EIROPAS
KOMISIJA

Briselē, 9.10.2024.
COM(2024) 451 final

KOMISIJAS ZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

par lēmuma par personas datu pietiekamu aizsardzības līmeni ES un ASV datu privātuma regulējuma ietvaros pirmo periodisko pārskatīšanu

1. PIRMĀ PERIODISKĀ PĀRSKATĪŠANA – PRIEKŠVĒSTURE, SAGATAVOŠANA UN PROCESS

Komisija 2023. gada 10. jūlija lēmumā ("lēmums par aizsardzības līmeņa pietiekamību") konstatēja, ka ES un ASV datu privātuma regulējums (DPR) nodrošina pietiekamu aizsardzības līmeni personas datiem, kas no Eiropas Savienības nosūtīti organizācijām Amerikas Savienotajās Valstīs[1]. Lēmumā par aizsardzības līmeņa pietiekamību noteikts, ka Komisijai ir jāveic periodiska pārskatīšana, un pirmajai no tām būtu jānotiek pēc viena gada no dienas, kad lēmums par aizsardzības līmeņa pietiekamību ir paziņots dalībvalstīm. Šis ziņojums noslēdz šo pirmo pārskatīšanu.

Kā norādīts lēmuma par aizsardzības līmeņa pietiekamību 211. apsvērumā, šī pirmā pārskatīšana, kas notiek pēc jaunā regulējuma pirmā darbības gada, bija vērsta uz to, lai pārbaudītu, vai visi regulējumā paredzētie elementi ir īstenoti un darbojas rezultatīvi. Pārskatīšana aptvēra visus regulējuma darbības aspektus, arī ņemot vērā juridiskās norises, kas notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas.

Sagatavojot šo pārskatīšanu, Komisija apkopoja informāciju no attiecīgajām ieinteresētajām personām, īpaši no nevalstiskajām organizācijām (NVO), kurām ir speciālās zināšanas digitālo tiesību un privātuma jomā[2], no DPR jomā sertificētām organizācijām – ar attiecīgo tirdzniecības apvienību starpniecību[3], kā arī no ASV iestādēm, kas iesaistītas regulējuma īstenošanā. Turklāt Komisija ir arī apkopojusi atsauksmes, kas saņemtas no plašas sabiedrības pēc īpaša uzaicinājuma iesniegt atsauksmes portālā "Izsakiet viedokli"[4].

Pārskatīšanas sanāksme notika Vašingtonā 2024. gada 18. un 19. jūlijā. To atklāja ES tieslietu un patērētāju komisārs Didjē Reinderss un ASV tirdzniecības sekretāre Džīna Reimondo[5].

Attiecībā uz ES pārskatīšanu veica Eiropas Komisijas Tiesiskuma un patērētāju ģenerāldirektorāta pārstāvji kopā ar pieciem Eiropas Datu aizsardzības kolēģijas (EDAK)

---

[1] Komisijas Īstenošanas lēmums (ES) 2023/1795 (2023. gada 10. jūlijs), kas pieņemts, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, par personas datu pietiekamu aizsardzības līmeni ES un ASV datu privātuma regulējuma ietvaros.

[2] Komisija nosūtīja anketu deviņām NVO ("*Human Rights Watch*", Amerikas Pilsonisko brīvību savienībai, Amerikas Patērētāju federācijai, Digitālās demokrātijas centram, *New America Open Technology Institute*, *Access Now*, *Electronic Frontier Foundation*, Elektroniskās privātuma informācijas centram, Demokrātijas un tehnoloģiju centram), kurā galvenā uzmanība bija pievērsta attiecīgajām norisēm ASV tiesiskajā regulējumā, pārraudzības un izpildes mehānismiem un tiesiskās aizsardzības mehānismu darbībai. Komisijas dienesti un EDAK pārstāvji 2024. gada 9. jūlijā arī tikās ar šīm NVO tiešsaistē.

[3] Komisija nosūtīja anketu deviņām tirdzniecības asociācijām (*Software & Information Industry Association*, ASV Tirdzniecības kamerai (*U.S. Chamber of Commerce*), Informācijas tehnoloģiju nozares padomei (*Information Technology Industry Council*), *Software Alliance*, *Centre for Information Policy Leadership*, *Interactive Advertising Bureau*, *United States Council for International Business*, *Computer and Communications Industry Association* un asociācijai *Engine*), kurā galvenā uzmanība bija pievērsta DPR jomā sertificēto uzņēmumu pieredzei, īpaši sertifikācijas procesam, pasākumiem, kas veikti, lai ievērotu DPR principus, mehānismiem fizisku personu pieprasījumu un sūdzību izskatīšanai utt.

[4] Saņemtās atsauksmes ir atrodamas, izmantojot šo saiti: 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_lv.

[5] Pārskatīšanas sanāksme bija organizēta pēc tematiem, un pirms katra īpašā darba kārtības punkta attiecīgā ASV iestāde, ES pārstāvis vai organizācija sniedza īsu izklāstu par to, kam sekoja detalizētu jautājumu un atbilžu sesija. Regulējuma "komerciālie aspekti" (t. i., to prasību piemērošana un izpilde, kas attiecas uz uzņēmumiem, kuri sertificēti saskaņā ar DPR) tika aptverti pirmajā dienā, savukārt otrajā dienā tika apspriesti jautājumi par valdības piekļuvi personas datiem.

ieceltiem pārstāvjiem no dažādām valstu datu aizsardzības iestādēm (DAI) un Eiropas Datu aizsardzības uzraudzītājs[6]. No ASV piedalījās pārstāvji no Tirdzniecības ministrijas (*DoC)*, Valsts departamenta, Federālās tirdzniecības komisijas (*FTC*), Transporta ministrijas (*DoT*), Nacionālās izlūkošanas direktora biroja (*ODNI*), Tieslietu ministrijas (*DoJ*), kā arī Izlūkdienestu ģenerālinspektors un Privātuma un pilsonisko brīvību pārraudzības padomes (*PCLOB*) locekļi. Turklāt attiecīgo pārskatīšanas sesiju laikā informāciju sniedza pārstāvji no organizācijām, kuras sniedz neatkarīgus strīdu izšķiršanas pakalpojumus, un Amerikas Šķīrējtiesu asociācijas. Turklāt pārskatīšanas gaitā informāciju par to, kā uzņēmumi ievēro regulējuma prasības sniedza arī DPR jomā sertificētu organizāciju prezentācijas.

Komisija konstatējumu izdarīšanai papildu informāciju ieguva no publiski pieejamiem materiāliem, piemēram, tiesas nolēmumiem, attiecīgo ASV iestāžu īstenošanas noteikumiem un procedūrām, nevalstisko organizāciju ziņojumiem un pētījumiem, DPR jomā sertificēto uzņēmumu izdotajiem pārredzamības ziņojumiem, neatkarīgu pārraudzības struktūru gada ziņojumiem, kā arī mediju ziņojumiem.

2. KONSTATĒJUMI

2.1. Komerciāli aspekti

2.1.1. Sertifikācijas process

Lai varētu saņemt personas datus, kas nosūtīti no ES, pamatojoties uz DPR, ASV uzņēmumam ir jāveic sertifikācija un pēc tam reizi gadā no jauna jāapliecina *DoC*, ka tas ievēro īpašas datu aizsardzības prasības ("DPR principi"). Sertifikācija paredz, ka uz uzņēmumu attiecas *FTC* vai *DoT* izmeklēšanas un izpildes pilnvaras, tas publiski paziņo par savu apņemšanos ievērot DPR principus un publiski atklāj savu privātuma politiku un pilnībā īsteno minētās prasības[7]. Pirms sertifikācijas pabeigšanas *DoC* pārbauda, vai uzņēmums ir izpildījis visas sertifikācijas prasības[8].

Pārskatīšanas sanāksmē *DoC* paskaidroja, ka šajā DPR pirmajā darbības gadā galvenā uzmanība tika pievērsta sertifikācijas procesa ieviešanai, tajā skaitā īpašu IT rīku izstrādei, procedūru atjaunināšanai, sadarbībai ar uzņēmumiem un citu informēšanas / izpratnes veicināšanas pasākumu veikšanai. Līdz pārskatīšanas sanāksmes dienai vairāk nekā 2800 uzņēmumu ir sertificēti saskaņā ar DPR. Tas nozīmē, ka pirmajā darbības gadā attiecībā uz DPR tika sertificēti vairāk uzņēmumu nekā saskaņā ar iepriekšējo regulējumu – privātuma vairogu[9]. Saskaņā ar *DoC* sniegto informāciju 70 % dalībnieku ir MVU un liels skaits DPR īstenojošo uzņēmumu (47 %) darbojas informācijas, komunikācijas un tehnoloģiju (IKT) nozarē. Turklāt 60 % uzņēmumu ir sertificēti tikai attiecībā uz datiem, kas nav cilvēkresursu dati, 2,5 % uzņēmumu ir sertificēti tikai attiecībā uz cilvēkresursu datiem un 37,5 % ir sertificēti gan attiecībā uz cilvēkresursu datiem, gan datiem, kas nav cilvēkresursu dati.

DoC ir pieņēmusi procedūras, kas vajadzīgas, lai izskatītu uzņēmumu pieteikumus. Uzņēmumiem sertifikācijas pieteikumi jāiesniedz *DoC* DPR tīmekļa vietnē (https://www.dataprivacyframework.gov/). Tajā ir iekļauta informācija par to, kā pievienoties

[6] Komisijas un EDAK pārstāvji tikās 2024. gada 12. jūnijā un 10. jūlijā, lai sagatavotos pārskatīšanai, apspriestu saņemto informāciju un noteiktu, kuriem aspektiem nepieciešama papildu informācijas vākšana un precizēšana.
[7] Lēmuma par aizsardzības līmeņa pietiekamību I pielikuma I.2. iedaļa.
[8] Lēmuma par aizsardzības līmeņa pietiekamību III pielikums.
[9] Tādā pašā periodā privātuma vairoga ietvaros bija sertificēti 2400 uzņēmumi.

DPR[10], un par uzņēmuma pienākumiem saskaņā ar regulējumu[11]. Īpaša *DoC* komanda, par kuru atbild īpašs datu privātuma regulējuma direktors, ir atbildīga par visiem aspektiem, kas saistīti ar DPR pārvaldību un administrēšanu, kā arī par sertifikācijas procesu un atbilstības uzraudzību. Katru pieteikumu piešķir konkrētam darbiniekam, kas ir atbildīgs par attiecīgo uzņēmumu visā sertifikācijas procesā.

Lai iegūtu sertifikāciju, uzņēmumi iesniedz savu pieteikumu, ieskaitot privātuma politikas projektu. *DoC* pārbauda, vai tas atbilst attiecīgajām DPR prasībām. Ja organizācijas vēlas sertificēt dažādas struktūras uzņēmumu grupā (piemēram, dažādus meitasuzņēmumus), *DoC* lūdz iesniegt un pārskata vai nu vienu visaptverošu privātuma politiku, kurā ir skaidri norādītas visas aptvertās struktūras, vai atsevišķu politiku katrai struktūrai. *DoC* arī pārbauda pieteikumā norādītajā neatkarīgajā tiesību aizsardzības mehānismā (*IRM*)[12], vai organizācija tajā faktiski ir reģistrējusies. Attiecībā uz uzņēmumiem, kas izvēlas datu aizsardzības iestādes darba grupu (piemēram, tāpēc, ka uzņēmumi apstrādā cilvēkresursu datus), *DoC* pārbauda, vai uzņēmums ir samaksājis noteikto maksu, lai varētu izmantot darba grupu. Vajadzības gadījumā *DoC* arī pārbauda, vai uz pieteikuma iesniedzēju attiecas *FTC* vai *DoT* jurisdikcija (un tāpēc tam ir tiesības pievienoties DPR).

Ja visi nosacījumi ir izpildīti, *DoC* informē organizāciju, ka tā savā tīmekļa vietnē var publicēt savu privātuma politiku, atsaucoties uz DPR. Tiklīdz privātuma politika ir publiski pieejama, *DoC* apstiprina sertifikāciju un iekļauj uzņēmumu DPR sarakstā savā tīmekļa vietnē. Sākot no dienas, kad *DoC* iekļauj organizāciju minētajā sarakstā[13], var atsaukties uz DPR, lai saņemtu personas datus no ES.

Kā paskaidrots pārskatīšanas sanāksmē, līdz šim *DoC* veikto pārbaužu rezultātā tika noraidīti 33 pieteikumi, jo tie nebija atbilstoši DPR prasībām. Parasti *DoC* sadarbojas ar uzņēmumu, lai novērstu visus trūkumus. Ja *DoC* konstatē trūkumus, tā informē uzņēmumu, ka tie ir jānovērš un ka gadījumā, ja atbilde netiek sniegta noteiktajā termiņā vai kā citādi pašsertifikācija netiek pabeigta saskaņā ar *DoC* procedūrām, pieteikums tiek uzskatīts par atsauktu. Ja 12 mēnešu laikā sākotnējā sertifikācija nav pabeigta / nav novērsti trūkumi, *DoC* uzskata, ka tā ir atsaukta.

Ikgadējās atkārtotās sertifikācijas termiņš katram uzņēmumam ir norādīts DPR sarakstā. Lai atgādinātu uzņēmumiem, ka ir jāpiesakās atkārtotai sertifikācijai, *DoC* ir izveidojusi sistēmu ar atgādinājumiem, ka sertifikācijas termiņš drīz beigsies. Organizācijas saņem atgādinājumu vienu mēnesi pirms, pēc tam divas nedēļas pirms un pēc tam vienu dienu pirms termiņa. Uzņēmumi, kuru sertifikācija vairs nav spēkā, tiek svītroti no DPR saraksta. Kā aprakstīts lēmuma par aizsardzības līmeņa pietiekamību III pielikumā, *DoC* tīmekļa vietnē ir īpaša sadaļa, kurā uzskaitītas ASV organizācijas, kuras vairs aktīvi nepiedalās regulējumā, un norādīti attiecīgie iemesli (piemēram, sertifikācijas izbeigšanās vai izstāšanās no DPR); attiecīgie uzņēmumi tiek svītroti no saraksta (“neaktīvais saraksts”). Kad organizācijas tiek svītrotas no DPR saraksta, jo tās ir pieļāvušas to sertifikācijas izbeigšanos, *DoC* sazinās ar tām, lai apstiprinātu, vai tās vēlas izstāties vai arī plāno atkārtoti iegūt sertifikāciju, un, ja tās vēlas veikt atkārtotu sertifikāciju, pārbaudītu, vai pēc termiņa beigām tās ir piemērojušas DPR principus personas datiem, kas saņemti saskaņā ar DPR, un precizētu, kādus pasākumus tās

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

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

[12] Privātā sektora strīdu izšķiršanas mehānismi, ar kuru palīdzību tiek izmeklētas un ātri atrisinātas katras fiziskās personas sūdzības un strīdi, neradot izmaksas attiecīgajai fiziskajai personai.

[13] Lēmuma par aizsardzības līmeņa pietiekamību I pielikuma I iedaļas 3. punkts.

veiks, lai risinātu neatrisinātos jautājumus, kas aizkavēja to atkārtotu sertifikāciju. Ja uzņēmumi paziņo *DoC*, ka vēlas izstāties no DPR, *DoC* lūdz tiem apstiprināt, vai tie atgriezīs saskaņā ar DPR saņemtos datus vai dzēsīs tos; saglabās tos un turpinās piemērot DPR principus šādiem datiem (kas jāapstiprina katru gadu); vai saglabās tos un ieviesīs citus aizsardzības pasākumus (piemēram, Eiropas Komisijas pieņemtās līguma standartklauzulas).

No tirdzniecības asociācijām un uzņēmumiem saņemtās atsauksmes liecina, ka DPR jomā sertificētie uzņēmumi ir veikuši vairākus pasākumus, lai nodrošinātu atbilstību DPR principiem. Piemēram, lai ievērotu *tiesību aizsardzības, izpildes panākšanas un atbildības principu*, organizācijas ir veikušas iekšējas pārbaudes, izmantojot pašnovērtējumu vai ārēju atbilstības pārbaudi. Divi privātā sektora *IRM*, kas piedalījās pārskatīšanas sanāksmē, paskaidroja, ka nodrošina arī ārēju atbilstības pārbaudi, kurā pārskata privātuma politiku, un viens no privātā sektora *IRM* paskaidroja, ka nodrošina arī revīzijas un izlases veida pārbaudes, kas koncentrējas, piemēram, uz *piekļuves*, *izvēles* un *tālākas nosūtīšanas* principiem. Turklāt sertificēti uzņēmumi ir izstrādājuši iekšējās atbilstības programmas un pārraudzības mehānismus, apmācījuši darbiniekus, īstenojuši mehānismus, lai fiziskas personas varētu izmantot savas tiesības, veikuši privātuma ietekmes novērtējumus un pārskatījuši spēkā esošos līgumus.

2.1.2. Atbilstības uzraudzība, nepatiesi apgalvojumi par dalību un izpilde

Saskaņā ar DPR *DoC* ir atbildīga par DPR principu ievērošanas uzraudzību un šim mērķim izmanto dažādus instrumentus, ieskaitot *ex-officio* pārbaudes (pēc savas iniciatīvas), *ad hoc* pārbaudes uz vietas un atbilstības anketas. Tas ietver nepatiesu apgalvojumu par dalību regulējumā meklēšanu un reaģēšanu uz tiem, piemēram, veicot meklēšanu internetā[14].

Lai uzraudzītu DPR jomā sertificētu uzņēmumu atbilstību DPR principiem, *DoC* pagājušajā gadā galvenokārt ir paļāvusies uz *ad hoc* meklēšanu tīmeklī un (sociālo) mediju pārbaudēm. *DoC* ziņoja, ka šajā pirmajā gadā tā nav konstatējusi problēmas saistībā ar atbilstību DPR principiem un ne par vienu uzņēmumu nav vērsusies *FTC* vai *DoT* iespējamu izpildes darbību veikšanai. *DoC* ir arī izveidojusi īpašu kontaktpunktu, lai atvieglotu sadarbību ar DAI un saņemtu sūdzības no fiziskām personām un citu iestāžu (piemēram, DAI vai *FTC*) pieprasījumus. Tomēr pēdējā gada laikā nav saņemti pieprasījumi vai sūdzības. Lai gan šajā DPR pirmajā darbības gadā galvenā uzmanība tika pievērsta regulējuma un sertifikācijas procesa izveidei, *DoC* pārskatīšanas sanāksmē paskaidroja, ka tā plāno veikt atbilstības pārbaudes ar automatizētiem līdzekļiem, lai tās veiktu sistemātiskāk, un pašlaik izstrādā šim nolūkam nepieciešamos IT rīkus.

Komisija atzīst, ka *DoC* šajā pirmajā gadā bija jākoncentrē centieni uz regulējuma un sertifikācijas procesa izveidi. Turpinot darbu, *DoC* būtu jāpastiprina centieni uzraudzīt un pārbaudīt principu ievērošanu, kas ir priekšnosacījums, lai nodrošinātu pastāvīgu augstu atbilstības līmeni regulējumam un konstatētu tos gadījumus, ieskaitot iespējamus nepatiesus apgalvojumus par uzņēmumu līdzdalību, kad nepieciešama turpmāka izpildes darbība. Šajā sakarā Komisija atzinīgi vērtē to, ka *DoC* apstiprināja savu nolūku izstrādāt un izmantot (automatizētus) rīkus, lai efektīvāk un sistemātiskāk identificētu atbilstības problēmas un nepatiesus apgalvojumus, un uzskata, ka tam vajadzētu būt daļai no plašākiem centieniem vairāk izmantot dažādos tās rīcībā esošos instrumentus (piemēram, pārbaudes uz vietas,

[14] Sk. lēmuma par aizsardzības līmeņa pietiekamību III pielikumu. Nepatiesi apgalvojumi var rasties, piemēram, ja uzņēmums apgalvo, ka piedalās DPR, un tas vai nu nekad nav uzsācis sertifikācijas procesu, vai ir to sācis, bet nav pabeidzis, vai ir pieļāvis tā sertifikācijas izbeigšanos.

atbilstības pārskatīšanas anketas, informācijas pieprasījumus utt.), arī, lai pārbaudītu atbilstību konkrētām prasībām saskaņā ar DPR[15].

Uz DPR jomā sertificētām organizācijām attiecas *FTC* un *DoT* jurisdikcija. Pārskatīšanas sanāksmē *DoT* apstiprināja, ka ir ieviesti visi procesi, lai veiktu atbilstošus izpildes pasākumus. Tā arī paskaidroja, ka DPR ir pievienojušies ļoti maz uzņēmumu, kas ir tās jurisdikcijā (t. i., daži biļešu pārdevēji, bet nav lidsabiedrību). *FTC* apstiprināja, ka katrā ar privātumu saistītā izmeklēšanā tā sistemātiski pārbauda DPR pārkāpumus. Līdz šim *FTC* nav saņēmusi nevienu pieprasījumu no citām iestādēm. Tā ir saņēmusi dažas sūdzības, kurās minēts DPR, lai gan divas no tām attiecās uz "neaktīvajā sarakstā" iekļautajiem uzņēmumiem, divas attiecās uz uzņēmumiem, kas nepiedalījās regulējumā, un viena neattiecās uz personas datiem, kas nosūtīti no ES. Pārskatīšanas laikā *FTC* nebija pieņēmusi lēmumus, lai panāktu atbilstību DPR, lai gan tā apstiprināja, ka pašlaik tiek izmeklēti vairāki DPR jomā sertificēti uzņēmumi.

Komisija atzinīgi vērtē to, ka *FTC* visās ar privātumu saistītās izmeklēšanās sistemātiski pārbauda DPR pārkāpumus. Tā kā DPR turpmāka efektivitāte ir atkarīga no tā stingras izpildes, paredzams, ka *FTC* turpinās īstenot savas izmeklēšanas pilnvaras saskaņā ar regulējumu, arī proaktīvi veicot kontrolreidus, kas vērsti uz atbilstību konkrētām DPR prasībām un/vai konkrētām nozarēm.

2.1.3. Sūdzību izskatīšana

DPR nodrošina ES fiziskām personām dažādas tiesiskās aizsardzības iespējas gadījumos, kad sertificētas organizācijas neievēro DPR principus[16]. Tas ietver risinājuma meklēšanu, tieši sazinoties ar DPR organizāciju, kurai 45 dienu laikā jāsniedz atbilde ietekmētajai fiziskajai personai. Fiziskas personas var arī iesniegt sūdzību *IRM*, kuru organizācija izraudzījusies sūdzību izmeklēšanai un atrisināšanai. Atkarībā no apstākļiem tā varētu būt vai nu strīdu alternatīvas izšķiršanas struktūra vai DAI[17]. Visbeidzot, ja datu subjekta sūdzība nav apmierinoši atrisināta ne ar vienu citu pieejamo tiesiskās aizsardzības līdzekli, fiziskas personas kā galēju tiesību aizsardzības mehānismu var izmantot iespēju pieprasīt saistošu šķīrējtiesu, ko spriež ES un ASV DPR kolēģija.

2.1.3.1. Sūdzību izskatīšana uzņēmumos

Tirdzniecības asociāciju un uzņēmumu atbildes uz Komisijas nosūtītajām anketām liecina, ka DPR jomā sertificētie uzņēmumi ir saņēmuši ļoti maz sūdzību (ja tādas ir) no fiziskām personām par neatbilstību DPR principiem. Tajā pašā laikā uzņēmumi ir ieviesuši dažādus mehānismus un rīkus, kas paredzēti tam, lai personas varētu izmantot savas tiesības un iesniegt sūdzības, arī izmantojot tīmeklī ievietotas veidlapas, e-pastu un tālruni.

2.1.3.2. *Neatkarīgi tiesību aizsardzības mehānismi (*IRM*)*

Pārskatīšanas sanāksmē saņemtās atsauksmes un tirdzniecības asociāciju sniegtā informācija liecina, ka ir bijis ļoti maz sūdzību, kas iesniegtas neatkarīgiem noregulējuma mehānismiem. Uzņēmumu izraudzītie *IRM* ietver *BBB National Programs JAMS*, *TRUSTe* un *VeraSafe*. DPR

[15] Piemēram, attiecībā uz tālāku nosūtīšanu, šim mērķim izmantojot iedaļas "DPR principi" 3. punkta b) apakšpunktā paredzēto iespēju pieprasīt attiecīgo līgumu par tālāku nosūtīšanu privātuma noteikumu kopsavilkumu vai reprezentatīvu kopiju.

[16] Sk. lēmuma par aizsardzības līmeņa pietiekamību 2.4. iedaļu.

[17] DPR organizācijām ir pienākums sadarboties, kad DAI veic izmeklēšanu un risina sūdzību – gan tad, ja tā attiecas uz cilvēkresursu datu apstrādi, kuri savākti saistībā ar darba tiesiskajām attiecībām, gan tad, ja attiecīgā organizācija ir brīvprātīgi piekritusi pārraudzībai, ko veic DAI.

ir noteikts, ka *IRM* jāpublicē gada ziņojums ar apkopotu statistiku par to strīdu izšķiršanas pakalpojumu izmantošanu. Šā ziņojuma pieņemšanas laikā visi attiecīgie *IRM* ir publicējuši savus gada ziņojumus[18].

Turklāt pārskatīšanas sanāksmē *BBB* un *VeraSafe* sniedza detalizētu izklāstu par savu darbību kopš pagājušā gada. Tie ziņoja, ka salīdzinājumā ar iepriekšējiem regulējumiem ir palielinājies uzņēmējdarbības dalībnieku skaits, kuri izvēlas to pakalpojumus, un minēja, ka ir saņēmuši dažas sūdzības, lai gan lielākā daļa no tām bija neatbilstīgas. Piemēram, *BBB* no ES fiziskām personām saņēma 87 sūdzības, no kurām tikai divas bija pieņemamas izskatīšanai. Lai gan *BBB* paskaidroja, ka sūdzības tiek izskatītas vidēji piecās darba dienās, šīs divas sūdzības galu galā tika slēgtas, jo attiecīgās personas nesniedza atbildes. *VeraSafe* saņēma 26 sūdzības, no kurām sešas bija pieņemamas izskatīšanai. Divas no tām attiecās uz piekļuves un dzēšanas pieprasījumiem un tika atrisinātas, bet divas joprojām nav izskatītas un divas tika atsauktas vai slēgtas, jo persona nesniedza atbildi. Abi *IRM* paskaidroja, ka to mērķis ir atbildēt uz sūdzībām personas dzimtajā valodā.

DPR uzņēmumiem, kas apstrādā no ES nosūtītos cilvēkresursu datus, kā *IRM* šiem datiem ir jāizvēlas ES DAI, savukārt DPR uzņēmums var brīvprātīgi izvēlēties ES DAI kā savu *IRM* cita veida personas datiem, kas nosūtīti, pamatojoties uz DPR. Faktiski vairāk nekā puse uzņēmumu, kas pārskatīšanas laikā sertificēti saskaņā ar DPR, izvēlējās šo risinājumu[19], kas ir atzinīgi vērtējama tendence. Kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas EDAK ir pieņēmusi "ES DAI neformālās darba grupas" reglamentu. Darba grupas kompetencē ir sniegt saistošus ieteikumus ASV organizācijām pēc neatrisinātām fizisku personu sūdzībām par tādu personas datu apstrādi, kas nosūtīti no ES saskaņā ar DPR. Saskaņā ar tās reglamentu darba grupu veido viena DAI, kas darbojas kā vadošā DAI, un citas izraudzītās papildu pārskatītājas DAI[20]. Darba grupa 60 dienu laikā pēc DPR sūdzības saņemšanas sniedz saistošu ieteikumu. EDAK arī ir publicējusi sūdzības veidlapas veidni, kas paredzēta sūdzību

[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 DPR pakalpojumi – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;

TRUSTe strīdu izšķiršana – 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.

[19] Neilgi pēc pārskatīšanas sanāksmes dienas DPR tīmekļa vietnē bija norādīts, ka 1511 no 2892 dalībniekiem kā tiesību aizsardzības mehānismu ir izraudzījušies ES datu aizsardzības iestādi.

[20] EDAK 2024. gada 17. aprīlī saskaņā ar ES un ASV datu privātuma regulējumu pieņēma "ES DAI neformālās darba grupas" reglamentu. Tas ir pieejams šeit: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

iesniegšanai DAI[21], kā arī sadaļu "Bieži uzdoti jautājumi par DPR", kas adresēta Eiropas fiziskām personām[22] un uzņēmumiem[23]. Pārskatīšanas laikā darba grupa nebija saņēmusi nevienu sūdzību.

2.1.3.3. Saistošais arbitrāžas mehānisms

Saistošā šķīrējtiesas mehānisma pārvaldībai *DoC* izvēlējās Starptautisko strīdu izšķiršanas centru (*ICDR*), kas ir Amerikas Šķīrējtiesu asociācijas starptautiskā nodaļa. Pēc lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas *DoC* kopā ar Komisiju izraudzījās 11 šķīrējtiesnešus ar pieredzi privātuma jomā un no dažādām vidēm, tajā skaitā šķīrējtiesām, tiesu iestādēm, akadēmiskajām aprindām un pilsoniskās sabiedrības[24]. Turklāt ir pieņemti DPR kolēģijas šķīrējtiesas noteikumi[25] un šķīrējtiesnešu rīcības kodekss[26], un visi šie dokumenti ir pieejami *ICDR* tīmekļa vietnē. Pārskatīšanas laikā šķīrējtiesas mehānismu vēl nebija izmantojusi neviena fiziska persona ES.

2.1.4. Norādījumi, sadarbība un izpratnes veicināšana

Kopš DPR stāšanās spēkā *DoC* ir veikusi dažādus izpratnes veicināšanas pasākumus, šajā nolūkā organizējot izbraukuma prezentācijas, tīmekļseminārus un konferences, kā arī vēršoties pie arodapvienībām un tieši sadarbojoties ar vairāk nekā 3000 uzņēmumiem, lai sniegtu informāciju par DPR. Tā arī ir publicējusi norādījumus, arī bieži uzdotu jautājumu veidā, kas adresēti fiziskām personām, kā arī ES un ASV uzņēmumiem[27]. Savukārt EDAK ir izstrādājusi sūdzību veidlapas un bieži uzdotos jautājumus, kas adresēti fiziskām personām un uzņēmumiem. Tāpat, kad Komisija pieņēma lēmumu par aizsardzības līmeņa pietiekamību, tā publicēja jautājumu un atbilžu un faktu lapu par DPR[28].

Tajā pašā laikā pārskatīšanas sanāksmē atklājās, ka ir jādara vairāk, lai veicinātu izpratni fizisku personu vidū un sniegtu norādījumus uzņēmumiem. No uzņēmumiem un *IRM* saņemtā informācija un ļoti nelielais sūdzību skaits liecina, ka fiziskas personas, iespējams, ne vienmēr ir informētas par savām tiesībām un/vai to izmantošanas mehānismu. Pārskatīšanas sanāksmē *DoC* pauda interesi sadarboties ar ES DAI, lai uzlabotu ES fizisko personu izpratni par regulējumu. Komisija mudina īstenot šādas iniciatīvas un arī veic pasākumus, lai labāk informētu fiziskas personas, arī tādējādi, ka savā tīmekļa vietnē sniedz papildu informāciju par DPR, piemēram, iekļaujot saites un atsauces uz attiecīgajiem norādījumu dokumentiem, ko pieņēmusi EDAK, *DoC* un citas ASV iestādes.

Attiecībā uz norādījumiem par DPR principiem EDAK pārstāvji pārskatīšanas sanāksmē vienojās turpmākajos mēnešos sadarboties, lai sniegtu papildu skaidrojumus par cilvēkresursu datu jēdzienu saskaņā ar DPR un konkrētiem pienākumiem, kas attiecas uz šādu datu apstrādi.

---

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en.

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en.

[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en.

[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.

[27] Sk., piemēram, https://www.dataprivacyframework.gov/US-Businesses.

[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

Tika izpētīti dažādi elementi, kas jāiekļauj šādos norādījumos. Piemēram, šajos norādījumos varētu pievērsties konkrētiem praktiskiem scenārijiem, kad darbinieku dati tiktu apstrādāti saskaņā ar DPR (piemēram, to veic mākoņdatošanas pakalpojumu sniedzējs), un paskaidrot, kuri scenāriji būtu būtiski. Turklāt tā varētu ieteikt uzņēmumiem, kas saņem darbinieku datus attiecībā uz ES fiziskām personām (bet ne vienmēr izmanto šādus datus darba attiecību kontekstā), izvēlēties DAI darba grupu par savu *IRM*. Tas nodrošinātu, ka šīs fiziskās personas varētu vērsties iestādē, kas ir "tuvu mājām" un vajadzības gadījumā labāk pārzina piemērojamos valsts tiesību aktus, kas attiecas uz cilvēkresursu datiem.

Turklāt konkrēts aspekts, par kuru varētu būt lietderīgi sniegt vairāk norādījumu (pamatojoties arī uz informāciju, kas saņemta no arodapvienībām), attiecas uz DPR prasībām attiecībā uz tālāku nosūtīšanu. Turklāt *DoC* norādīja, ka būtu vērts izpētīt, vai dažas nozares varētu gūt labumu no papildu norādījumiem par DPR principu piemērošanu to darbībām, piemēram, veselības pētniecības un finanšu pakalpojumu jomā.

Komisija atzinīgi vērtē abu pušu gatavību izstrādāt norādījumus un sagaida, ka drīz sāksies darbs saistībā ar iepriekš minētajiem tematiem.

Vispārīgāk runājot, ir izveidoti vairāki mehānismi, lai nodrošinātu apmaiņu un sadarbību starp ASV iestādēm un DAI, arī, ieceļot īpašas kontaktpersonas no *FTC* un *DoC* DAI jautājumu un pieprasījumu izskatīšanai.

2.1.5. Attiecīgās izmaiņas ASV tiesību sistēmā

Kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas ir notikušas vairākas izmaiņas ASV tiesiskajā regulējumā privātuma jomā. Tās ietver leģislatīvas izmaiņas, regulējuma un judikatūras izmaiņas. Kopumā tās liecina par lielāku konverģenci starp ES un ASV pieejām konkrētām privātuma problēmām, arī tādējādi, ka tiek izmantoti līdzīgi juridiskie jēdzieni. Dažas no šīm izmaiņām joprojām notiek, un tās būs jāturpina uzraudzīt.

Federālā līmenī prezidents izdeva vairākus izpildrīkojumus (IR), kas attiecas uz personas datu izmantošanu. Konkrētāk, ar 2024. gada 28. februāra Izpildrīkojumu Nr. 14117[29] ir aizliegti vai ierobežoti darījumi, kas saistīti ar konkrētu kategoriju sensitīviem personas datiem (piemēram, veselības datiem, biometriskajiem identifikatoriem, cilvēka genoma datiem), ar struktūrām dažās "problemātiskās valstīs"[30]. Pieņemtajā rīkojumā ģenerālprokuroram ir uzdots ierosināt noteikumus, kas vēl jāpieņem šā ziņojuma pieņemšanas laikā, lai sīkāk precizētu rīkojuma īstenošanu. Turklāt 2023. gada 30. oktobra Izpildrīkojumā Nr. 14110 par mākslīgo intelektu[31] galvenā uzmanība ir pievērsta droša, neapdraudēta un uzticama mākslīgā intelekta attīstībai. Tajā paredzēts, ka vairākām federālajām aģentūrām ir jāizstrādā ar MI saistīti drošības standarti un pamatnostādnes, arī par konkrētiem MI riskiem privātumam un privātuma saglabāšanas metodēm.

---

[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] Kā ierosinājis ģenerālprokurors iepriekšējā paziņojumā par ierosināto noteikumu izstrādi, kas izdots 2024. gada 3. maijā, to vidū ir Ķīna, Kuba, Honkonga un Makao, Irāna, Ziemeļkoreja un Venecuēla. Sk. 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.

Attiecībā uz likumdošanas darbu jānorāda, ka, lai gan pēdējos gados Kongresā ir ieviesti federālie privātuma likumprojekti, 20 ASV pavalstis no 2024. gada jūlija ir ieviesušas visaptverošus privātuma tiesību aktus, no kuriem astoņi ir stājušies spēkā attiecīgi šādās pavalstīs: Kalifornija, Kolorādo, Oregona, Virdžīnija, Konektikuta, Jūta, Teksasa un Florida. Turklāt 17 ASV pavalstis ir pieņēmušas tiesību aktus, kas attiecas uz automatizētu apstrādi (vai vismaz dažiem tās veidiem) un parasti pieļauj atteikšanos no konkrētu veidu lēmumu pieņemšanas, pamatojoties uz "profilēšanu"[32].

Attiecībā uz judikatūras izmaiņām vairāki pilsoniskās sabiedrības pārstāvji ir norādījuši uz neseno Augstākās tiesas spriedumu lietā *Loper Bright Enterprises / Raimondo* (2024. gada 28. jūnijs). Ar šo spriedumu tiek atcelta iepriekšējā judikatūra par *Chevron* doktrīnu, saskaņā ar kuru tiesas piemēro principu par atturēšanos no tiesību aktu saprātīgas interpretācijas, ko veic regulatīvā aģentūra, ja pastāv neskaidrības šīs aģentūras īstenotajā tiesību aktā. Īpaši dažas NVO ir paudušas bažas par šā Augstākās tiesas sprieduma ietekmi uz *FTC* likumdošanas pilnvarām privātuma jomā, vienlaikus atzīstot, ka var nebūt ietekmes uz tās izpildes pilnvarām vai tā var būt ierobežota. Pārskatīšanas sanāksmē *FTC* informēja, ka vēl ir par agru, lai zinātu precīzu šā sprieduma ietekmi. Tajā pašā laikā tā paskaidroja, ka *FTC* noteikumu izstrāde notiek saskaņā ar *FTC* likumā paredzēto pilnvarojumu, kas atšķiras no citu administratīvo aģentūru pilnvarām un kam *Chevron* doktrīna nav tik nozīmīga. Tāpēc nesenajam spriedumam šajā jomā var būt ierobežota ietekme.

Turklāt *FTC* informēja par jaunākajām izmaiņām savā pieejā automatizētai apstrādei un mākslīgajam intelektam. Tas ietver kopīga paziņojuma pieņemšanu kopā ar citām izpildiestādēm, kas vērsts pret diskrimināciju un neobjektivitāti automatizētajās sistēmās[33], kā arī vairākām izpildes panākšanas darbībām, kurās *FTC* cita starpā pievēršas pārredzamībai, automatizētas apstrādes taisnīgumam un fizisko personu spējai apstrīdēt rezultātus. Šajā ziņā visnozīmīgākais gadījums ir *FTC* 2024. gada marta lēmums par *Rite Aid*, ar kuru šim uzņēmumam tika noteikts piecu gadu aizliegums izmantot sejas atpazīšanas tehnoloģiju drošības nolūkos[34]. Konkrētāk, *FTC* konstatēja, ka *Rite Aid* neveica saprātīgus pasākumus, lai novērstu kļūdainus rezultātus un informētu patērētājus par izmantoto tehnoloģiju. Vispārīgāk runājot, pārskatīšanas sanāksmē *FTC* pievērsās savām pašreizējām prioritātēm un īpaši jomām, kuras, pēc tās domām, turpmāk ir pelnījušas proaktīvāku izpildes pieeju. Tas ietver sensitīvu

[32] Lai gan "profilēšana" dažādās pavalstīs atšķiras, profilēšana parasti tiek definēta kā jebkura veida automatizēta personas datu apstrāde, ko veic, lai izvērtētu, analizētu vai prognozētu personiskus aspektus, kas saistīti ar identificētas vai identificējamas fiziskas personas ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos. Parasti patērētāji var atteikties no profilēšanas. Tiesību aktus par profilēšanu ir izstrādājušas šādas pavalstis: Kolorādo (Colo. Rev. Stat. Ann. § 6-1-1306), Konektikuta (Conn. Gen. Stat. Ann. § 42-518), Delavēra (Del. Code Ann. tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiāna (Ind. Code Ann. § 24-15-3-1), Kentuki (Ky. Rev. Stat. Ann. § 367.3615), Merilenda (Merilendas 2024. gada Tiešsaistes datu privātuma likums, pieņemts 2024. gada 9. maijā), Minesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), Ņūhempšīra (N.H. Rev. Stat. Ann. § 507-H:4), Ņūdžersija (N.J. Stat. Ann. § 56:8–166.8), Oregona (Or. Rev. Stat. Ann. § 646A.574), Rodailenda (Rodailendas Datu pārredzamības un privātuma aizsardzības likums, pieņemts 2024. gada 29. jūnijā), Tenesī (Tenn. Code Ann. § 47-18-3304), Teksasa (Tex. Bus. & Com. Code Ann. § 541.051) un Virdžīnija (Va. Code Ann. § 59.1-577).

[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.

datu (piemēram, veselības datu, biometrisko datu, ģeolokācijas) aizsardzību[35], bērnu[36] un nepilngadīgo aizsardzību tiešsaistē un datu drošību[37].

Komisija turpinās stingri sekot šīm un citām norisēm ASV, īpaši jebkādiem turpmākiem pasākumiem virzībā uz visaptverošu federālo privātuma likumu un Augstākās tiesas nesenās judikatūras iespējamo ietekmi uz *FTC* lomu privātuma jomā.

Komisija atzinīgi vērtē *FTC* sniegto informāciju par tās nesenajām izpildes panākšanas darbībām un pašreizējām prioritātēm, kas lielā mērā atbilst datu aizsardzības izpildes tendencēm un prioritātēm Eiropā. *FTC* arī aktīvi piedalās tīklā, ko Komisija sāka veidot 2024. gada martā un kas apvieno valstis, kuras gūst labumu no ES lēmuma par aizsardzības līmeņa pietiekamību[38]. Šai palielinātai konverģencei būtu jāveicina un jāatvieglo ciešāka sadarbība starp privātuma aizsardzības iestādēm abās Atlantijas okeāna pusēs, īpaši jautājumos, kas attiecas uz DPR darbību.

2.2. Aspekti, kas saistīti ar ASV publisko iestāžu piekļuvi personas datiem, kuri nosūtīti saskaņā ar ES un ASV datu privātuma regulējumu, un to izmantošanu

Lēmumā par aizsardzības līmeņa pietiekamību ir sīki izklāstīts to noteikumu novērtējums, kas reglamentē to, kā ASV publiskās iestādes vāc un izmanto personas datus, kurus no ES nosūta DPR jomā sertificētiem uzņēmumiem, īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, ko pārskatīšanas sanāksmē apstiprināja ASV iestādes, DPR pirmajā gadā nav notikušas būtiskas izmaiņas attiecībā uz tiesisko regulējumu, ko piemēro piekļuvei datiem tiesībaizsardzības vai regulatīviem mērķiem. Šā iemesla dēļ turpmāk minētie konstatējumi attiecas tikai uz norisēm nacionālās drošības jomā.

Lēmumā par aizsardzības līmeņa pietiekamību izdarītie secinājumi par izlūkošanas aģentūru piekļuvi datiem balstās uz to nosacījumu un ierobežojumu analīzi, kas attiecas uz sakaru izlūkošanas darbībām saskaņā ar juridiskām pilnvarām, īpaši Ārējās izlūkošanas uzraudzības likuma (*FISA*) 702. pantu un Izpildrīkojumu Nr. 12333[39], ko papildina un pastiprina ASV

---

[35] Sk., piemēram, neseno *FTC* rīkojumu attiecībā uz uzņēmumu *X-Mode* par sensitīvas atrašanās vietas informācijas pārdošanas un kopīgošanas aizliegumu (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) un attiecībā uz uzņēmumu *Monument* par aizliegumu atklāt sensitīvus veselības datus trešām personām šādu datu izmantošanai tirgvedības nolūkos (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Piemēram, *FTC* nesen paziņoja par izmeklēšanu, kuras rezultātā tika ierosināta tiesvedība pret uzņēmumu *TikTok* un tā mātesuzņēmumu *Bytedance* par iespējamu bērnu privātuma tiesību pārkāpumu. Tiek apgalvots, ka abi uzņēmumi nav izpildījuši prasību paziņot vecākiem un saņemt to piekrišanu, pirms personas datu vākšanas no bērniem, kas nav sasnieguši 13 gadu vecumu, un šo datu izmantošanas (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Sk. pārskatu par nesenajām izpildes panākšanas darbībām *FTC* 2023. gada privātuma un datu drošības atjauninājumā: https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] Sk. https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. 2024. gada marta sanāksmes rezultātā tika nolemts rīkot vairākas tematiskas sesijas. Pirmā sesija notika 2024 gada jūlijā, un tajā galvenā uzmanība tika pievērsta tādu rīku izstrādei, kas var palīdzēt maziem un vidējiem uzņēmumiem ievērot privātuma tiesību aktus.

[39] Citi pasākumi, ko saskaņā ar *FISA* var veikt attiecībā uz datiem, kas nosūtīti no ES, ir individualizēta elektroniskā uzraudzība (*FISA* 105. pants), fiziska meklēšana (*FISA* 302. pants), zvanīto numuru reģistrētāju vai uztveršanas un izsekošanas ierīču izmantošana (*FISA* 402. pants) un komercdarbības dokumentu vākšana no konkrētiem uzņēmumiem (pārvadātājiem, publiskām izmitināšanas iestādēm, transportlīdzekļu nomas iestādēm

prezidenta 2022. gada 7. oktobrī pieņemtais Izpildrīkojums Nr. 14086 par aizsardzības pasākumu uzlabošanu Amerikas Savienoto Valstu sakaru izlūkošanas vajadzībām (IR Nr. 14086). Izpildrīkojumā Nr. 14086 noteiktie aizsardzības pasākumi attiecas uz visām ASV sakaru izlūkošanas darbībām neatkarīgi no juridiskajām pilnvarām, kas ir minēto darbību pamatā, un no vietas, kur tās notiek, un aizsargā to fizisko personu datus, kas nav ASV fiziskās personas (ieskaitot eiropiešus)[40]. Ar Izpildrīkojumu Nr. 14086 tika izveidots arī jauns tiesiskās aizsardzības mehānisms, ar kura palīdzību fiziskas personas ES var izmantot un īstenot šos saistošos aizsardzības pasākumus.

Nākamajās iedaļās ir aprakstīti pasākumi, ko ASV iestādes veikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, lai izpildītu IR Nr. 14086, kā arī attiecīgās norises saistībā ar iepriekš minēto tiesisko regulējumu.

2.2.1. Attiecīgās norises saistībā ar ASV tiesisko regulējumu

2.2.1.1. Izpildrīkojuma Nr. 14086 īstenošana, ko veic izlūkošanas aģentūras

Ar Izpildrīkojumu Nr. 14086 ieviestie ierobežojumi un aizsardzības pasākumi papildina tos pasākumus, kas paredzēti *FISA* 702. pantā un IR Nr. 12333. Tie ir saistoši visām izlūkošanas aģentūrām, un to darbību praksē tālāk nodrošina katras aģentūras pieņemtā politika un procedūras.

Pirmās pārskatīšanas ietvaros ASV iestādes apstiprināja, ka IR Nr. 14086 kopš tā pieņemšanas nav veiktas izmaiņas. Turklāt tika precizēts, ka ASV prezidents nav izmantojis IR Nr. 14086 iedaļā 2(b)(i)(B) un 2(b)(ii)(C) paredzētās pilnvaras atjaunināt to leģitīmo mērķu sarakstu, kuru sasniegšanai var veikt sakaru izlūkošanas darbības, vai to mērķu sarakstu, kuriem var izmantot lielos apjomos savāktos datus[41]. Lai noteiktu konkrētākas izlūkošanas prioritātes, attiecībā uz kurām var faktiski vākt sakaru izlūkošanas datus, ar IR Nr. 14086 tika ieviesta īpaša procedūra. Jo īpaši, ir jāapspriežas ar *ODNI* pilsonisko brīvību aizsardzības speciālistu (*ODNI CLPO*), lai attiecībā uz katru prioritāti novērtētu, vai 1) tā sekmē vienu vai vairākus leģitīmos mērķus, kas uzskaitīti IR; 2) tas netika izstrādāts vai paredzēts, lai tā rezultātā vāktu sakaru izlūkošanas datus kāda no IR uzskaitīto aizliegto mērķu sasniegšanai, un 3) tas tika izveidots, pienācīgi ņemot vērā visu personu privātumu un pilsoniskās brīvības[42]. Pārskatīšanas sanāksmē *ODNI CLPO* vadītāja apstiprināja, ka ir pārskatījusi nacionālās izlūkošanas direktora ierosinātās prioritātes 2023. gada Nacionālajā izlūkošanas prioritāšu satvarā un secinājusi, ka tās atbilst iepriekš minētajām prasībām, un ir darījusi zināmu savu secinājumu nacionālās izlūkošanas (DNI) direktoram, kurš savukārt iesniedza prioritātes apstiprināšanai prezidentam. *ODNI CLPO* arī nodrošināja apmācību par IR Nr. 14086 prasībām tām izlūkdienestu daļām, kas iesaistītas izlūkošanas prioritāšu izstrādē.

Turklāt ASV iestādes pagājušajā gadā ir veikušas turpmākus praktiskus pasākumus ar mērķi ieviest IR Nr. 14086 savās ikdienas darbībās. Konkrētāk, izlūkošanas aģentūras ir ieviesušas papildu iekšējo politiku un pamatnostādnes par IR piemērošanu, piemēram, iekšējos procesus

vai fiziskām noliktavām, *FISA* 501. pants). Šie dažādie juridiskie pamati ir sīki analizēti lēmumā par aizsardzības līmeņa pietiekamību (142.–152. apsvērums).

[40] Sīkāku informāciju sk. lēmuma par aizsardzības līmeņa pietiekamību 3.2.1.2. iedaļā.

[41] Šie likumīgie mērķi/nolūki ietver, piemēram, aizsardzību pret spiegošanu, sabotāžu, slepkavībām vai citām izlūkošanas darbībām, ko veic ārvalstu valdība, organizācija vai persona vai kas tiek veiktas to vārdā vai ar to palīdzību; aizsardzību pret terorismu, ķīlnieku sagrābšanu un personu turēšanu nebrīvē, ko veic ārvalstu valdība, organizācija vai persona vai kas tiek veikta to vārdā.

[42] IR Nr. 14086 iedaļa 2(b)(iii).

(izmantojot iekšējās atļaujas prasības, dokumentētu piekļuves kontroli, lai panāktu, ka piekļuve informācijai ir tikai tām personām, kuras ir pienācīgi apmācītas un kurām ir uzdevumam nepieciešamās pilnvaras utt.), lai nodrošinātu, ka IR paredzētās nepieciešamības un samērīguma prasības tiek ievērotas gan mērķorientētas, gan lielapjoma datu vākšanas kontekstā[43]. Turklāt dažādu izlūkošanas aģentūru (piemēram, *NSA*, CIP, FIB) darbiniekiem ir nodrošināta apmācība par IR Nr. 14086, ieskaitot *ODNI CLPO* organizētas ikgadējas un *ad hoc* apmācības un obligātas mācības visiem jaunajiem darbiniekiem, kas pievienojas *ODNI*.

Komisija atzinīgi vērtē dažādos pasākumus, kas ieviesti, lai īstenotu IR Nr. 14086 un nodrošinātu tā ievērošanu. Tā kā tagad jau ir gūta lielāka pieredze IR aizsardzības pasākumu praktiskajā piemērošanā, Komisija atzinīgi vērtētu iespēju turpmākajās pārskatīšanās apspriest konkrētus piemērus par to, kā IR tiek piemērots praksē (vienlaikus ievērojot piemērojamos konfidencialitātes apsvērumus).

2.2.1.2. FISA *702. panta piemērošanas atļaujas atjaunošana*

Ar *FISA* 702. pantu ir atļauts ārvalstu izlūkošanas informācijas iegūšanas nolūkā izsekot personas, attiecībā uz kurām ir pamats uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām Valstīm. Informācijas iegūšana notiek, pamatojoties uz Ārējās izlūkošanas uzraudzības tiesai (*FISC*) iesniegtiem un apstiprinātiem ikgadējiem apliecinājumiem. Šajos apliecinājumos ir noteiktas konkrētas vācamās ārējās izlūkošanas informācijas kategorijas. 2023. gada 21. jūlijā *ODNI* paziņoja, ka saskaņā ar *FISA* 702. pantu ir trīs apstiprināti apliecinājumi, kas aptver šādas ārējās izlūkošanas kategorijas: 1) ārvalstu valdības un ar tām saistītas struktūras, 2) terorisma apkarošana un 3) ieroču izplatīšanas apkarošana[44]. Apliecinājumos ir jāiekļauj arī mērķorientēšanas un minimizēšanas procedūras, ko apstiprinājusi *FISC*[45]. Konkrētāk, mērķorientēšanu veic, pieprasot ASV uzņēmumiem, kas atbilst *FISA* "elektronisko sakaru pakalpojumu sniedzēja" definīcijai, izpaust elektronisko sakaru datus par saziņas saturu, kas nosūtīts uz "selektoriem" vai no tiem un kas identificē konkrētu saziņas kontu, piemēram, tālruņa numuru vai e-pasta adresi. ASV valdība ir publicējusi vairākus materiālus par *FISA* 702. pantu, lai informētu sabiedrību par pārraudzības programmu darbību, piemērojamajām prasībām un privātuma aizsardzību, kā arī *FISC* lomu[46].

Turpināmības klauzulas rezultātā bija paredzēts, ka *FISA* 702. pants 2023. gada beigās zaudēs spēku, ja vien Kongress nepiešķirts atkārtotu atļauju tā piemērošanai. Pēc tā piemērošanas pagaidu atļaujas piešķiršanas bez jebkādām izmaiņām Kongress 2024. gada 19. aprīlī pieņēma Likumu par Amerikas izlūkošanas un drošības reformu (*RISAA)*, ar ko atkārtoti apstiprināja *FISA* 702. pantu uz diviem gadiem un ieviesa tajā vairākas izmaiņas. Būtībā tās var iedalīt divās kategorijās: 1) izmaiņas saskaņā ar *FISA* 702. pantu atļauto novērošanas darbību tvērumā un 2) institucionālas un procesuālas izmaiņas.

Izmaiņas atļauto uzraudzības darbību tvērumā saskaņā ar FISA *702. pantu*

[43] Sk. https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, publicēts 2023. gada 3. jūlijā.

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Šādas procedūras ierobežo datu vākšanu par konkrētu ārvalstu izlūkošanas mērķi, ierobežo piekļuvi datubāzēm, kurās tiek glabāta informācija, kas iegūta saskaņā ar *FISA* 702. pantu (arī, izmantojot piekļuves kontroli), un nosaka ierobežojumus šādas informācijas izmantošanai, glabāšanai un izplatīšanai.

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

Ar *RISAA* ir ieviestas trīs galvenās izmaiņas to novērošanas darbību tvērumā, kuras var veikt saskaņā ar *FISA* 702. pantu.

Pirmkārt ir noteikti aizliegta "par izlūkošanas subjektu netieši iegūtas " informācijas vākšana[47]. Tas attiecas uz saziņas informācijas vākšanu, ja 702. pantā minētais selektors (piemēram, e-pasta adrese) nav ietverts saziņā tieši "uz" vai "no" izlūkošanas subjekta, bet saziņas saturā ir iekļauta atsauce uz šādu selektoru (piemēram, e-pasta saziņas saturs, kas nav tieši nosūtīts uz atlasīto e-pasta adresi vai no tās, bet ietver atlasīto e-pasta adresi e-pasta vēstules tekstā vai struktūrā). Lai gan šāda informācijas vākšana jau bija izslēgta pēc *FISA* grozījumiem 2018. gadā, *FISA* joprojām bija paredzēta iespēja atsākt "par izlūkošanas subjektu netieši iegūtas" informācijas vākšanu nākotnē pēc īpašas atļaujas piešķiršanas procedūras, kurā iesaistīta *FISC* un Kongress. Pēdējā *RISAA* ieviestā grozījuma rezultātā šī iespēja ir svītrota.

Otrkārt, ārējās izlūkošanas informācijas definīcija ir paplašināta, lai iekļautu informāciju saistībā ar narkotiku apkarošanu[48]. Pārskatīšanas sanāksmē ASV iestādes paskaidroja, ka papildinājums tika ieviests, ņemot vērā pašreizējo fentanila krīzi un pieaugošos draudus nacionālajai drošībai, ko rada starptautiskie narkotiku tirgotāji un ražotāji. Ņemot vērā iepriekš minēto, tika apstiprināts, ka uz šo jēdzienu attiecas vairāki IR Nr. 14086 uzskaitītie leģitīmie mērķi, t. i., izprast vai novērtēt ārvalstu organizāciju spējas, nodomus vai darbības, kas rada pašreizējus vai potenciālus draudus ASV vai tās sabiedroto nacionālajai drošībai; izprast vai novērtēt starptautiskus apdraudējumus, kas ietekmē globālo drošību, ieskaitot riskus sabiedrības veselībai; un aizsargāt pret transnacionāliem noziedzības draudiem[49].

Treškārt, *RISAA* tika paplašināta "elektronisko sakaru pakalpojumu sniedzēja" (*ECSP*) definīcija un tādējādi paplašināts to uzņēmumu loks, kuriem var būt pienākums sniegt informāciju saskaņā ar *FISA* 702. pantu[50]. Definīcija tagad ietver citus pakalpojumu sniedzējus, kuriem ir "piekļuve aprīkojumam, ko izmanto vai var izmantot, lai nosūtītu vai glabātu pa vadiem pārraidītas vai elektroniskas saziņas saturu", vienlaikus skaidri izslēdzot sabiedriskās izmitināšanas iestādes, mājokļus, kopienas objektus un ēdināšanas iestādes. Vēstulē Kongresam *DoJ* atsaucās uz šo grozījumu kā uz tehniskām izmaiņām, kas paredzētas, lai aptvertu "ārkārtīgi nelielu" tehnoloģiju uzņēmumu skaitu, kuri saskaņā ar nesenajiem *FISC* un Ārējās izlūkošanas uzraudzības pārskatīšanas tiesas (*FISCR*) nolēmumiem netika iekļauti iepriekšējā *ECSP* definīcijā[51]. Tajā pašā vēstulē *DoJ* apņēmās sašaurināt piemērošanas jomu, izmantojot šo definīciju vienīgi tam, lai aptvertu attiecīgo pakalpojumu sniedzēja veidu tiesvedībā, kuras rezultātā tika pieņemts *FISC* nolēmums. Tā rezultātā attiecīgie uzņēmumi ir minēti klasificētā Kongresa pielikumā. Vairākas NVO, ieskaitot tās, kas pārskatīšanas ietvaros sniedza atsauksmes, pauda bažas par šo paplašināšanu, apgalvojot, ka tā varētu aptvert daudzus ASV uzņēmumus (jo daudzi no tiem sniedz noteikta veida pakalpojumus un tiem ir piekļuve sakaru iekārtām). Ņemot vērā minētās bažas, ar izlūkdienestu atbalstu ir ierosināts vēl viens grozījums Izlūkošanas atļauju likumprojektā 2025. finanšu gadam, kas pašlaik tiek apspriests Kongresā. Ja Kongress pieņems šo grozījumu, tas nodrošinātu, ka papildu uzņēmumi, uz kuriem attiecas *ECSP* definīcija, būtu tikai tie, kas minēti iepriekš minētajos *FISC* nolēmumos.

---

[47] *RISAA* 22. pants.
[48] *RISAA* 23. pants.
[49] IR Nr. 14086 iedaļa 2(b)(ii)(A)(2), (3) un (10).
[50] *RISAA* 25. pants.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. Sk. *FISC* 2022. gada nolēmumu (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) un Ārējās izlūkošanas uzraudzības pārskatīšanas tiesas nolēmumu, ar kuru šis nolēmums ir apstiprināts (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

Likumprojektā arī paredzēts, ka par katru direktīvu, kas adresēta šādam uzņēmumam, būtu jāziņo *FISC*, lai tā varētu pārbaudīt, vai uzņēmums patiešām ietilpst direktīvas darbības jomā. Savā vēstulē Kongresam *DoJ* apņēmās reizi sešos mēnešos ziņot Kongresam par atjauninātās definīcijas piemērošanu, lai Kongress varētu veikt pienācīgu uzraudzību attiecībā uz definīcijas šauru piemērošanu.

Svarīgi ir tas, ka pārskatīšanas sanāksmē ASV iestādes un Privātuma un pilsonisko brīvību pārraudzības padome (*PCLOB*) apstiprināja, ka visi IR Nr. 14086 paredzētie aizsardzības pasākumi saskaņā ar *FISA* 702. pantu, arī pēc šiem grozījumiem, joprojām pilnībā attiecas uz visu datu vākšanu un izmantošanu. Tādējādi, lai gan ar *RISAA* nedaudz tika paplašināts to uzņēmumu loks, kuri var saņemt rīkojumu, tas neierobežo tiesību izmantošanu. Tomēr būs svarīgi uzraudzīt turpmākās (likumdošanas un ziņošanas) izmaiņas un saņemt informāciju par šo jauno noteikumu piemērošanu praksē. Tas ietver, piemēram, ārējās izlūkošanas un *ECSP* definīciju paplašināšanas ietekmi uz *FISA* 702. pantā noteikto izlūkošanas subjektu skaitu (kā to katru gadu paziņo *ODNI*, sk. turpmāk attiecībā uz pārredzamību). Nākamajam ziņojumam par turpmākajiem pasākumiem saistībā ar neseno *PCLOB* ziņojumu par *FISA* 702. pantu (sk. turpmāk) šajā ziņā vajadzētu būt īpaši informatīvam.

Institucionālas un procesuālas izmaiņas

Attiecībā uz institucionālajām un procesuālajām izmaiņām *RISAA* kodificēja vairākas procedūras, kas jau tika ievērotas praksē, un ieviesa jaunus aizsardzības pasākumus. Lai gan dažas no tām attiecas tikai uz ASV fiziskām personām, vairākas izmaiņas palielina aizsardzību gan ASV fiziskām personām, gan tām, kas nav ASV fiziskās personas un kuru datus var vākt saskaņā ar *FISA* 702. pantu[52], un tāpēc tās ir būtiskas DPR darbībai.

Pirmkārt, tika ieviestas vairākas papildu pārskatatbildības, pārraudzības un ziņošanas prasības. Jo īpaši FIB darbinieki tagad katru gadu jāapmāca par noteikumiem, kas attiecas uz vaicājumu veikšanu informācijas iegūšanai saskaņā ar *FISA* 702. pantu[53]. FIB ir arī jāziņo Kongresam par savām vaicājumu veikšanas darbībām (piemēram, vaicājumu skaitu, izmantojot "pakešuzdevuma tehnoloģijas", t. i., izmantojot vairākus atslēgvārdus kā daļu no viena vaicājuma) un par pārskatatbildības pasākumiem, kas ieviesti, lai nodrošinātu atbilstību juridisko vaicājumu veikšanas prasībām (*RISAA* 11.–12. pants). Turklāt DAI ģenerālinspektoram ir uzdots sagatavot ziņojumu par FIB atbilstību vaicājumu veikšanas prasībām (*RISAA* 9. pants). Vispārīgāk runājot, lai palielinātu procedūru pārredzamību *FISC*, *ODNI* un ģenerālprokuroram tagad 180 dienu laikā ir jāpabeidz *FISC* nolēmumu deklasificēšanas pārskatīšana (*RISAA* 7. pants). Turklāt visu *FISC* un Ārējās izlūkošanas pārskatīšanas tiesā (*FISCR*, kur var pārsūdzēt *FISC* nolēmumus) notikušo uzklausīšanu protokoli ir jāglabā un jānosūta Kongresam (*RISAA* 8. pants).

Otrkārt, ar *RISAA* tika ieviesti papildu ierobežojumi attiecībā uz to, kā FIB izmanto datus, kas savākti saskaņā ar *FISA* 702. pantu. *RISAA* 2. panta d) punktā ir noteikts, ka vaicājumu,

[52] Turklāt ar *RISAA* tika ieviestas dažas izmaiņas attiecībā uz tradicionālo individualizēto elektronisko uzraudzību saskaņā ar *FISA* 105. pantu (pamatojoties uz *FISC* orderi, kas izdots, ja ir atbilstība pietiekama pamata standartam). Lai izlūkošanas aģentūra iesniegtu ģenerālprokuroram pieprasījumu izdot rīkojumu veikt individualizētu elektronisku novērošanu, tagad ir vajadzīgs ar zvērestu apliecināts paziņojums, kas pamato pārliecību, ka ir izpildīti *FISA* 105. panta nosacījumi (*RISAA* 6. panta a) punkts). Elektroniskās uzraudzības iespējamais ilgums attiecībā uz ārvalstu pilnvarām vai ārvalstu varas aģentiem ir pagarināts no 120 dienām līdz vienam gadam (*RISAA* 6. panta g) punkts).

[53] *RISAA* 2. panta d) punkts.

izmantojot "pakešuzdevuma tehnoloģijas", var veikt tikai pēc tam, kad ir saņemts FIB advokāta apstiprinājums, ja vien nepastāv ārkārtēji apstākļi. Turklāt FIB tagad ir aizliegts automātiski pārbaudīt neminimizētu informāciju, kas iegūta saskaņā ar *FISA* 702. pantu, un tā vietā tam ir jānodrošina, ka analītiķiem jāapstiprina izvēle meklēt šādu informāciju. *RISAA* arī ir noteikts aizliegums FIB veikt vaicājumus, kas ir paredzēti vienīgi tam, lai atrastu un iegūtu pierādījumus par noziedzīgu darbību (ja vien nav pamatotas pārliecības, ka tie varētu palīdzēt mazināt vai novērst draudus dzīvībai vai nopietnus miesas bojājumus, vai vajadzības gadījumā izpildīt informācijas atklāšanas pienākumus tiesvedībā)[54]. Turklāt FIB ir aizliegts analītiskajos repozitorijos ievadīt neminimizētus datus, ja vien attiecīgā fiziskā persona nav saistīta ar notiekošu izmeklēšanu saistībā ar nacionālo drošību[55].

Treškārt, ir mainīti daži noteikumi par *amici curiae* statusu un lomu *FISC*[56]. *Amici* tiek iecelti par ekspertiem, kas palīdz Tiesai (un *FISCR*) jautājumos, kas saistīti ar privātumu un pilsoniskajām brīvībām, vai palīdz precizēt tehnoloģiskus jautājumus, kad tiek izskatīts konkrēts valdības pieteikums. Lai gan *FISA* iepriekš pieprasīja, ka *amici* jābūt zināšanām par privātumu / pilsoniskajām brīvībām, izlūkdatu vākšanu, sakaru tehnoloģijām vai citās saistītās jomās, tagad tiem būtībā ir vajadzīgas speciālās zināšanas par privātumu / pilsoniskajām brīvībām un izlūkdatu vākšanu. Tiesai jau bija iespēja iecelt *amicus* jebkurā gadījumā, ko tā uzskatīja par atbilstošu, un tai tas bija jādara, izskatot jaunu vai būtisku tiesību aktu interpretāciju. Pēc atļaujas atjaunošanas *FISC* tagad ir arī jāieceļ *amicus* katru reizi, kad tai tiek lūgts apstiprināt *FISA* 702. pantā paredzētos apliecinājumus un saistītās procedūras (piemēram, mērķorientēšanas procedūras), ja vien tā neuzskata, ka tas nebūtu atbilstīgi vai varētu izraisīt nepamatotu kavēšanos[57]. Turklāt tā vietā, lai ieceltu tikai vienu, Tiesa tagad var nolemt iecelt vienu vai vairākus *amici*. Ir arī precizēts, ka informācijai, ko sniedz *amici*, ir "jāattiecas tikai uz konkrētiem tiesas konstatētajiem jautājumiem", lai gan jomas, par kurām *amici* varētu izteikt komentārus, joprojām ir plašas (t. i., juridiskie argumenti un informācija, kas saistīta ar Amerikas Savienoto Valstu fizisko personu privātās dzīves un pilsonisko brīvību aizsardzību, izlūkdatu vākšanu un sakaru tehnoloģijām vai jebkuru citu attiecīgu jomu).

Visbeidzot, ar *RISAA* 18. pantu ir izveidota "*FISA* reformu komisija", kas citu starpā sastāv no Kongresa locekļiem, *PCLOB* priekšsēdētāja, Nacionālās izlūkošanas galvenā direktora vietnieka un ģenerālprokurora vietnieka, kā arī papildu locekļiem, kurus iecels Kongress[58], lai tie ieteiktu papildu reformas attiecībā uz *FISA*.

Komisija stingri uzraudzīs turpmākās norises saistībā ar *FISA* 702. pantu, arī saistībā ar *PCLOB* pārraudzības darbībām (sk. turpmāk), Reformu komisijas darbu un gaidāmo *FISA* pārskatīšanu pēc diviem gadiem.

2.2.1.3. Uzraudzības darbības praksē: skaitļi un tendences

ODNI ikgadējais statistikas pārredzamības ziņojums par to, kā izlūkdienesti izmantojuši valsts drošības uzraudzības pilnvaras 2023. kalendārajā gadā (publicēts 2024. gada aprīlī),[59] liecina, ka *FISA* 702. pantā noteikto izlūkošanas subjektu skaits palielinājās no 245 073 izlūkošanas

[54] *RISAA* 3. panta a) punkts.
[55] *RISAA* 3. panta b) punkts. Ja tas nepieciešams ārkārtēju apstākļu dēļ, FIB direktors var lemt par izņēmumu no šā noteikuma un par to ir jāpaziņo Kongresam.
[56] Skaidrības labad jāatzīmē, ka šie grozījumi neietekmē īpašo advokātu statusu un lomu *DPRC*, kā to pārskatīšanas sanāksmē apstiprināja ASV.
[57] *RISAA* 5. panta b) punkts.
[58] 18. pantā ir īpaši noteikts, ka pārstāvībai ir jābūt ārpus Kongresa.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

subjektiem 2022. kalendārajā gadā līdz 268 590 subjektiem 2023. kalendārajā gadā. Ziņojumā paskaidrots, ka izlūkošanas subjektu skaita svārstības var būt saistītas ar dažādiem iemesliem, tajā skaitā izmaiņām darbības prioritātēs, notikumiem pasaulē, tehniskajām spējām, izlūkošanas subjekta uzvedību un izmaiņām telekomunikāciju nozarē. Ziņojumā arī norādīts, ka ne pret vienu personu, kas nav ASV persona (salīdzinājumā ar vienu personu 2021. gadā un 0 personām 2022. gadā), nenotika mērķtiecīga vēršanās saskaņā ar *FISA* 402. pantu (tiesības izmantot zvanīto numuru reģistrētāju un uztveršanas un trasēšanas ierīces), savukārt seši rīkojumi (salīdzinājumā ar 11 rīkojumiem gan 2021. gadā, gan 2022. gadā) tika izdoti attiecībā uz sešiem izlūkošanas subjektiem (salīdzinājumā ar 13 rīkojumiem 2021. gadā un 11 rīkojumiem 2022. gadā) saskaņā ar *FISA* 501. pantu (piekļuve pārvadātāju, transportlīdzekļu nomas iestāžu vai fizisku noliktavu komercdarbības dokumentiem), kas aptver 5412 unikālos identifikatorus (salīdzinājumā ar 23 157 identifikatoriem 2021. gadā un 55 431 identifikatoriem 2022. gadā), kurus izmanto, lai paziņotu informāciju, kas tiek vākta saskaņā ar šiem rīkojumiem.

DoJ ikgadējā ziņojumā Kongresam par Ārējās izlūkošanas uzraudzības likuma īstenošanu ir norādīts, ka 2023. kalendārajā gadā *FISC* tika iesniegti 327 pieteikumi, lai veiktu elektronisku novērošanu un/vai fizisku meklēšanu ārējās izlūkošanas nolūkos saskaņā ar attiecīgi *FISA* 105. un 302. pantu[60]. Kopējais mērķtiecīgi novēroto fizisko personu skaits bija 500 līdz 999. Attiecībā uz nacionālās drošības vēstulēm (*NSL*) ziņojumā precizēts, ka bija izdoti 10 115 pieprasījumi (izņemot tikai abonenta informācijas pieprasījumus) informācijas iegūšanai par personām, kas nav ASV personas, kas tika veikts, meklējot informāciju par 3033 dažādām personām, kas nav ASV personas[61].

Vairāki DPR sertificēti uzņēmumi (piemēram, *Google*, *Meta*) izmanto ASV tiesību aktos paredzēto iespēju publicēt pārredzamības ziņojumus, kur ir sniegta informācija par *FISA* un *NSL* pieprasījumu skaitu, ko tie ir saņēmuši konkrētajā pārskata periodā. Šā ziņojuma sagatavošanas laikā statistika par *FISA* pieprasījumiem pēc 2023. gada jūlija vēl nebija pieejama. Piemēram, uzņēmums *Google* ziņoja, ka no 2023. gada jūlija līdz decembrim ir saņēmis 500–999 *NSL* pieprasījumus, kas ietekmē 2000 līdz 2499 kontus[62]. Uzņēmums *Meta* ziņoja, ka tajā pašā pārskata periodā ir saņēmis no 0 līdz 499 *NSL* pieprasījumus, kas ietekmē 500–999 kontus[63]. Pēdējos gados šis skaits ir saglabājies diezgan stabils. Lai vēl vairāk palielinātu pārredzamību, daži uzņēmumi (piemēram, *Google*) proaktīvi publicē *NSL*, ko tie saņēmuši pēc tam, kad ir atcelti informācijas neizpaušanas ierobežojumi[64].

2.2.1.4. Citas norises

Saistībā ar pārskatīšanas sagatavošanu vairākas NVO ir izvirzījušas jautājumus par jauniem datu iegūšanas veidiem, ko ASV izlūkošanas aģentūras veic, iegādājoties datus no komercsavienībām, īpaši no datu mākleriem. Tās paskaidroja, ka, lai gan uz šā pamata savāktie

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

[61] Salīdzinājumā ar iepriekšējo pārskata gadu (2022. gads) šie skaitļi lielā mērā ir saglabājušies stabili. Salīdzinājumam – 2022. gadā *FISC* tika iesniegti 317 galīgie pieteikumi elektroniskas novērošanas un/vai fiziskas meklēšanas veikšanai ārējās izlūkošanas nolūkos. Kopējais to personu skaits, uz kurām attiecas elektroniskās novērošanas rīkojumi, bija no 0 līdz 499. FIB 2022. gadā iesniedza 9103 *NSL* informācijas pieprasījumus par personām, kas nav ASV personas (izņemot tikai abonenta informācijas pieprasījumus). Avots: 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.

dati joprojām ir jāapstrādā saskaņā ar citām prasībām, ieskaitot, piemēram, saskaņā ar IR Nr. 12333[65], šāda iegūšana notiek ārpus *FISA* un IR Nr. 14086 regulējuma.

Šajā sakarā jāatgādina, ka uz jebkāda veida brīvprātīgu datu apmaiņu ar trešām personām attiecas vairāki sīki izstrādāti nosacījumi saskaņā ar DPR. Pirmkārt, sertificēta organizācija nevar kopīgot datus ar trešo personu (kas nedarbojas kā pārstāvis/apstrādātājs), nesniedzot paziņojumu un nepiedāvājot izvēli attiecīgajām personām[66]. Otrkārt, saskaņā ar *atbildības par tālāku nosūtīšanu principu* tālāku nosūtīšanu var veikt tikai 1) ierobežotos un konkrētos nolūkos, 2) pamatojoties uz līgumu starp ES un ASV DPR organizāciju un trešo personu un 3) tikai tad, ja minētajā līgumā noteikts, ka trešai personai ir jānodrošina tāds pats aizsardzības līmenis kā DPR principos garantētais[67].

Turklāt, kā tika apspriests arī pārskatīšanas sanāksmē, *FTC* ir veikusi izpildes panākšanas darbības pret datu brokeriem, kas pārdod sensitīvus patērētāju datus. Piemēram, lietā pret uzņēmumu *X-Mode* un tā tiesībpārņēmēju uzņēmumu *Outlogic FTC* 2024. gada 9. janvārī pieņēma rīkojumu, kurā noteikts aizliegums uzņēmumam pārdot ģeolokācijas datus trešām personām, un dzēsa datus, ko tas bija nelikumīgi izmantojis un kopīgojis. *FTC* izmeklēšanā cita starpā tika konstatēts, ka uzņēmums nav pilnībā informējis personas par viņu ģeolokācijas datu izmantošanu un pārdošanu, nav ieviesis pasākumus, kas ļautu personām atteikties no izsekošanas, ir ļāvis datus izmantot potenciāli diskriminējošiem mērķiem un nav ierobežojis šādas informācijas izmantošanu trešām personām[68]. Komisija sagaida, ka *FTC* pieņems tādu pašu pieeju, ja DPR jomā sertificēti uzņēmumi kopīgotu datus, pārkāpjot iepriekš minētos noteikumus.

Visbeidzot, ir vērts pieminēt, ka 2024. gada maijā *ODNI* izdeva Izlūkdienestu politikas satvaru attiecībā uz komerciāli pieejamu informāciju[69]. Šajā satvarā ir noteikti vairāki principi un prasības, kas izlūkošanas aģentūrām būtu jāievēro, arī, lai samazinātu privātuma un pilsonisko brīvību riskus, kad tās iegūst un izmanto informāciju komercdarījuma kontekstā.

2.2.2. Neatkarīga pārraudzība

ASV izlūkošanas aģentūru darbības uzrauga dažādas struktūras, tajā skaitā privātuma un pilsonisko brīvību amatpersonas, ģenerālinspektori, Kongress un *PCLOB*. Pirmkārt, IR Nr. 14086 noteikts, ka katrā izlūkošanas aģentūrā jābūt augsta līmeņa amatpersonām juridiskajā, pārraudzības un atbilstības jomā, lai nodrošinātu atbilstību piemērojamajiem ASV tiesību aktiem. Šo pārraudzības funkciju veic amatpersonas, kas ir atbildīgas par atbilstības nodrošināšanu, kā arī privātuma un pilsonisko brīvību amatpersonas un ģenerālinspektori[70].

---

[65] Sk., piemēram, IR Nr. 12333 2.4. iedaļu par savākšanas paņēmieniem.
[66] Sk. lēmuma par aizsardzības līmeņa pietiekamību 40. apsvērumu.
[67] Sk. lēmuma par aizsardzības līmeņa pietiekamību 38. apsvērumu.
[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. Izlūkošanas aģentūrām politikas satvars ir jāievēro kopš 2024. gada augusta.
[70] Katrai izlūkošanas aģentūrai ir ģenerālinspektors, kurš ir likumiski neatkarīgs un atbildīgs par revīziju un izmeklēšanu veikšanu saistībā ar darbībām, ko attiecīgā aģentūra veic nacionālās drošības nolūkos. Viņiem ir piekļuve visiem attiecīgajiem (tostarp klasificētajiem) materiāliem, vajadzības gadījumā izmantojot pavēsti, un viņi var sniegt liecību. Lietas, kurās paustas aizdomas par noziedzīgiem nodarījumiem, ģenerālinspektori nodod

Tām ir regulāri jāpārrauga sakaru izlūkošanas darbības un jānodrošina, ka tiek novērstas jebkādas neatbilstības. Izlūkošanas aģentūrām jānodrošina šādām amatpersonām piekļuve visai attiecīgajai informācijai, kas vajadzīga, lai tās varētu veikt pārraudzības funkcijas, un aģentūras nedrīkst veikt nekādas darbības, lai kavētu vai neatbilstoši ietekmētu to pārraudzības darbības.

Pārskatīšanas sanāksmē piedalījās Izlūkdienestu ģenerālinspektora biroja (*ICIG*) ģenerālpadomnieks no *ODNI*, kuram ir visaptveroša jurisdikcija attiecībā uz visu Izlūkdienestu un kurš ir pilnvarots izmeklēt sūdzības vai informāciju par apgalvojumiem par nelikumīgu rīcību vai pilnvaru ļaunprātīgu izmantošanu. Viņš apstiprināja, ka *ICIG* sistemātiski pārbauda atbilstību IR Nr. 14086 viņa veiktās pārraudzības darbības ietvaros. Viņš pieminēja arī citu izlūkdienestu ģenerālinspektoru nesen veiktās pārraudzības darbības, kas aprakstītas regulārajos ziņojumos. Piemēram, savā pusgada ziņojumā Kongresam par laikposmu no 2023. gada aprīļa līdz septembrim[71] Nacionālās drošības aģentūras (*NSA*) ģenerālinspektors informēja par *NSA* iekšējās kontroles sistēmas izvērtējumu attiecībā uz mērķorientēšanas lēmumiem un pieprasījumiem. Tajā tika secināts, ka šī sistēma darbojas pienācīgi, lai nodrošinātu atbilstību tiesību aktiem, direktīvām un politikai, kas aizsargā pilsoniskās brīvības un privātumu. Tajā pašā ziņojumā ir minēta arī izmeklēšana, kurā atklājās, ka kāds *NSA* darbinieks ļaunprātīgi izmantoja sakaru izlūkošanas rīku neatļautiem mērķiem.

Saskaņā ar IR 14086 *PCLOB*[72] ir uzticētas īpašas pārraudzības funkcijas[73]. *PCLOB* priekšsēdētājs un trīs tās locekļi piedalījās pārskatīšanas sanāksmē un informēja, ka *PCLOB* 2023. gada aprīlī sniedza padomus izlūkošanas aģentūrām par to politikas un procedūru projektiem, ar ko īsteno IR Nr. 14086, un ka ar to notika apspriešanās par Datu aizsardzības pārskatīšanas tiesas (*DPRC*) tiesnešu un īpašo advokātu iecelšanu. Padome arī uzsāka pārraudzības projektu, lai 1) pārskatītu izlūkošanas aģentūru pieņemtās atjauninātās politikas un procedūru īstenošanu nolūkā nodrošināt, ka tās atbilst IR, un 2) katru gadu pārskatītu jaunā tiesiskās aizsardzības mehānisma darbību (sk. turpmāk)[74]. *PCLOB* locekļi apstiprināja, ka valde plāno tuvākajā nākotnē veikt abas pārskatīšanas. Attiecībā uz tiesisko aizsardzību tie paskaidroja, ka, ja netiks iesniegtas sūdzības, *PCLOB* veiktajā pārskatīšanā galvenā uzmanība tiks pievērsta politikai un procedūrām, kas ieviestas, lai izveidotu mehānismu.

Attiecībā uz citām pārraudzības darbībām *PCLOB* 2023. gada 28. septembrī izdeva ziņojumu par *FISA* 702. pantu[75]. Šis ziņojums ir turpinājums iepriekšējam 2014. gada ziņojumam un

---

krimināvajāšanas sākšanai un sniedz ieteikumus aģentūru vadītājiem par korektīvām darbībām. Lai gan ģenerālinspektoru ieteikumi nav saistoši, to ziņojumi, arī par turpmākiem pasākumiem (vai to trūkumu), parasti tiek publiskoti un nosūtīti Kongresam. Šajā sakarā sk. lēmuma par aizsardzības līmeņa pietiekamību 136. zemsvītras piezīmi par ģenerālinspektora lomu.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] *PCLOB* ir neatkarīga izpildiestāde, kurai uzticēti pienākumi pretterorisma politikas un tās īstenošanas jomā ar mērķi aizsargāt privātumu un pilsoniskās brīvības. Tā var piekļūt visai būtiskajai (tostarp klasificētajai) informācijai, veikt intervijas un uzklausīt liecības. Tā var sniegt ieteikumus tiesībaizsardzības un izlūkošanas iestādēm un regulāri ziņot Kongresam un prezidentam. Tās ziņojumi, cik vien iespējams, ir publiski pieejami.

[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.

satur atjauninātu faktisko un juridisko informāciju par *FISA* 702. panta uzraudzības programmu darbību. Ziņojumā ir iekļauti arī ieteikumi par to, kā izlūkošanas aģentūrām ievērot piemērojamās prasības, kā arī ieteikumi Kongresam vēl vairāk stiprināt vairākus *FISA* 702. panta aspektus saistībā ar tā piemērošanas atļaujas atjaunošanu (arī kodificējot novērošanas darbību leģitīmos mērķus, kas uzskaitīti IR Nr. 14086).[76] Pārskatīšanas sanāksmē *PCLOB* informēja, ka tā plāno drīzumā saņemt atbildes no izlūkošanas aģentūrām par tās ieteikumu īstenošanu, kas tiks izmantoti nākamajā ziņojumā par turpmākajiem pasākumiem. Starp citiem notiekošiem pārraudzības projektiem ir viens projekts par cīņu pret iekšējo terorismu un tā ietekmi uz privātumu un pilsoniskajām brīvībām, kā arī par atvērtā pirmkoda vai komerciāli pieejamu datu vākšanu, ko veic FIB[77].

Visbeidzot, NVO, ar kurām notika apspriešanās saistībā ar pārskatīšanu, pauda bažas par to, ka tuvākajā nākotnē beigsies vairāku *PCLOB* locekļu pilnvaru termiņš, tāpēc iespējams, ka *PCLOB* zaudēs kvorumu. Konkrētāk, ir beidzies priekšsēdētājas pilnvaru termiņš, un periods, kurā viņa var turpināt pildīt savus pienākumus, beidzas 2025. gada janvārī, savukārt vēl viens amats ir vakants, un trešais amats arī kļūs vakants nākamā gada janvārī. Pārskatīšanas sanāksmē *PCLOB* locekļi paskaidroja, ka neprognozē, ka padome zaudēs kvorumu, jo jau ir izvirzīta kandidatūra amatam, kas pašlaik ir vakants (un gaida Senāta apstiprinājumu)[78]. Viņi arī uzsvēra, ka pat tad, ja padome zaudētu kvorumu, tas neietekmētu tās spēju turpināt īstenot pārraudzības projektus. Tomēr, ņemot vērā *PCLOB* svarīgo lomu IR Nr. 14086 īstenošanas pārskatīšanā, Komisija cieši uzraudzīs turpmāko vakanču un kandidātu izvirzīšanas/iecelšanas statusu.

2.2.3. Tiesiskā aizsardzība

Ar IR Nr. 14086, ko papildināja ģenerālprokurora noteikumi, tika izveidots jauns tiesiskās aizsardzības mehānisms, kas paredzēts, lai izskatītu un atrisinātu fizisku personu iesniegtās atbilstīgās sūdzības par ASV sakaru izlūkošanas darbībām[79]. Ikvienai personai ES ir tiesības iesniegt sūdzību tiesiskās aizsardzības mehānismam par iespējamu ASV tiesību aktu, kas reglamentē sakaru izlūkošanas darbības, pārkāpumu (piemēram, IR Nr. 14086, *FISA* 702. pants, IR Nr. 12333) attiecībā uz ASV nosūtītajiem personas datiem, kas negatīvi ietekmē viņu privātumu un pilsoniskās brīvības. Fiziskas personas var iesniegt sūdzību DAI ES dalībvalstī, kas ar EDAK sekretariāta starpniecību nosūta sūdzību uz tiesiskās aizsardzības mehānismu. Mehānismu veido divi līmeņi – *ODNI CLPO* veic sūdzību sākotnējo izmeklēšanu, un fiziskām personām ir iespēja pārsūdzēt *CLPO* lēmumu neatkarīgā *DPRC*. Kad *ODNI CLPO* vai *DPRC* veiktā pārbaude ir pabeigta, ar valsts iestādes starpniecību fiziskas personas tiek informētas, ka "pārbaudē nav konstatēti nekādi pārkāpumi vai arī *ODNI CLPO / DPRC* ir pieņēmusi lēmumu, kurā noteikts veikt atbilstošus korektīvus pasākumus". *ODNI CLPO* un *DPRC* lēmumi ir saistoši izlūkošanas aģentūrām.

Kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas ir veikti turpmāki pasākumi, lai tiesiskās aizsardzības mehānisms pilnībā darbotos.

[76] Komisija norāda, ka daži no šiem ieteikumiem ir iekļauti kā daļa no *RISAA*, ieskaitot ieteikumu par informācijas vākšanu vai ieteikumu par *FISC* ekspertu (*amici*) lomas stiprināšanu.
[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] Lēmuma par aizsardzības līmeņa pietiekamību 176.–194. apsvērums.

Pēc *DPRC* izveidošanas 2023. gada 14. novembrī šajā tiesā tika iecelti astoņi tiesneši (t. i., par diviem tiesnešiem vairāk nekā minimālais skaits, kas noteikts IR Nr. 14086, ko papildina ģenerālprokurora noteikumi 28 C.F.R. § 201.3(a))[80]. Tiesneši tika iecelti, pamatojoties uz IR Nr. 14086 noteiktajiem kritērijiem un saskaņā ar tajā noteikto procesu, kā arī pēc apspriešanās ar *PCLOB*[81]. To vidū ir bijušie Federālās apgabaltiesas un Apelācijas tiesas tiesneši, bijušais ASV ģenerālprokurors un bijušais *PCLOB* loceklis. Kā noteikts IR, vismaz pusei tiesnešu ir iepriekšēja pieredze tieslietu jomā. Turklāt 2024. gada aprīlī tika iecelti divi īpaši advokāti – praktizējoši juristi ar speciālām zināšanām gan privātuma, gan valsts drošības jomā, – lai pārstāvētu fizisku personu intereses *DPRC*. Pārskatīšanas sanāksmē tika apstiprināts, ka visi tiesneši un īpašie advokāti ir saņēmuši augstāko drošības pielaidi un tāpēc, pildot savus uzdevumus *DPRC* uzdevumā, var piekļūt klasificētiem materiāliem. *DPRC* bija arī publicējusi virkni bieži uzdotu jautājumu, sniedzot vairāk informācijas par tās lomu, neatkarību un darbību[82].

Attiecībā uz sūdzību izskatīšanu *ODNI* 2022. gada 6. decembrī pieņēma Izlūkdienestu direktīvu Nr. 126, kurā detalizēti reglamentēti (nosakot termiņus, izveidojot drošu elektronisko repozitoriju un saziņas kanālus, pieprasot *CLPO* un izlūkdienestu struktūrām sadarboties ar *PCLOB* tiesiskās aizsardzības mehānisma ikgadējās pārskatīšanas kontekstā utt.) dažādi sūdzību izmeklēšanas un iztiesāšanas procesa aspekti[83]. Šī direktīva ir piemērojama visā ASV Izlūkdienestā, un to papildina turpmākas iekšējās procedūras, ko pieņēmušas atsevišķas izlūkošanas aģentūras attiecībā uz to sadarbību ar *ODNI CLPO* saistībā ar sūdzības izskatīšanu (piemēram, droša repozitorija izveide sūdzību un atbildes dokumentu apmaiņai un droša saziņa starp attiecīgajām aģentūrām). Turpmākajos mēnešos *DPRC* arī izstrādās detalizētākus noteikumus par sūdzību izskatīšanu un citiem procedūras aspektiem.

Eiropas Savienībā un Amerikas Savienotajās Valstīs tika veikti vairāki papildu pasākumi, lai informētu plašu sabiedrību, kā arī atvieglotu sūdzību iesniegšanu un izskatīšanu. Tas ietver EDAK pieņemto informatīvo norādi par jauno tiesiskās aizsardzības mehānismu[84], sūdzības veidlapas veidni (ko paredzēts tulkot un ko visas DAI publicēs savās valsts valodās)[85] un reglamentu, kas reglamentē sadarbību starp valstu uzraudzības iestādēm un EDAK sekretariātu[86]. Tāpat *ODNI* publicēja bieži uzdotus jautājumus un faktu lapu par jauno tiesiskās aizsardzības mehānismu un iesaistījās sabiedrības izpratnes veicināšanas pasākumos[87].

Turklāt pagājušajā gadā EDAK un attiecīgās ASV iestādes ir cieši sadarbojušās vairākos darbības aspektos. Konkrētāk, kā tika apstiprināts pārskatīšanas sanāksmē, tās izveidoja šifrētu saziņas kanālu sūdzību nosūtīšanai no ES valstu iestādēm EDAK sekretariātam, no EDAK

---

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.

[81] IR Nr. 14086 iedaļa 3(d)(A).

[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_en.

[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en.

[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.

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

sekretariāta uz *ODNI CLPO*, kā arī uz *DoJ* Privātuma un pilsonisko brīvību biroju (*OPCL*) un starp *ODNI CLPO* un citām iestādēm ASV (piemēram, *DPRC*). Turklāt *ODNI CLPO* paskaidroja, ka ir ieviestas papildu iekšējās procedūras atsevišķu izlūkošanas aģentūru sadarbībai ar *ODNI CLPO* attiecībā uz sūdzību izskatīšanu.

Visbeidzot, *OPCL*, kas sniedz administratīvu atbalstu *DPRC*, arī informēja, ka *DPRC* darbojas saskaņā ar savu īpašo budžeta pozīciju un tai ir nodrošinātas nepieciešamās iekārtas uzdevumu veikšanai, tajā skaitā droši datori un klēpjdatori, tālruņi u. c. Turklāt, kā noteikts IR Nr. 14086, *DoC* ir veikusi nepieciešamos pasākumus, arī izveidojot šifrētu sakaru kanālu ar *ODNI CLPO*, lai reģistrētu visas saņemtās atbilstīgās sūdzības. *DoC* regulāri sazināsies ar *ODNI CLPO* par to, vai informācija, kas attiecas uz fiziskas personas sūdzību, ir deklasificēta. Ja atbilde ir apstiprinoša, *DoC* par to paziņos attiecīgajai personai, lai ļautu tai piekļūt šādai informācijai.

Pārskatīšanas sanāksmes laikā ES uzraudzības iestādes nebija saņēmušas sūdzības, un tāpēc jaunais tiesiskās aizsardzības mehānisms vēl nebija sācis darboties.

3. SECINĀJUMS

Pamatojoties uz šajā pirmajā pārskatīšanā savākto informāciju, Komisija secina, ka ASV iestādes ir ieviesušas vajadzīgās struktūras un procedūras, lai nodrošinātu datu privātuma regulējuma efektīvu darbību. Šajā kontekstā Komisija augstu vērtē ļoti labo sadarbību ar ASV iestādēm pārskatīšanas veikšanai.

Lai gan šī pirmā pārskatīšana pamatoti bija vērsta uz to, lai pārbaudītu, vai ir ieviesti visi regulējuma pamatelementi, pieredze, kas iegūta tikai pēc viena darbības gada, praktiski piemērojot aizsardzības pasākumus, kuri attiecas gan uz datu apstrādi, ko veic sertificēti uzņēmumi, gan uz publisko iestāžu piekļuvi datiem, protams, ir ierobežota. Tāpēc Komisija stingri uzraudzīs attiecīgās norises nākamajos mēnešos un gados, īpašu uzmanību pievēršot 1) gaidāmajiem *PCLOB* ziņojumiem par IR Nr. 14086 īstenošanu un sakaru izlūkošanas tiesiskās aizsardzības mehānisma un jo īpaši *DPRC* darbību; 2) iespējamiem turpmākiem *FISA* 702. panta grozījumiem un 3) *PCLOB* locekļu kandidātu izvirzīšanai un iecelšanai, lai aizpildītu gaidāmās vakances.

Turklāt, lai nodrošinātu nepārtrauktu un efektīvu darbību, Komisija uzskata, ka ir svarīgi, ka:

- kā paziņots pārskatīšanas sanāksmē, *DoC* pilnīgāk izmanto dažādus DPR paredzētos rīkus, lai uzraudzītu, kā uzņēmumi ievēro DPR principus, un atklātu nepatiesus apgalvojumus par dalību;
- *FTC* turpina attīstīt savu proaktīvo pieeju izmeklēšanai un izpildei attiecībā uz to, kā sertificēti uzņēmumi ievēro DPR principus, un
- *DoC*, *FTC* un ES datu aizsardzības iestādes izstrādā kopīgus norādījumus par galvenajām prasībām saskaņā ar DPR principiem, piemēram, attiecībā uz cilvēkresursu datiem un tālāku nosūtīšanu.

Ņemot vērā šo pārskatīšanas rezultātu un kā paredzēts lēmuma par aizsardzības līmeņa pietiekamību 211. apsvērumā, Komisija uzskata, ka ir lietderīgi nākamo periodisko pārskatīšanu veikt pēc trim gadiem. Tam vajadzētu dot iespēju gūt lielāku pieredzi DPR praktiskajā piemērošanā un ņemt vērā iepriekš minētās gaidāmās norises. Tāpēc Komisija

saskaņā ar lēmuma par aizsardzības līmeņa pietiekamību 3. panta 4. punktu apspriedīsies ar EDAK un komiteju, kas izveidota saskaņā ar Vispārīgās datu aizsardzības regulas 93. panta 1. punktu, par turpmākās pārskatīšanas periodiskumu.