *pristupa, izbora* i *odgovornosti za daljnji prijenos*. Osim toga, certificirana poduzeća uspostavila su interne programe za usklađenost i mehanizme nadzora, obučile su zaposlenike, uvele mehanizme da bi pojedinci mogli ostvariti svoja prava, provele procjene utjecaja na privatnost i preispitale postojeće ugovore.

2.1.2. Praćenje usklađenosti, lažne izjave o sudjelovanju i provedba

U skladu s okvirom za privatnost podataka Ministarstvo trgovine odgovorno je za praćenje usklađenosti s Načelima okvira za privatnost podataka raznim sredstvima, uključujući provjere po službenoj dužnosti (na vlastitu inicijativu), *ad hoc* terenske provjere i upitnike o usklađenosti. To uključuje pretraživanje i rješavanje problema lažnih tvrdnji o sudjelovanju u okviru, primjerice pretraživanjem interneta[14].

Kako bi pratilo usklađenost poduzeća uključenih u okvir za privatnost podataka s načelima, Ministarstvo trgovine u protekloj se godini uglavnom oslanjalo na *ad hoc* internetska pretraživanja i provjere (društvenih) medija. Ministarstvo trgovine izvijestilo je da u prvoj godini nije otkrilo probleme s usklađenošću s načelima okvira za privatnost podataka i da nije uputilo nijedan predmet FTC-u ili Ministarstvu prometa radi mogućeg izricanja provedbenih

[14] Vidjeti Prilog III. odluci o primjerenosti. Lažne izjave mogu se pojaviti ako, na primjer, poduzeće tvrdi da sudjeluje u okviru za privatnost podataka, a zapravo nikad nije započelo postupak certificiranja ili ga je započelo, ali nije dovršilo ili je dopustilo da certifikat istekne.

mjera. Uspostavilo je i posebnu kontaktnu točku da bi olakšalo suradnju s tijelima za zaštitu podataka i primanje pritužbi pojedinaca i upućivanja od drugih tijela (npr. tijela za zaštitu podataka ili FTC-a). Međutim, u protekloj godini nije zaprimljen nijedan upućeni predmet ili pritužba. Iako je u prvoj godini primjene okvira za privatnost podataka Ministarstvo trgovine bilo usmjereno na uspostavu okvira i postupka certificiranja, na sastanku za preispitivanje objasnilo je da planira provoditi automatizirane provjere usklađenosti kako bi one bile sustavnije te da trenutačno razvija potrebne informatičke alate.

Komisija potvrđuje da je Ministarstvo trgovine u prvoj godini trebalo raditi na uspostavi okvira i postupka certificiranja. Važno je da Ministarstvo trgovine u budućnosti dodatno radi na praćenju i provjeri usklađenosti s Načelima, što je nužno za osiguravanje trajne visoke razine usklađenosti s okvirom i otkrivanje slučajeva za koje su potrebne daljnje provedbene mjere, uključujući moguće lažne izjave o sudjelovanju poduzeća. U tom pogledu Komisija pozdravlja činjenicu da je Ministarstvo trgovine potvrdilo svoju namjeru da razvije i upotrebljava (automatizirane) alate za učinkovitije i sustavnije utvrđivanje problema usklađenosti i pronalazak lažnih izjava te smatra da bi to trebalo biti dio općih nastojanja da se u većoj mjeri iskoriste razna sredstva koja su mu na raspolaganju (npr. terenske provjere, upitnici za preispitivanje usklađenosti, zahtjevi za informacije itd.), među ostalim kako bi se provjerila usklađenost s posebnim zahtjevima okvira za privatnost podataka[15].

Za organizacije uključene u okvir za privatnost podataka nadležni su FTC i Ministarstva prometa. Na sastanku za preispitivanje Ministarstvo prometa potvrdilo je da ima uspostavljene sve postupke potrebne za poduzimanje odgovarajućih provedbenih mjera. Objasnilo je i da se vrlo malo poduzeća u njegovoj nadležnosti uključilo u okvir za privatnost podataka (tj. nekoliko posrednika u prodaji karata, ali nijedan zračni prijevoznik). FTC je potvrdio da sustavno provjerava povrede okvira za privatnost podataka u svim svojim istragama o zaštiti privatnosti. Druga tijela dosad nisu uputila nijedan predmet FTC-u. Zaprimio je nekoliko pritužbi u kojima se spominje okvir za privatnost podataka, ali dvije su se odnosile na poduzeća s „popisa neaktivnih organizacija”, dvije na poduzeća koja nisu sudjelovala u okviru, a jedna se nije odnosila na osobne podatke prenesene iz EU-a. U trenutku pisanja ovog izvješća FTC nije donio odluke za osiguranje usklađenosti s okvirom za zaštitu privatnosti podataka, ali je potvrdio da je nekoliko poduzeća certificiranih u skladu s okvirom za zaštitu privatnosti podataka trenutačno pod istragom.

Komisija pozdravlja činjenicu da FTC sustavno provjerava povrede okvira za privatnost podataka u svim svojim istragama o zaštiti privatnosti. Budući da trajna djelotvornost okvira za privatnost podataka ovisi o njegovoj strogoj provedbi, očekuje se da će FTC i dalje izvršavati svoje istražne ovlasti u skladu s okvirom, među ostalim proaktivnom provedbom opsežnih mjera usmjerenih na usklađenost s posebnim zahtjevima okvira za privatnost podataka i/ili određenim sektorima.

2.1.3. Rješavanje pritužbi

Okvir za privatnost podataka obuhvaća razne mogućnosti pravne zaštite pojedincima iz EU-a u slučajevima neusklađenosti certificiranih organizacija s Načelima okvira za privatnost podataka[16]. To uključuje traženje rješenja izravnim kontaktima s organizacijom uključenom u

[15] Na primjer, kad je riječ o daljnjim prijenosima, može na temelju načela 3. točke (b) okvira za privatnost podataka zatražiti sažetak ili reprezentativni primjerak relevantnih odredaba o privatnosti iz ugovora o daljnjim prijenosima.

[16] Vidjeti odjeljak 2.4. odluke o primjerenosti.

okvir za privatnost podataka, koja oštećenom pojedincu mora odgovoriti u roku od 45 dana. Pojedinci također mogu podnijeti pritužbu neovisnom mehanizmu pravne zaštite koji je organizacija imenovala za istraživanje i rješavanje pritužbi. Ovisno o okolnostima to može biti tijelo za alternativno rješavanje sporova ili tijelo za zaštitu podataka[17]. Naposljetku, ako se nijednim drugim dostupnim oblikom pravne zaštite pritužbu ispitanika ne riješi na zadovoljavajući način, pojedinci mogu pokrenuti obvezujuću arbitražu pred Odborom za okvir EU-a i SAD-a za privatnost podataka kao posljednji mehanizam pravne zaštite.

2.1.3.1. Rješavanje pritužbi u okviru poduzeća

Odgovori trgovinskih udruženja i poduzeća na upitnike koje je poslala Komisija upućuju na to da su poduzeća certificirana u skladu s okvirom za privatnost podataka zaprimila vrlo malo pritužbi, ako ijednu, zbog neusklađenosti s Načelima okvira za privatnost podataka od pojedinaca. Poduzeća su istodobno uspostavila razne mehanizme i alate kako bi pojedincima omogućila ostvarivanje prava i podnošenje pritužbi, uključujući internetskim obrascima, e-poštom i telefonom.

2.1.3.2. *Neovisni mehanizmi pravne zaštite*

Povratne informacije primljene na sastanku za preispitivanje i informacije koje su dostavila trgovinska udruženja upućuju na to da je bilo vrlo malo pritužbi neovisnim mehanizmima pravne zaštite. Neki su od neovisnih mehanizama pravne zaštite koje su odabrala poduzeća BBB National Programs, JAMS, TRUSTe i VeraSafe. U skladu s okvirom za privatnost podataka neovisni mehanizmi pravne zaštite moraju objavljivati godišnja izvješća s objedinjenim statističkim podacima o upotrebi njihovih usluga rješavanja sporova. U trenutku donošenja ovog izvješća svi uključeni neovisni mehanizmi pravne zaštite objavili su svoja godišnja izvješća[18].

Osim toga, na sastanku za preispitivanje BBB i VeraSafe imali su detaljna izlaganja o svojim aktivnostima prošle godine. Izvijestili su o povećanju broja poslovnih sudionika koji su odabrali njihove usluge u odnosu na prethodne okvire i spomenuli da su zaprimili neke pritužbe, ali je velika većina bila neprihvatljiva. Na primjer, BBB je zaprimio 87 pritužbi pojedinaca iz EU-a, od kojih su samo dvije bile prihvatljive za rješavanje. Iako je BBB objasnio da se pritužbe u prosjeku obrađuju pet radnih dana, te su dvije pritužbe naposljetku zaključene

[17] Organizacije uključene u okvir za privatnost podataka dužne su surađivati s tijelima za zaštitu podataka pri istrazi i rješavanju pritužbi ako se one odnose na obradu podataka o ljudskim resursima prikupljenih u kontekstu radnog odnosa ili ako se predmetna organizacija dobrovoljno podvrgnula nadzoru tijela za zaštitu podataka.

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers,
BBB National Programs – https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf, ICDR – AAA – https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0,
Insights Association – https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf,
JAMS – https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf,
Privacy Trust DPF Services – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf,
TRUSTe Dispute Resolution – https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf,
VeraSafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

zbog izostanka odgovora pojedinaca. VeraSafe je zaprimio 26 pritužbi, od kojih je šest bilo prihvatljivo za rješavanje. Dvije pritužbe odnosile su se na zahtjeve za pristup i brisanje te su riješene, dvije su još u tijeku, a dvije su povučene ili zaključene zbog izostanka odgovora pojedinca. Oba neovisna mehanizma pravne zaštite objasnila su da se trude odgovoriti na pritužbe na jeziku pojedinca.

Poduzeća uključena u okvir za privatnost podataka koja obrađuju podatke o ljudskim resursima prenesene iz EU-a moraju odabrati tijela za zaštitu podataka iz EU-a kao svoj neovisni mehanizam pravne zaštite za te podatke, a za druge vrste osobnih podataka prenesenih na temelju okvira za privatnost podataka poduzeća također mogu odabrati tijela za zaštitu podataka iz EU-a kao svoj neovisni mehanizam pravne zaštite, ali na dobrovoljnoj osnovi. Zapravo, više od polovine poduzeća certificiranih u skladu s okvirom za privatnost podataka u trenutku preispitivanja odabralo je to rješenje[19], što je dobrodošao razvoj događaja. Nakon što je donesena odluka o primjerenosti, EDPB je donio poslovnik za Neslužbeni odbor tijela za zaštitu podataka iz EU-a. Odbor je nadležan za pružanje obvezujućih savjeta američkim organizacijama ako ne riješe pritužbe pojedinaca povezane s okvirom za privatnost podataka o postupanju s osobnim podacima koji su preneseni iz EU-a u skladu s tim okvirom. U skladu s poslovnikom odbor čini jedno tijelo za zaštitu podataka koje djeluje kao vodeće tijelo za zaštitu podataka i druga imenovana tijela za zaštitu podataka koja sudjeluju u preispitivanju[20]. Pruža obvezujuće savjete u roku od 60 dana od primitka pritužbe povezane s okvirom za privatnost podataka. Europski odbor za zaštitu podataka objavio je i predložak obrasca za pritužbe tijelima za zaštitu podataka[21] te često postavljana pitanja za europske pojedince[22] i poduzeća[23] o okviru EU-a i SAD-a za privatnost podataka. Odbor do preispitivanja nije zaprimio nijednu pritužbu.

2.1.3.3. Obvezujući arbitražni mehanizam

Ministarstvo trgovine odabralo je Međunarodni centar za rješavanje sporova (ICDR), međunarodni odjel Američkog udruženja za arbitražu, za vođenje obvezujućih arbitraža. Nakon što je donesena odluka o primjerenosti, Ministarstvo trgovine je s Komisijom odabralo 11 arbitara s iskustvom u području privatnosti i iz različitih sektora, uključujući arbitražu, pravosuđe, akademsku zajednicu i civilno društvo[24]. Osim toga, doneseni su pravila arbitraže[25] za Odbor za okvir za privatnost podataka i kodeks ponašanja za arbitre[26] koji su dostupni na internetskim stranicama Međunarodnog centra za rješavanje sporova. Do trenutka preispitivanja ni jedan pojedinac iz EU-a još nije pokrenuo arbitražni mehanizam.

2.1.4. Smjernice, suradnja i informiranje

[19]Ubrzo nakon datuma sastanka, na internetskim stranicama okvira navedeno je da je 1511 od 2892 sudionika imalo tijelo EU-a za zaštitu podataka kao mehanizam pravne zaštite.
[20]EDPB je 17. travnja 2024. donio Poslovnik za „neformalni odbor tijela za zaštitu podataka iz EU-a" u skladu s okvirom EU-a i SAD-a za privatnost podataka. Može mu se pristupiti ovdje: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.
[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_hr.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_hr.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_hr.
[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26]https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.

Otkad je okvir za privatnost podataka stupio na snagu, Ministarstvo trgovine provodilo je razne aktivnosti informiranja, kao što su prezentacije, internetski seminari i konferencije, razgovaralo je s trgovinskim udruženjima i stupilo u izravan kontakt s više od 3000 poduzeća kako bi im pružilo informacije o okviru za privatnost podataka. Objavilo je i smjernice, među ostalim u obliku najčešćih pitanja za pojedince i poduzeća iz EU-a i SAD-a[27]. S druge strane, EDPB je izradio obrasce za pritužbe i popis najčešćih pitanja za pojedince i poduzeća. Slično tomu, Komisija je objavila pitanja i odgovore te informativni članak o okviru za privatnost podataka kad je donijela odluku o primjerenosti[28].

Isto tako, na sastanku za preispitivanje zaključeno je da je potrebno dodatno raditi na informiranju pojedinaca i pružanju smjernica poduzećima. Povratne informacije poduzeća i neovisnih mehanizama pravne zaštite i vrlo malo pritužbi upućuju na to da pojedinci možda nisu uvijek upoznati sa svojim pravima i/ili mehanizmom za njihovo ostvarivanje. Na sastanku za preispitivanje Ministarstvo trgovine izrazilo je interes za suradnju s tijelima za zaštitu podataka iz EU-a na informiranju pojedinaca iz EU-a o okviru. Komisija potiče takve inicijative i poduzima radnje za bolje informiranje pojedinaca, među ostalim pružanjem dodatnih informacija o okviru za privatnost podataka na svojim internetskim stranicama, na primjer uključivanjem poveznica i upućivanja na relevantne smjernice koje su donijeli EDPB, Ministarstvo trgovine i druga američka tijela.

Kad je riječ o smjernicama o Načelima okvira za privatnost podataka, predstavnici EDPB-a na sastanku za preispitivanje pristali su surađivati u nadolazećim mjesecima kako bi dodatno pojasnili što su podaci o ljudskim resursima u okviru za privatnost podataka i posebne obveze koje se primjenjuju na obradu takvih podataka. Istraženi su razni elementi koje treba uključiti u smjernice. Na primjer, te bi se smjernice mogle odnositi na određene slučajeve u praksi u kojima bi se podaci zaposlenika obrađivali u skladu s okvirom za privatnost podataka (npr. kad bi ih obrađivao pružatelj usluga u oblaku) te bi se moglo objasniti koje bi obveze iz okvira za privatnost podataka bile relevantne u takvim slučajevima. Nadalje, poduzećima koja primaju podatke o zaposlenicima pojedinaca iz EU-a (ali ne upotrebljavaju nužno takve podatke u kontekstu radnog odnosa) moglo bi se predložiti da kao svoj neovisni mehanizam pravne zaštite odaberu odbor tijela za zaštitu podataka. Tako bi se tim pojedincima omogućilo da se obrate tijelu „na bližoj lokaciji” i koje je, prema potrebi, bolje upoznato s nacionalnim zakonima koji se primjenjuju na podatke o ljudskim resursima.

Nadalje, čini da bi bilo korisno pružiti više smjernica (i na temelju informacija dobivenih od trgovinskih udruženja) u vezi sa zahtjevima za daljnje prijenose u skladu s okvirom za privatnost podataka. Osim toga, Ministarstvo trgovine smatra da bi bilo vrijedno istražiti mogu li neki sektori imati koristi od dodatnih smjernica o primjeni Načela okvira za privatnost podataka na svoje aktivnosti, npr. u području zdravstvenih istraživanja i financijskih usluga.

Komisija pozdravlja spremnost obiju strana da izrade smjernice i očekuje da će rad na navedenim temama uskoro započeti.

Općenitije, uspostavljeno je nekoliko mehanizama kako bi se omogućile razmjene i suradnja između američkih tijela i tijela za zaštitu podataka, uključujući uspostavljanjem posebnih

[27] Vidjeti npr. https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_hr.

kontaktnih točaka u okviru FTC-a i Ministarstva trgovine za rješavanje upita i predmeta koje je uputilo tijelo za zaštitu podataka.

2.1.5. Relevantne promjene u pravnom sustavu SAD-a

Od donošenja odluke o primjerenosti došlo je do niza promjena pravnog okvira SAD-a u području privatnosti. To uključuje zakonodavne i regulatorne promjene te promjene u sudskoj praksi. One općenito upućuju na sve veću usklađenost pristupa EU-a i SAD-a određenim pitanjima u području zaštite privatnosti, među ostalim zbog upotrebe sličnih pravnih koncepata. Neke su od tih promjena u tijeku i potrebno je dalje ih pratiti.

Na saveznoj razini predsjednik je izdao nekoliko izvršnih naloga koji su relevantni za upotrebu osobnih podataka. Konkretno, Izvršnim nalogom br. 14117 od 28. veljače 2024.[29] zabranjuju se ili ograničavaju transakcije koje uključuju određene kategorije osjetljivih osobnih podataka (npr. zdravstveni podaci, biometrijski identifikatori, genomski podaci o ljudima) sa subjektima u nekim „problematičnim zemljama”[30]. U donesenom se nalogu glavnom državnom odvjetniku nalaže da predloži propise, na čije se izdavanje još čeka u trenutku donošenja ovog izvješća, kako bi se dodatno usmjerila njegova provedba. Isto tako, Izvršni nalog br. 14110 od 30. listopada 2023. o umjetnoj inteligenciji[31] usmjeren je na razvoj sigurne, zaštićene i pouzdane umjetne inteligencije. U skladu s njim nekoliko saveznih agencija treba uspostaviti sigurnosne standarde i smjernice povezane s umjetnom inteligencijom, uključujući o posebnim rizicima koje umjetna inteligencija predstavlja za privatnost i tehnikama očuvanja privatnosti.

Kad je riječ o zakonodavnom radu, iako su u Kongresu u posljednjih nekoliko godina podneseni prijedlozi saveznih zakona o zaštiti privatnosti, 20 američkih saveznih država donijelo je sveobuhvatne zakone o privatnosti u srpnja 2024., od kojih je osam stupilo na snagu: u Kaliforniji, Coloradu, Oregonu, Virginiji, Connecticutu, Uti, Teksasu i Floridi. Nadalje, 17 američkih saveznih država donijelo je zakonodavstvo koje se odnosi na automatiziranu obradu

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Među njima su, u skladu s prijedlogom glavnog državnog odvjetnika u prethodnoj obavijesti o predloženom donošenju propisa objavljenoj 3. svibnja 2024., Kina, Kuba, Hong Kong i Makao, Iran, Sjeverna Koreja i Venezuela. Vidjeti https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

(ili barem neke njezine oblike) i koje općenito dopušta izuzeća za određene vrste donošenja odluka na temelju „izrade profila”[32].

Kad je riječ o promjenama sudske prakse, nekoliko predstavnika civilnog društva uputilo je na nedavnu presudu Vrhovnog suda u predmetu *Loper Bright Enterprises protiv Raimonda* (od 28. lipnja 2024.). Ova presuda poništava dosadašnju sudsku praksu o doktrini *Chevron*, prema kojoj sudovi moraju poštovati razumno tumačenje zakona regulatorne agencije u slučaju dvosmislenosti zakona koji provodi ta agencija. Konkretno, neke nevladine organizacije izrazile su zabrinutost zbog učinka te presude Vrhovnog suda na nadležnost FTC-a za donošenje propisa u području privatnosti, iako možda neće biti nikakvog ili će biti samo ograničenog učinka na njegove izvršne ovlasti. Na sastanku za preispitivanje FTC je izjavio da je još rano da se utvrde točne posljedice te presude. Objasnio je i da FTC donosi propise na temelju ovlasti iz Zakona o FTC-u koje se razlikuju od ovlasti drugih upravnih agencija i za koje doktrina *Chevron* nije toliko relevantna. Stoga nedavna presuda može imati ograničen učinak u tom području.

Osim toga, FTC je izvijestio o nedavnim promjenama u svojem pristupu automatiziranoj obradi i umjetnoj inteligenciji. To uključuje donošenje zajedničke izjave s drugim provedbenim tijelima protiv diskriminacije i pristranosti u automatiziranim sustavima[33] kao i nekoliko provedbenih mjera, u kojima se FTC usmjerava na, među ostalim, transparentnost, pravednost automatizirane obrade i mogućnost pojedinaca da osporavaju ishode. U tom je pogledu najvažnija odluka FTC-a protiv poduzeća Rite Aid u ožujku 2024., u kojoj mu je izrekao petogodišnju zabranu upotrebe tehnologije prepoznavanja lica u sigurnosne svrhe[34]. Konkretno, FTC je utvrdio da Rite Aid nije poduzeo razumne mjere kako bi spriječio dobivanje pogrešnih rezultata i informirao potrošače o tehnologiji koju upotrebljava. Općenito, FTC se na sastanku za preispitivanje osvrnuo na svoje trenutačne prioritete, a posebno na područja za koja smatra da u budućnosti zaslužuju proaktivniji pristup provedbi. To uključuje zaštitu

[32] Iako savezne države imaju različito shvaćanje pojma „izrada profila”, ona se općenito definira kao svaki oblik automatizirane obrade osobnih podataka radi evaluacije, analize ili predviđanja osobnih aspekata povezanih s ekonomskim stanjem, zdravljem, osobnim preferencijama, interesima, pouzdanošću, ponašanjem, lokacijama ili kretanjem pojedinca čiji je identitet utvrđen ili se može utvrditi. Od izrade profila obično se mogu izuzeti potrošači. Sljedeće savezne države izradile su zakonodavstvo o izradi profila: Colorado (članak 6-1-1306 Revidiranog zakonika Colorada s komentarima), Connecticut (članak 42-518 Općeg zakonika Connecticuta s komentarima), Delaware (glava 6. članak 12D-104 Zakonika Delawarea s komentarima), Florida (članak 501.705 Zakonika Floride s komentarima), Indiana (članak 24-15-3-1 Zakonika Indiane s komentarima), Kentucky (članak 367.3615 Revidiranog zakonika Kentuckyja s komentarima), Maryland (Zakon savezne države Maryland o zaštiti privatnosti podataka na internetu iz 2024., donesen 9. svibnja 2024.), Minnesota (članak 325O.07 Zakonika Minnesote s komentarima), Montana (članak 30-14-2808 Zakonika Montane s komentarima), Nebraska (članci 87.–1107. Revidiranog zakonika Nebraske s komentarima), New Hampshire (članak 507-H:4 Revidiranog zakonika New Hampshirea s komentarima), New Jersey (Zakonik New Jerseyja s komentarima), Oregon (članak 646A.574 Revidiranog zakonika Oregona s komentarima), Rhode Island (Zakon savezne države Rhode Island o transparentnosti i zaštiti privatnosti podataka, donesen 29. lipnja 2024.), Tennessee (članak 47-18-3304 Zakonika Tennesseeja s komentarima), Teksas (članak 541.051 Poslovnog i trgovačkog zakonika Teksasa s komentarima) i Virginija (članak 59.1-577 Zakonika Virginije).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

osjetljivih podataka (npr. zdravstveni podaci, biometrijski podaci, geolokacija)[35], zaštitu djece[36] i maloljetnika na internetu te sigurnost podataka[37].

Komisija će nastaviti pomno pratiti te i druge promjene u SAD-u, a posebno sve daljnje radnje prema donošenju sveobuhvatnog saveznog zakona o privatnosti i mogući učinak nedavne sudske prakse Vrhovnog suda o ulozi FTC-a u području privatnosti.

Komisija izražava zadovoljstvo informacijama koje je FTC dostavio o svojim nedavnim provedbenim aktivnostima i trenutačnim prioritetima koji se u velikoj mjeri podudaraju s trendovima i prioritetima u provedbi zaštite podataka u Europi. FTC aktivno sudjeluje i u mreži zemalja koje imaju koristi od odluke EU-a o primjerenosti, koju je Komisija pokrenula u ožujku 2024.[38] Ta sve veća usklađenost trebala bi potaknuti i olakšati pojačanu suradnju tijela za provedbu zaštite privatnosti s obje strane Atlantika, posebno u pogledu pitanja relevantnih za funkcioniranje okvira za privatnost podataka.

2.2. Aspekti koji se odnose na pristup i upotrebu osobnih podataka koje u skladu s okvirom EU-a i SAD-a za privatnost podataka prenesu američka javna tijela

Odluka o primjerenosti sadržava detaljnu procjenu pravila kojima se uređuju prikupljanje i upotreba osobnih podataka koje američka javna tijela prenose iz EU-a poduzećima certificiranima u skladu s okvirom za privatnost podataka, posebno za potrebe kaznenog progona i nacionalne sigurnosti. Američka tijela potvrdila su na sastanku za preispitivanje da od donošenja odluke o primjerenosti nije bilo relevantnih promjena pravnog okvira koji se primjenjuje na pristup podacima za potrebe kaznenog progona ili u regulatorne svrhe u prvoj godini primjene okvira za privatnost podataka. Zbog toga se nalazi u nastavku odnose samo na promjene u području nacionalne sigurnosti.

Zaključci odluke o primjerenosti o pristupu obavještajnih agencija podacima temelje se na analizi uvjeta i ograničenja koji se primjenjuju na operacije prikupljanja obavještajnih podataka elektroničkim izviđanjem u skladu s nekoliko relevantnih pravnih osnova, posebno s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti (FISA) i Izvršnim nalogom br. 12333[39], koje dopunjuje i jača Izvršni nalog br. 14086 o poboljšanju zaštitnih mjera u

[35] Vidjeti npr. nedavni nalog FTC-a protiv poduzeća X-Mode za prodaju i dijeljenje osjetljivih informacija o lokaciji (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) i protiv poduzeća Monument u vezi s otkrivanjem osjetljivih zdravstvenih podataka trećim stranama u marketinške svrhe (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Na primjer, FTC je nedavno najavio istragu koja je dovela do tužbe protiv TikToka i njegova matičnog poduzeća ByteDance zbog navodnog kršenja zakona o privatnosti djece. Tvrdi se da oba društva nisu ispunila zahtjev obavješćivanja i dobivanja pristanka roditelja prije prikupljanja i korištenja osobnih podataka djece mlađe od 13 godina (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Vidjeti pregled nedavnih provedbenih aktivnosti u FTC-ovom dokumentu iz 2023. „Privacy and Data Security Update:. https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] Vidjeti https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. Na sastanku u ožujku 2024. odlučeno je da će se održati niz tematskih sjednica. Prva je održana u srpnju 2024. i bila je usmjerena na razvoj alata kojima se malim i srednjim poduzećima može pružiti potpora u usklađivanju sa zakonima o privatnosti.

[39] U skladu sa Zakonom o nadzoru stranih obavještajnih aktivnosti u pogledu podataka prenesenih iz EU-a mogu se provesti i sljedeće mjere: individualizirani elektronički nadzor (članak 105. Zakona o nadzoru stranih obavještajnih aktivnosti), fizičke pretrage (članak 302. Zakona o nadzoru stranih obavještajnih aktivnosti), upotreba uređaja za bilježenje ulaznih i izlaznih poziva (članak 402. Zakona o nadzoru stranih obavještajnih aktivnosti) i prikupljanje poslovnih evidencija određenih društava (javni prijevoznici, javni smještajni objekti, subjekti za iznajmljivanje vozila ili subjekti za fizičko skladištenje, članak 501. Zakona o nadzoru stranih

američkim aktivnostima elektroničkog izviđanja koji je izdao predsjednik SAD-a 7. listopada 2022. Zaštitne mjere utvrđene u Izvršnom nalogu br. 14086 primjenjuju se na sve aktivnosti elektroničkog izviđanja koje provodi SAD, neovisno o pravnoj osnovi za te aktivnosti i mjestu na kojem se odvijaju, i omogućuju zaštitu podataka osoba koje nisu državljani SAD-a (uključujući Europljane)[40]. U Izvršnom nalogu br. 14086 uspostavljen je i novi mehanizam pravne zaštite na temelju kojeg se pojedinci u EU-u mogu pozvati na te obvezujuće zaštitne mjere i ostvariti prava koja one jamče.

U sljedećim odjeljcima opisuju se koraci koje su američka tijela poduzela od donošenja odluke o primjerenosti radi usklađivanja s Izvršnim nalogom br. 14086 te relevantne promjene povezane s prethodno navedenim pravnim okvirom.

2.2.1. Relevantne promjene s obzirom na pravni okvir SAD-a

2.2.1.1. Provedba Izvršnog naloga br. 14086 u obavještajnim agencijama

Ograničenja i zaštitne mjere uvedene Izvršnim nalogom br. 14086 dopunjuju ograničenja i zaštitne mjere iz članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti i Izvršnog naloga br. 12333. Obvezujuće su za sve obavještajne agencije, a u praksi se provode u okviru politika i postupaka koje je donijela pojedinačna agencija.

U okviru prvog preispitivanja američka tijela potvrdila su da nije bilo izmjena Izvršnog naloga br. 14086 od njegova donošenja. Osim toga, pojasnila su da predsjednik SAD-a nije iskoristio ovlast predviđenu u članku 2. točki (b)(i)(B) i članku 2. točki (b)(ii)(C) Izvršnog naloga br. 14086 kako bi ažurirao popis legitimnih ciljeva za koje se obavještajni podaci mogu prikupljati elektroničkim izviđanjem ili popis svrha za koje se mogu upotrebljavati skupno prikupljeni podaci[41]. Kako bi se utvrdili konkretniji obavještajni prioriteti za koje se obavještajni podaci uistinu mogu prikupljati elektroničkim izviđanjem, u Izvršnom nalogu br. 14086 uspostavljen je poseban postupak. Konkretno, potrebno je savjetovati se sa službenikom za zaštitu građanskih sloboda ODNI-ja kako bi se za svaki prioritet ishodilo procjenu 1. da se njime nastoji ostvariti jedan ili više legitimnih ciljeva iz Izvršnog naloga, 2. da nije osmišljen da dovede niti se očekuje da će dovesti do prikupljanja podataka elektroničkim izviđanjem za cilj zabranjen Izvršnim nalogom i 3. da je prioritet postavljen nakon što su se u odgovarajućoj mjeri uzele u obzir privatnost i građanske slobode svih osoba[42]. Službenica za zaštitu građanskih sloboda ODNI-ja potvrdila je na sastanku za preispitivanje da je preispitala prioritete koje je direktor za nacionalna obavještajna pitanja predložio u Okviru za nacionalne obavještajne prioritete za 2023., zaključila je da su u skladu s navedenim zahtjevima i podijelila svoj zaključak s direktorom za nacionalna obavještajna pitanja, koji je zatim predsjedniku podnio prioritete na potvrdu. Službenica za zaštitu građanskih sloboda ODNI-ja organizirala je i osposobljavanje o zahtjevima Izvršnog naloga br. 14086 za dijelove obavještajne zajednice uključene u utvrđivanje obavještajnih prioriteta.

obavještajnih aktivnosti). Te drukčije pravne osnove detaljno su analizirane u odluci o primjerenosti (uvodne izjave od 142. do 152.).

[40] Za dodatne informacije vidjeti odjeljak 3.2.1.2 odluke o primjerenosti.

[41] Ti legitimni ciljevi/svrhe uključuju, na primjer, zaštitu od špijunaže, sabotaže, atentata ili drugih obavještajnih aktivnosti koje provodi strana vlada, organizacija ili osoba ili koje se provode u njihovo ime ili uz njihovu pomoć; zaštitu od terorizma, uzimanje talaca i držanje zatočenih pojedinaca koje provodi strana vlada, organizacija ili osoba ili koje se provode u njihovo ime.

[42] Članak 2. točka (b)(ii) Izvršnog naloga br. 14086.

Osim toga, američka su tijela prošle godine poduzela daljnje praktične radnje za provedbu Izvršnog naloga br. 14086 u svojem svakodnevnom radu. Konkretno, obavještajne agencije uspostavile su dodatne interne politike i smjernice o provedbi Izvršnog naloga, kao što su interni postupci (uspostavom zahtjeva za interno odobrenje, kontrole dokumentiranog pristupa kako bi samo osobe s odgovarajućom obukom koje ispunjavaju potrebne zahtjeve za misije imale pristup informacijama itd.) kako bi osigurale da se zahtjevi u pogledu nužnosti i razmjernosti poštuju i pri ciljanom i pri skupnom prikupljanju[43]. Nadalje, organizirano je osposobljavanje za osoblje više obavještajnih agencija (npr. NSA, CIA, FBI) o Izvršnom nalogu br. 14086, uključujući godišnje i *ad hoc* tečajeve osposobljavanja koje je organizirala službenica za zaštitu građanskih sloboda ODNI-ja kao i obvezna osposobljavanja za sve novo osoblje ODNI-ja.

Komisija je izrazila zadovoljstvo jer su uvedene razne mjere za provedbu i usklađivanje s Izvršnim nalogom br. 14086. Kad se stekne više iskustva praktičnom primjenom zaštitnih mjera iz Izvršnog naloga, Komisija bi bila zahvalna da u budućim preispitivanjima dobije priliku da raspravi o konkretnim primjerima provedbe zaštitnih mjera Izvršnog naloga u praksi (vodeći računa o povjerljivosti).

2.2.1.2. Ponovno odobrenje članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti

U članku 702. Zakona o nadzoru stranih obavještajnih aktivnosti dopušteno je prikupljanje stranih obavještajnih podataka o osobama koje nisu američki državljani i za koje se opravdano vjeruje da se nalaze izvan Sjedinjenih Američkih Država. Podaci se prikupljaju godišnjim potvrdama koje se podnose Sudu za nadzor stranih obavještajnih aktivnosti (FISC) na odobravanje. U tim se potvrdama utvrđuju posebne kategorije stranih obavještajnih podataka koje će se prikupljati. ODNI je 21. srpnja 2023. objavio da su odobrene tri potvrde u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti koje obuhvaćaju sljedeće kategorije stranih obavještajnih podataka: 1. strane vlade i povezani subjekti, 2. borba protiv terorizma i 3. borba protiv širenja oružja[44]. Potvrde moraju obuhvaćati i postupke ciljanog praćenja i smanjenja količine podataka koje je odobrio FISC[45]. Konkretno, ciljano praćenje provodi se tako da se od poduzeća iz SAD-a koja zadovoljavaju definiciju „pružatelja usluga elektroničke komunikacije" zatraži da otkriju podatke o elektroničkoj komunikaciji koja je primljena ili poslana preko „selektora", kojima se označuju korištena komunikacijska sredstva, kao što su telefonski broj ili e-adresa. Vlada SAD-a objavila je niz materijala o članku 702. Zakona o nadzoru stranih obavještajnih aktivnosti kako bi informirala javnost o funkcioniranju programa nadzora, primjenjivim zahtjevima i zaštiti privatnosti te ulozi FISC-a[46].

Zbog klauzule o vremenskom ograničenju valjanosti članak 702. Zakona o nadzoru stranih obavještajnih aktivnosti trebao je isteći krajem 2023. ako ga Kongres ponovno ne odobri. Nakon privremenog ponovnog odobrenja bez izmjena, Kongres je 19. travnja 2024. donio

[43] Vidjeti https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, objavljeno 3. srpnja 2023.
[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.
[45] Takvi postupci ograničavaju prikupljanje podataka u svrhu stranih obavještajnih aktivnosti, pristup bazama podataka u kojima su pohranjene informacije prikupljene u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti (među ostalim kontrolom pristupa) i uvode ograničenja za upotrebu, čuvanje i širenje takvih informacija.
[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

Zakon o reformi obavještajnih aktivnosti i osiguravanju Amerike (RISAA), u kojem je ponovno odobrio članak 702. Zakona o nadzoru stranih obavještajnih aktivnosti na dvije godine i uveo nekoliko izmjena. One se mogu razvrstati u dvije opće kategorije: 1. izmjene opsega aktivnosti nadzora dopuštenih na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti i 2. institucionalne i postupovne izmjene.

Izmjene opsega aktivnosti nadzora dopuštenih na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti

Zakon o reformi obavještajnih aktivnosti i osiguravanju Amerike uvodi tri glavne izmjene opsega aktivnosti nadzora koje se mogu provoditi u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti.

Kao prvo, prikupljanje podataka iz komunikacija „s upućivanjima na selektora" potpuno je zabranjeno[47]. Odnosi se na prikupljanje podataka iz komunikacija u kojima selektor iz članka 702. (kao što je adresa e-pošte) nije primatelj ili pošiljatelj komunikacija, nego se upućuje na njega u komunikaciji (npr. poruke e-pošte koje nisu poslane na odabranu adresu e-pošte ili s nje, već je ona spomenuta u tekstu ili tijelu e-pošte). Iako je takvo prikupljanje već bilo isključeno nakon izmjene Zakona o nadzoru stranih obavještajnih aktivnosti iz 2018., taj je zakon i dalje predviđao mogućnost ponovnog dopuštanja prikupljanja podataka iz komunikacija „s upućivanjima na selektora" u budućnosti, nakon posebnog postupka odobrenja u kojem sudjeluju FISC i Kongres. U najnovijoj izmjeni koju uvodi Zakon o reformi obavještajnih aktivnosti i osiguravanju Amerike ta je mogućnost uklonjena.

Drugo, definicija stranih obavještajnih informacija proširena je i sad uključuje i informacije koje se odnose na borbu protiv droge[48]. Na sastanku za preispitivanje američka tijela objasnila su da je ta izmjena uvedena zbog aktualne krize uzrokovane upotrebom fentanila i sve veće prijetnje nacionalnoj sigurnosti koju predstavljaju međunarodni trgovci i proizvođači opojnih droga. U tom je kontekstu potvrđeno da nekoliko legitimnih ciljeva iz Izvršnog naloga br. 14086 obuhvaća taj aspekt, odnosno cilj utvrđivanja ili procjene kapaciteta, namjera ili aktivnosti stranih organizacija koje jesu ili bi mogle biti prijetnja nacionalnoj sigurnosti SAD-a ili njegovih saveznika, cilj utvrđivanja ili procjene transnacionalnih prijetnji globalnoj sigurnosti, uključujući rizike za javno zdravlje i humanitarne prijetnje i zaštita od transnacionalnih kriminalnih prijetnji[49].

Treće, Zakon o reformi obavještajnih aktivnosti i osiguravanju Amerike proširuje definiciju pojma „pružatelj usluga elektroničke komunikacijske", čime se povećava broj poduzeća koja mogu biti obvezna dostavljati informacije u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti[50]. Definicija sad uključuje pružatelje drugih usluga koji imaju „pristup opremi koja se upotrebljava ili bi se mogla upotrebljavati za prijenos ili pohranu telefonske ili elektroničke komunikacije", pri čemu se izričito isključuju javni smještajni objekti, stambeni objekti, društveni objekti i objekti za posluživanje hrane. U dopisu Kongresu Ministarstvo pravosuđa uputilo je na tu izmjenu kao na tehničku izmjenu čiji je cilj obuhvatiti „iznimno malo" tehnoloških poduzeća koja, prema nedavnim odlukama FISC-a i Žalbenog suda za nadzor stranih obavještajnih aktivnosti (FISCR), nisu obuhvaćena prethodnom definicijom

[47] Članak 22. Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike.
[48] Članak 23. Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike.
[49] Članak 2. točke (b)(ii)(A)(2), (3) i (10) Izvršnog naloga br. 14086.
[50] Članak 25. Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike.

pružatelja usluga elektroničke komunikacije[51]. Ministarstvo pravosuđa u tom se dopisu obvezalo suziti definiciju tako da obuhvaća isključivo vrstu pružatelja usluga o kojoj je riječ u sporu zbog kojeg je FISC donio odluku. Zato su ta predmetna poduzeća navedena u klasificiranom prilogu za Kongres. Nekoliko nevladinih organizacija, uključujući one koje su dostavile povratne informacije u okviru preispitivanja, izrazilo je zabrinutost zbog tog proširenja jer smatraju da bi ono moglo obuhvaćati velik broj poduzeća iz SAD-a (jer brojna ta poduzeća pružaju neku vrstu usluge i imaju pristup komunikacijskoj opremi). Zbog toga je, uz potporu obavještajne zajednice, predložena dodatna izmjena Nacrta zakona o odobravanju obavještajnih aktivnosti za fiskalnu godinu 2025., koji Kongres trenutačno razmatra. Ako Kongres donese tu izmjenu, osiguralo bi se da dodatna poduzeća obuhvaćena definicijom pružatelja usluga elektroničke komunikacije budu ograničena na ona iz prethodno navedenih odluka FISC-a. U prijedlogu zakona predviđa se i da se svaka direktiva upućena takvom poduzeću mora prijaviti FISC-u kako bi provjerio treba li poduzeće doista biti obuhvaćeno područjem primjene. U svojem dopisu Kongresu Ministarstvo pravosuđa obvezalo se da će svakih šest mjeseci izvješćivati Kongres o svakoj primjeni ažurirane definicije kako bi se Kongresu omogućilo da provede odgovarajući nadzor u pogledu uske primjene definicije.

Važno je napomenuti da su na sastanku za preispitivanje američka tijela i PCLOB potvrdili da se sve zaštitne mjere iz Izvršnog naloga br. 14086 i dalje u potpunosti primjenjuju na sve prikupljanje i upotrebu podataka u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti, uključujući i nakon tih izmjena. Stoga, iako se u Zakonu o reformi obavještajnih aktivnosti i osiguravanju Amerike donekle povećava broj poduzeća koja mogu dobiti nalog, taj zakon ne ograničava ostvarivanje prava. Međutim, bit će važno pratiti daljnji razvoj događaja (u pogledu zakonodavstva i izvješćivanja) i primati informacije o primjeni tih novih pravila u praksi. To uključuje, na primjer, učinak proširenja definicija stranih obavještajnih informacija i pružatelja usluga elektroničke komunikacije na broj ciljeva iz članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti (kako ih svake godine priopćuje ODNI, vidjeti u nastavku povezano s transparentnosti). Buduće izvješće o praćenju nedavnog izvješća PCLOB-a o članku 702. Zakona o nadzoru stranih obavještajnih aktivnosti (vidjeti u nastavku) trebalo bi biti posebno informativno u tom pogledu.

Institucionalne i postupovne izmjene

Kad je riječ o institucionalnim i postupovnim izmjenama, u Zakonu o reformi obavještajnih aktivnosti i osiguravanju Amerike kodificirano je nekoliko postupaka koji su se već primjenjivali u praksi i uvele nove zaštitne mjere. Iako se neke od njih odnose samo na državljane SAD-a, nekoliko izmjena uvodi veću zaštitu i za državljane SAD-a i za osobe koje nisu državljani SAD-a čiji se podaci mogu prikupljati u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti[52] te su zato relevantne za funkcioniranje okvira za privatnost podataka.

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Vidjeti odluku FISC-a iz 2022. (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) i presudu Žalbenog suda za nadzor stranih obavještajnih aktivnosti koja potvrđuje tu odluku (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

[52] Osim toga, u Zakonu o reformi obavještajnih aktivnosti i osiguravanju Amerike uvode se određene izmjene u pogledu tradicionalnog individualiziranog elektroničkog nadzora u skladu s člankom 105. Zakona o nadzoru stranih obavještajnih aktivnosti (na temelju naloga FISC-a koji se izdaje ako postoji osnovana sumnja). Da bi obavještajna agencija glavnom državnom odvjetniku podnijela zahtjev za izdavanje naloga za provedbu

Prvo, uveden je niz dodatnih zahtjeva u pogledu odgovornosti, nadzora i izvješćivanja. Konkretno, osoblje FBI-a sad svake godine mora pohađati osposobljavanje o pravilima koja se primjenjuju na pretraživanje informacija dobivenih u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti[53]. FBI je također dužan izvijestiti Kongres o svojim aktivnostima pretraživanja (npr. o broju pretraživanja u kojima se upotrebljavaju „tehnologije za skupno pretraživanje", tj. pretraživanje više pojmova u okviru jednog pretraživanja) i mjerama odgovornosti koje su uspostavljene kako bi se osigurala usklađenost sa zahtjevima za pretraživanje pravnih pojmova (članci 11. i 12. Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike). Nadalje, glavni inspektor Ministarstva pravosuđa mora sastaviti izvješće o usklađenosti FBI-a sa zahtjevima u pogledu pretraživanja (članak 9. Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike). Općenitije, kako bi se povećala transparentnost postupaka pred FISC-om, ODNI i glavni državni odvjetnik sad su dužni dovršiti preispitivanje odluka FISC-a u pogledu deklasifikacije u roku od 180 dana (članak 7. Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike). Osim toga, prijepisi svih saslušanja pred FISC-om i Žalbenim sudom za nadzor stranih obavještajnih aktivnosti (pred kojim se može uložiti žalba na odluke FISC-a) moraju se čuvati i prosljeđivati Kongresu (članak 8. Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike).

Drugo, u skladu sa Zakonom o reformi obavještajnih aktivnosti i osiguravanju Amerike uvedena su dodatna ograničenja za FBI-evu upotrebu podataka prikupljenih na temelju članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti. U članku 2. točki (d) Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike navodi se da se pretraživanje „tehnologijom za skupno pretraživanje" može provesti tek nakon ishođenja odobrenja odvjetnika FBI-a, osim u hitnim okolnostima. Osim toga, FBI-u je sad zabranjeno automatski provjeravati informacije čija količina nije smanjena prikupljene u skladu s člankom 702. Zakona o nadzoru stranih obavještajnih aktivnosti, a umjesto toga analitičari moraju dobiti privolu za pretraživanje takvih informacija. Zakon o reformi obavještajnih aktivnosti i osiguravanju Amerike također zabranjuje FBI-u da provodi pretraživanja čija je jedina svrha pronalazak i izvlačenje dokaza o kriminalnoj aktivnosti (osim ako postoji osnovana sumnja da bi oni mogli pomoći u ublažavanju ili uklanjanju životne opasnosti ili opasnosti od teških tjelesnih ozljeda ili ako je to potrebno za ispunjavanje obveza otkrivanja informacija u sudskom postupku)[54]. Nadalje, FBI-u je zabranjeno unositi podatke čija količina nije smanjena u analitičke repozitorije, osim ako je osoba koju se ciljano prati relevantna za istragu u području nacionalne sigurnosti u tijeku[55].

Treće, izmijenjene su određene odredbe koje se odnose na status i ulogu koju *amici curiae* imaju pred FISC-om[56]. *Amici* se imenuju kao stručnjaci koji pomažu Sudu (i FISCR-u) u pitanjima povezanima s privatnošću i građanskim slobodama ili koji pomažu u razjašnjavanju

individualiziranog elektroničkog nadzora, sad treba dostaviti službenu izjavu s razlozima zbog kojih smatra da su ispunjeni uvjeti iz članka 105. Zakona o nadzoru stranih obavještajnih aktivnosti (članak 6. stavak (a) Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike). Moguće trajanje elektroničkog nadzora stranih sila ili agenata stranih sila produljeno je sa 120 dana na godinu dana (članak 6. stavak (g) Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike).

[53] Članak 2. točka (d) Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike.

[54] Članak 3. točka (a) Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike.

[55] Članak 3. točka (b) Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike. Ako je to potrebno zbog hitnih okolnosti, ravnatelj FBI-a može odlučiti o iznimci od te odredbe, o čemu se mora obavijestiti Kongres.

[56] Radi jasnoće te izmjene ne utječu na status i ulogu posebnih odvjetnika pred Žalbenim sudom za zaštitu podataka, kako su američka tijela potvrdila na sastanku za preispitivanje.

tehnoloških pitanja pri obradi zahtjeva određene vlade. U Zakonu o nadzoru stranih obavještajnih aktivnosti bilo je propisano da *amici* trebaju imati stručno znanje u području privatnosti i građanskih sloboda, prikupljanja obavještajnih informacija, komunikacijske tehnologije ili drugih relevantnih područja, a sad propisuje da, u načelu, trebaju imati stručno znanje u području privatnosti i građanskih sloboda i u području prikupljanja obavještajnih informacija. Sud je već imao mogućnost imenovati pojedinca ili skupinu kao *amicus* u svakom slučaju u kojem je smatrao da je to primjereno, a bio je dužan to učiniti u slučaju novog ili značajnog tumačenja zakona. Nakon ponovnog odobrenja FISC je dužan imenovati pojedinca ili skupinu kao *amicus* svaki put kad dobije zahtjev da odobri certifikate i popratne postupke (npr. postupke ciljanog prikupljanja) iz članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti, osim ako smatra da to ne bi bilo primjereno ili da bi vjerojatno dovelo do neopravdane odgode[57]. Osim toga, umjesto imenovanja samo jedne skupine ili pojedinca kao *amicus*, Sud ih sad može imenovati više. Pojašnjeno je i da informacije koje trebaju dostaviti *amici* moraju biti „ograničene na rješavanje posebnih pitanja koja je utvrdio sud" iako su područja o kojima *amici* mogu iznijeti primjedbe i dalje široka (tj. pravni argumenti i informacije povezane sa zaštitom privatnosti i građanskih sloboda pojedinaca iz Sjedinjenih Američkih Država, prikupljanjem obavještajnih informacija i komunikacijskom tehnologijom ili bilo kojim drugim relevantnim područjem).

Naposljetku, u članku 18. Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike osniva se Povjerenstvo za reformu Zakona o nadzoru stranih obavještajnih aktivnosti, koje se sastoji od, među ostalim, članova Kongresa, predsjednika PCLOB-a, glavnog zamjenika direktora za nacionalna obavještajna pitanja i zamjenika glavnog državnog odvjetnika te dodatnih članova koje imenuje Kongres[58] i koje treba preporučiti dodatne reforme Zakona o nadzoru stranih obavještajnih aktivnosti.

Komisija će pomno pratiti daljnji razvoj događaja u pogledu članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti, među ostalim u kontekstu nadzornih aktivnosti PCLOB-a (vidjeti u nastavku), rada Komisije za reforme i predstojećeg preispitivanja Zakona o nadzoru stranih obavještajnih aktivnosti nakon dvije godine.

2.2.1.3. Aktivnosti nadzora u praksi: brojke i trendovi

Godišnje statističko izvješće ODNI-ja o transparentnosti koje prikazuje kako obavještajna zajednica koristi ovlasti povezane s nacionalnom sigurnosti za kalendarsku godinu 2023. (objavljeno u travnju 2024.)[59] pokazuje da se broj ciljanih praćenja iz odjeljka 702. Zakona o nadzoru stranih obavještajnih aktivnosti povećao s 245 073 u kalendarskoj godini 2022. na 268 590 u kalendarskoj godini 2023. U izvješću se objašnjava da oscilacije broja ciljanih praćenja mogu biti povezane s više razloga, uključujući promjene operativnih prioriteta, događaje u svijetu, tehničke mogućnosti, ponašanja subjekata ciljanog praćenja i promjene u telekomunikacijskom sektoru. U izvješću se navodi i da nijedna osoba koja nije državljanin SAD-a (u odnosu na jednu 2021. i nijednu 2022.) nije ciljano praćena na temelju članka 402. Zakona o nadzoru stranih obavještajnih aktivnosti (upotreba uređaja za bilježenje ulaznih i izlaznih poziva), dok je za šest ciljanih praćenja (u odnosu na 13 u 2021. i 11 u 2022.) izdano šest naloga (u odnosu na po 11 naloga 2021. i 2022.) na temelju članka 501. Zakona o nadzoru stranih obavještajnih aktivnosti (prikupljanje poslovnih evidencija javnih prijevoznika,

[57] Članak 5. točka (b) Zakona o reformi obavještajnih aktivnosti i osiguravanju Amerike.
[58] U članku 18. izričito je propisano da se imenuju predstavnici koji nisu članovi Kongresa.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

subjekata za iznajmljivanje vozila ili subjekata za fizičko skladištenje), koji obuhvaćaju 5412 jedinstvenih identifikatora (u odnosu na 23 157 u 2021. i 55 431 u 2022.) za prenošenje informacija prikupljenih na temelju takvih naloga.

U godišnjem izvješću Ministarstva pravosuđa Kongresu o Zakonu o nadzoru stranih obavještajnih aktivnosti navodi se da je u kalendarskoj godini 2023. FISC-u podneseno 327 zahtjeva za provođenje elektroničkog nadzora i/ili fizičkih pretraga u svrhu prikupljanja stranih obavještajnih informacija u skladu s člancima 105. i 302. Zakona o nadzoru stranih obavještajnih aktivnosti[60]. Ukupan broj osoba obuhvaćenih ciljanim praćenjem bio je između 500 i 999. Kad je riječ o dopisima o nacionalnoj sigurnosti, u izvješću se navodi da je izdano 10 115 zahtjeva (isključujući samo zahtjeve za informacije o pretplatnicima) za prikupljanje informacija o osobama koje nisu državljani SAD-a za 3033 osobe koje nisu državljani SAD-a[61].

Nekoliko poduzeća certificiranih u skladu s okvirom za privatnost podataka (npr. Google, Meta) koristi mogućnost predviđenu pravom SAD-a da objavljuju izvješća o transparentnosti u kojima se navodi broj zahtjeva na temelju Zakona o nadzoru stranih obavještajnih aktivnosti i dopisima o nacionalnoj sigurnosti koje su zaprimili u određenom razdoblju izvješćivanja. U trenutku sastavljanja ovog izvješća statistički podaci o zahtjevima na temelju Zakona o nadzoru stranih obavještajnih aktivnosti nakon srpnja 2023. još nisu bili dostupni. Na primjer, Google je izvijestio da je od srpnja do prosinca 2023. primio između 500 i 999 zahtjeva na temelju dopisa o nacionalnoj sigurnosti, koji se odnose na između 2000 i 2499 računa[62]. Meta je izvijestila da je u istom razdoblju izvješćivanja zaprimila između 0 i 499 zahtjeva na temelju dopisa o nacionalnoj sigurnosti, koji se odnose na između 500 i 999 računa[63]. Brojke su posljednjih godina bile prilično stabilne. Kako bi se dodatno povećala transparentnost, neka poduzeća (npr. Google) proaktivno objavljuju dopise o nacionalnoj sigurnosti koje su zaprimile nakon ukidanja ograničenja povezanih s povjerljivošću[64].

2.2.1.4. Ostale promjene

U kontekstu pripreme preispitivanja nekoliko nevladinih organizacija postavilo je pitanja o novim oblicima prikupljanja podataka koje koriste američke obavještajne agencije, kao što je kupnja podataka od poslovnih subjekata, posebno pružatelja usluga posredovanja podataka. Objasnile su da iako se tako prikupljeni podaci i dalje moraju obrađivati u skladu s drugim zahtjevima, među ostalim, na primjer, u skladu s Izvršnim nalogom br. 12333[65], takvo prikupljanje nije u skladu sa Zakonom o nadzoru stranih obavještajnih aktivnosti i Izvršnim nalogom br. 14086.

U tom pogledu treba podsjetiti da se na svaku vrstu dobrovoljnog dijeljenja podataka s trećim stranama primjenjuje nekoliko detaljnih zahtjeva okvira za privatnost podataka. Prvo,

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.

[61] Te su brojke uglavnom ostale stabilne u odnosu na prethodnu godinu izvješćivanja (2022.). Za usporedbu, 2022. podneseno je 317 konačnih zahtjeva FISC-u za provođenje elektroničkog nadzora i/ili fizičkih pretraga u svrhu prikupljanja stranih obavještajnih informacija. Ukupan broj osoba obuhvaćenih elektroničkim nadzorom bio je između 0 i 499. FBI je 2022. podnio 9103 zahtjeva za prikupljanje informacija o osobama koje nisu državljani SAD-a (isključujući samo zahtjeve za informacije o pretplatnicima) na temelju dopisa o nacionalnoj sigurnosti. Izvor: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

[62] https://transparencyreport.google.com/user-data/us-national-security.

[63] https://transparency.meta.com/reports/government-data-requests/country/US/.

[64] https://transparencyreport.google.com/user-data/us-national-security.

[65] Vidjeti, na primjer, članak 2.4. Izvršnog naloga br. 12333 o tehnikama prikupljanja.

certificirana organizacija ne smije dijeliti podatke s trećom stranom (koja ne djeluje kao posrednik / izvršitelj obrade) bez obavijesti i ponuđenog izbora ispitanicima[66]. Drugo, u skladu s *načelom odgovornosti za daljnji prijenos*, daljnji prijenos dopušten je samo 1. u ograničene i određene svrhe, 2. na temelju ugovora između organizacije uključene u okvir EU-a i SAD-a za privatnost podataka i treće strane i 3. ako je treća strana ugovorno obvezana pružati razinu zaštite jednaku onoj koja je zajamčena Načelima[67].

Nadalje, kako se raspravljalo i na sastanku za preispitivanje, FTC je poduzeo provedbene mjere protiv pružatelja usluga posredovanja podataka koji prodaju osjetljive podatke o potrošačima. Na primjer, u predmetu protiv poduzeća X-Mode i njegova nasljednika Outlogic, FTC je 9. siječnja 2024. donio nalog u kojem se poduzeću zabranjuje prodaja geolokacijskih podataka trećim stranama i nalaže brisanje podataka koje je nezakonito upotrijebilo i podijelilo. U istrazi FTC-a utvrđeno je, među ostalim, da poduzeće nije u potpunosti obavijestilo pojedince o upotrebi i prodaji njihovih geolokacijskih podataka niti uvelo mjere kojima bi se pojedincima omogućilo da traže izuzeće, da je dopustilo upotrebu podataka u potencijalno diskriminirajuće svrhe i nije trećim stranama ograničilo upotrebu takvih informacija[68]. Komisija očekuje da će FTC primijeniti isti pristup ako poduzeća certificirana u skladu s okvirom za privatnost podataka budu dijelila podatke kršeći prethodno navedene odredbe.

Naposljetku, valja napomenuti da je ODNI u svibnju 2024. objavio Okvir politike obavještajne zajednice za komercijalno dostupne informacije[69]. U tom se okviru utvrđuje niz načela i zahtjeva koje bi obavještajne agencije trebale slijediti, među ostalim kako bi se smanjili rizici za privatnost i građanske slobode pri prikupljanju i upotrebi informacija u kontekstu poslovne transakcije.

2.2.2. Neovisni nadzor

Aktivnosti američkih obavještajnih agencija podliježu nadzoru više tijela, uključujući službenike za privatnost i građanske slobode, glavne inspektore, Kongres i PCLOB. Konkretno, u Izvršnom nalogu br. 14086 propisano je da svaka obavještajna agencija mora imati više službenike za pravna pitanja, nadzor i usklađenost kako bi se osigurala usklađenost s primjenjivim pravom SAD-a. Tu nadzornu funkciju obavljaju službenici nadležni za usklađenost, ali i službenici za privatnost i građanske slobode te glavni inspektori[70]. Oni moraju redovito nadzirati aktivnosti elektroničkog izviđanja i pobrinuti se za to da se sve neusklađenosti isprave. Obavještajne agencije moraju tim službenicima dati pristup svim

[66] Vidjeti uvodnu izjavu 40. odluke o primjerenosti.
[67] Vidjeti uvodnu izjavu 38. odluke o primjerenosti.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.
[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Obavještajne agencije moraju se pridržavati okvira od kolovoza 2024.
[70] Svaka obavještajna agencija ima glavnog inspektora koji je zakonski neovisan i odgovoran za provedbu revizija i istraga povezanih s aktivnostima koje dotična agencija provodi za potrebe nacionalne sigurnosti. Imaju pristup svim relevantnim materijalima (uključujući klasificirane) prema potrebi na temelju sudskog naloga i mogu uzimati iskaze. Glavni inspektori upućuju slučajeve navodnih povreda kaznenih propisa u postupak kaznenog progona i ravnateljima agencijama preporučuju korektivne mjere. Iako su njihove preporuke neobvezujuće, njihova izvješća, uključujući ona o daljnjim mjerama (ili nepostojanju takvih mjera), u pravilu se objavljuju i šalju Kongresu. Vidjeti u tom pogledu bilješku 136. odluke o primjerenosti o ulozi glavnog inspektora.

informacijama koje su bitne za izvršavanje njihovih nadzornih funkcija i ne smiju poduzimati ništa što bi ih spriječilo u provedbi nadzornih aktivnosti ili neprimjereno utjecalo na nju.

Glavni savjetnik Ureda glavnog inspektora obavještajne zajednice (ICIG) u ODNI-ju, koji ima sveobuhvatnu nadležnost nad cijelom obavještajnom zajednicom i ovlasti za istraživanje pritužbi ili informacija povezanih s navodima o nezakonitom postupanju ili zloupotrebi ovlasti, sudjelovao je na sastanku za preispitivanje. Potvrdio je da ICIG u okviru svojih aktivnosti nadzora sustavno provjerava usklađenost s Izvršnim nalogom br. 14086. Osvrnuo se i na nedavne aktivnosti nadzora drugih glavnih inspektora obavještajne zajednice, kako je detaljno opisano u redovitim izvješćima. Na primjer, u svojem polugodišnjem izvješću Kongresu za razdoblje od travnja do rujna 2023.[71] glavni inspektor NSA-a obavijestio je o evaluaciji okvira unutarnje kontrole NSA-a za odluke i zahtjeve za ciljano praćenje. Zaključio je da taj okvir pravilno funkcionira kako bi se osigurala usklađenost sa zakonima, direktivama i politikama koje štite građanske slobode i privatnost. U istom izvješću spominje i istragu u kojoj je otkriveno da je zaposlenik NSA-a zloupotrijebio alat za prikupljanje obavještajnih informacija elektroničkim izviđanjem u nedopuštene svrhe.

Na temelju Izvršnog naloga br. 14086 PCLOB-u[72] su povjerene posebne nadzorne funkcije[73]. Predsjednik PCLOB-a i njegova tri člana sudjelovali su na sastanku za preispitivanje i obavijestili da je PCLOB u travnju 2023. savjetovao obavještajne agencije o njihovim nacrtima politika i postupcima za provedbu Izvršnog naloga br. 14086 te da je provedeno savjetovanje o imenovanju sudaca i posebnih odvjetnika Žalbenog suda za zaštitu podataka. Osim toga, pokrenuo je i projekt nadzora kako bi 1. preispitao provedbu ažuriranih politika i postupaka koje su donijele obavještajne agencije kako bi osigurao da su usklađene s Izvršnim nalogom i 2. proveo godišnje preispitivanje funkcioniranja novog mehanizma pravne zaštite (vidjeti u nastavku)[74]. Članovi su potvrdili su da PCLOB planira uskoro provesti oba preispitivanja. Kad je riječ o pravnoj zaštiti, objasnili su da će, s obzirom na izostanak pritužbi, preispitivanje PCLOB-a biti usmjereno na politike i postupke za uspostavu mehanizma.

Kad je riječ o drugim nadzornim aktivnostima, PCLOB je 28. rujna 2023. objavio izvješće o članku 702. Zakona o nadzoru stranih obavještajnih aktivnosti[75]. To se izvješće nadovezuje na prethodno izvješće iz 2014. i sadržava ažurirane činjenične i pravne informacije o provedbi programa nadzora iz članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti. Izvješće sadržava i preporuke o usklađenosti obavještajnih agencija s primjenjivim zahtjevima i prijedloge Kongresu za daljnje jačanje nekoliko aspekata članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti u kontekstu njegova ponovnog odobrenja (među ostalim

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.
[72] PCLOB je neovisna agencija odgovorna za politike za borbu protiv terorizma i njihovu provedbu u cilju zaštite privatnosti i građanskih sloboda. Može pristupiti svim relevantnim informacijama (uključujući klasificirane), obavljati razgovore i uzimati iskaze. Može davati preporuke tijelima kaznenog progona i obavještajnim tijelima i redovito izvješćivati Kongres i predsjednika. Njegova izvješća moraju biti što dostupnija javnosti.
[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.
[74] https://www.pclob.gov/OversightProjects/Details/1115.
[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

kodifikacijom legitimnih ciljeva aktivnosti nadzora navedenih u Izvršnom nalogu br. 14086)[76]. Na sastanku za preispitivanje PCLOB je izjavio da očekuje da će uskoro primiti odgovore obavještajnih agencija o provedbi njegovih preporuka, koje će uključiti u buduće izvješće o daljnjim mjerama. Ostali aktualni nadzorni projekti uključuju projekt o borbi protiv domaćeg terorizma i njegovu utjecaju na privatnost i građanske slobode te aktivnosti FBI-a za prikupljanje podataka otvorenog koda ili komercijalno dostupnih podataka[77].

Naposljetku, nevladine organizacije s kojima je provedeno savjetovanje u kontekstu preispitivanja izrazile su zabrinutost jer mandat nekoliko članova PCLOB-a uskoro ističe, zbog čega bi PCLOB mogao ostati bez kvoruma. Konkretno, predsjednici je istekao mandat, a razdoblje u kojem može obnašati dužnost do pronalaska novog predsjednika završava u siječnju 2025., još je jedno mjesto slobodno, a treće će se također osloboditi u siječnju sljedeće godine. Na sastanku za preispitivanje članovi su objasnili da ne očekuju da će PCLOB ostati bez kvoruma jer već postoji kandidat za mjesto koje je trenutačno slobodno (i čeka da ga Senat odobri)[78]. Naglasili su i da, čak i ako PCLOB ostane bez kvoruma, to ne bi utjecalo na njegovu sposobnost da nastavi provoditi projekte nadzora. Međutim, s obzirom na važnu ulogu PCLOB-a u preispitivanju provedbe Izvršnog naloga br. 14086 Komisija će pomno pratiti status budućih slobodnih radnih mjesta i kandidatura/imenovanja.

2.2.3. Pravna zaštita

U Izvršnom nalogu br. 14086, koji je dopunjen Uredbom glavnog državnog odvjetnika, uspostavljen je novi mehanizam pravne zaštite za rješavanje pritužbi pojedinaca koje ispunjavaju uvjete, a odnose se na američke aktivnosti elektroničkog izviđanja[79]. Svaki pojedinac u EU-u ima pravo podnijeti pritužbu u okviru mehanizma pravne zaštite u vezi s navodnom povredom prava SAD-a koje uređuje aktivnosti elektroničkog izviđanja (npr. Izvršni nalog br. 14086, članak 702. Zakona o nadzoru stranih obavještajnih aktivnosti, Izvršni nalog br. 12333) osobnih podataka koji se prenose u SAD koje štetno djeluje na njihovu privatnost i građanske slobode. Pojedinci mogu podnijeti pritužbu tijelu za zaštitu podataka u državi članici EU-a, koje će proslijediti pritužbu u mehanizam pravne zaštite preko tajništva Europskog odbora za zaštitu podataka Mehanizam ima dvije razine, pri čemu pritužbe prvo istražuje službenik za zaštitu građanskih sloboda ODNI-ja, a pojedinci se mogu žaliti na njegovu odluku pred neovisnim Žalbenim sudom za zaštitu podataka. Nakon što službenik za zaštitu građanskih sloboda ODNI-ja ili Žalbeni sud za zaštitu podataka dovrši preispitivanje, preko nacionalnog tijela obavješćuje pojedinca da „preispitivanjem nisu utvrđene predmetne povrede ili je službenik za zaštitu građanskih sloboda ODNI-ja utvrdio koje primjerene korektivne mjere treba provesti”. Odluke službenika za zaštitu građanskih sloboda ODNI-ja i Žalbenog suda za zaštitu podataka obvezujuće su za obavještajne agencije.

Od donošenja odluke o primjerenosti poduzete su daljnje mjere kako bi mehanizam pravne zaštite postao potpuno operativan.

---

[76] Komisija napominje da su neke od tih preporuka uključene u Zakon o reformi obavještajnih aktivnosti i osiguravanju Amerike, uključujući preporuku o prikupljanju podataka iz komunikacija „s upućivanjima na selektora” ili preporuku o jačanju uloge stručnjaka pred FISC-om (*amici*).

[77] https://www.pclob.gov/OversightProjects.

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.

[79] Uvodne izjave 176.–194. odluke o primjerenosti.

Kad je riječ o osnivanju Žalbenog suda za zaštitu podataka, 14. studenog 2023. za sud je imenovano osam sudaca (tj. dva suca više od najmanjeg broja koji je predviđen u Izvršnom nalogu br. 14086, koji je dopunjen uredbama glavnog državnog odvjetnika iz glave 28. članka 201.3. točke (a) Kodeksa saveznih propisa)[80]. Imenovani su na temelju kriterija i u skladu s postupkom koji su utvrđeni u Izvršnom nalogu br. 14086, među ostalim nakon savjetovanja s PCLOB-om i drugima[81]. Među njima su bivši suci saveznog okružnog suda i Žalbenog suda, bivši glavni državni odvjetnik SAD-a i bivši član PCLOB-a. U skladu s Izvršnim nalogom najmanje polovina sudaca ima prethodno sudačko iskustvo. Osim toga, u travnju 2024. imenovana su dva posebna odvjetnika, odnosno pravna stručnjaka za privatnost i nacionalnu sigurnost, koji zastupaju interese pojedinaca pred Žalbenim sudom za zaštitu podataka. Na sastanku za preispitivanje potvrđeno je da su svi suci i posebni odvjetnici prošli najvišu razinu sigurnosne provjere te zato mogu pristupiti klasificiranim materijalima pri obavljanju svojih zadaća za Žalbeni sud za zaštitu podataka. Žalbeni sud za zaštitu podataka također je objavio niz najčešćih pitanja, u kojima je dodatno pojasnio svoju ulogu, neovisnost i funkcioniranje[82].

Kad je riječ o rješavanju pritužbi, ODNI je 6. prosinca 2022. donio Direktivu 126. o obavještajnoj zajednici, u kojoj detaljno uređuje različite aspekte postupka istrage i odlučivanja o pritužbama (utvrđivanjem rokova, uspostavom sigurnog elektroničkog repozitorija i komunikacijskih kanala, zahtjevom da službenici za zaštitu građanskih sloboda i članovi obavještajne zajednice surađuju s PCLOB-om u kontekstu godišnjeg preispitivanja mehanizma pravne zaštite itd.)[83]. Ta se direktiva primjenjuje u cijeloj američkoj obavještajnoj zajednici, a dopunjena je dodatnim internim postupcima koje su obavještajne agencije donijele u pogledu suradnje sa službenikom za zaštitu građanskih sloboda ODNI-ja u kontekstu rješavanja pritužbi (npr. uspostava sigurnog repozitorija za razmjenu pritužbi i odgovarajućih dokumenata i sigurne komunikacije među relevantnim agencijama). Žalbeni sud za zaštitu podataka u narednim će mjesecima izdati detaljnija pravila o rješavanju pritužbi i drugim postupovnim aspektima.

U Europskoj uniji i Sjedinjenim Američkim Državama poduzet je niz dodatnih mjera kako bi se informirala šira javnost te olakšalo podnošenje i rješavanje pritužbi. Na primjer, Europski odbor za zaštitu podataka donio je informativnu obavijest o novom mehanizmu pravne zaštite[84], predložak obrasca za pritužbe (koji bi sva tijela za zaštitu podataka trebala prevesti i objaviti na svojim nacionalnim jezicima)[85] i poslovnik kojim se uređuje suradnja nacionalnih nadzornih tijela i tajništva EDPB-a[86]. Slično tomu, ODNI je objavio najčešća pitanja i

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Članak 3. točka (d)(A) Izvršnog naloga br. 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_hr.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_hr.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_hr.

informativni članak o novom mehanizmu pravne zaštite te je sudjelovao u aktivnostima informiranja javnosti[87].

Nadalje, protekle godine EDPB i relevantna američka tijela blisko su surađivali na nekoliko operativnih aspekata. Konkretno, kako je potvrđeno na sastanku za preispitivanje, uspostavili su šifrirani komunikacijski kanal za prosljeđivanje pritužbi od nacionalnih tijela u EU-u tajništvu EDPB-a, od tajništva EDPB-a službeniku za zaštitu građanskih sloboda ODNI-ja i za privatnost i građanske slobode pri Ministarstvu pravosuđa (OPCL) te između službenika za zaštitu građanskih sloboda ODNI-ja i drugih američkih tijela (npr. Žalbeni sud za zaštitu podataka). Osim toga, službenica za zaštitu građanskih sloboda ODNI-ja objasnila je da su uspostavljeni dodatni interni postupci za suradnju pojedinačnih obavještajnih agencija sa službenikom za zaštitu građanskih sloboda ODNI-ja u pogledu rješavanja pritužbi.

Naposljetku, OPCL, koji pruža administrativnu potporu Žalbenom sudu za zaštitu podataka, obavijestio je i da Žalbeni sud za zaštitu podataka djeluje u okviru vlastite namjenske proračunske linije i da ima potrebna sredstva za obavljanje svojih zadaća, uključujući sigurna računala i prijenosna računala, telefone itd. Osim toga, kako je propisano u Izvršnom nalogu br. 14086, Ministarstvo trgovine poduzelo je potrebne mjere, među ostalim uspostavom šifriranog komunikacijskog kanala sa službenikom za zaštitu građanskih sloboda ODNI-ja, kako bi se vodila evidencija o svim zaprimljenim pritužbama koje ispunjavaju uvjete. Ministarstvo trgovine povremeno će od službenika za zaštitu građanskih sloboda ODNI-ja tražiti potvrdu o tome jesu li informacije koje se odnose na pojedinačnu pritužbu deklasificirane. Ako jesu, Ministarstvo trgovine o tome će obavijestiti dotičnu osobu kako bi joj omogućio pristup takvim informacijama.

U vrijeme sastanka za preispitivanje nadzorna tijela EU-a nisu zaprimila nijednu pritužbu, pa novi mehanizam pravne zaštite još nije bio pokrenut.

3. ZAKLJUČAK

Na temelju informacija prikupljenih u okviru prvog preispitivanja Komisija zaključuje da su američka tijela uspostavila potrebne strukture i postupke kako bi osigurala djelotvorno funkcioniranje okvira za privatnost podataka. U tom kontekstu Komisija iznimno cijeni vrlo dobru suradnju s američkim tijelima u provedbi preispitivanja.

Iako je prvo preispitivanje razumljivo bilo usmjereno na provjeru jesu li uspostavljeni svi sastavni elementi okvira, iskustvo s praktičnom primjenom zaštitnih mjera koje se odnose i na obradu podataka koju provode certificirana poduzeća i na pristup javnih tijela podacima nužno je ograničeno nakon samo godine dana rada. Stoga će Komisija pomno pratiti relevantne događaje u sljedećim mjesecima i godinama, pri čemu će posebnu pozornost obratiti na 1. predstojeća izvješća PCLOB-a o provedbi Izvršnog naloga br. 14086 i funkcioniranju mehanizma pravne zaštite za prikupljanje obavještajnih podataka elektroničkim izviđanjem, posebno Žalbenog suda za zaštitu podataka, 2. moguće dodatne izmjene članka 702. Zakona o nadzoru stranih obavještajnih aktivnosti i 3. imenovanje članova PCLOB-a kako bi se popunila radna mjesta koja će se uskoro osloboditi.

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf i https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

Nadalje, kako bi se osiguralo trajno i djelotvorno funkcioniranje, Komisija smatra da je važno da:

- kako je najavljeno na sastanku za preispitivanje, Ministarstvo trgovine bolje iskoristi razna sredstva predviđena okvirom za privatnost podataka za nadzor usklađenosti poduzeća s Načelima i utvrđivanje lažnih izjave o sudjelovanju,
- FTC dodatno unaprijedi svoj proaktivan pristup istragama i provedbi mjera za osiguravanje usklađenosti certificiranih poduzeća s Načelima okvira za privatnost podataka, i
- Ministarstvo trgovine, FTC i tijela EU-a za zaštitu podataka izrade zajedničke smjernice o najvažnijim zahtjevima Načela okvira za privatnost podataka, npr. u pogledu podataka o ljudskim resursima i daljnjim prijenosima.

S obzirom na taj ishod preispitivanja i kako je predviđeno u uvodnoj izjavi 211. odluke o primjerenosti, Komisija smatra da sljedeće periodično preispitivanje treba provesti nakon tri godine. Tako bi se omogućilo stjecanje više iskustva u praktičnoj primjeni okvira za privatnost podataka vodeći računa o spomenutom budućem razvoju događaja. Stoga će se Komisija, u skladu s člankom 3. stavkom 4. odluke o primjerenosti, o periodičnosti budućih preispitivanja savjetovati s Europskim odborom za zaštitu podataka i Odborom osnovanim na temelju članka 93. stavka 1. Opće uredbe o zaštiti podataka.