II

(Neleģislatīvi akti)

LĒMUMI

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2016/1250

(2016. gada 12. jūlijs)

saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK par pienācīgu aizsardzību, ko nodrošina ES un ASV privātuma vairogs

(izziņots ar dokumenta numuru C(2016) 4176)

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti ([1]) un jo īpaši tās 25. panta 6. punktu,

pēc apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju ([2]),

1. IEVADS

(1) Direktīvā 95/46/EK ir paredzēti noteikumi datu pārsūtīšanai no dalībvalstīm uz trešajām valstīm tādā mērā, cik šāda pārsūtīšana ietilpst tās darbības jomā.

(2) Direktīvas 95/46/EK 1. panta un tās preambulas 2. un 10. apsvēruma mērķis ir nodrošināt ne tikai efektīvu un pilnīgu fizisku personu pamattiesību un brīvību aizsardzību, jo īpaši pamattiesības uz privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi, bet arī augstu šo pamattiesību un brīvību aizsardzības līmeni ([3]).

(3) Tas, cik svarīgas ir gan pamattiesības uz privātās dzīves neaizskaramību, kas noteiktas Eiropas Savienības Pamattiesību hartas 7. pantā, gan pamattiesības uz personas datu aizsardzību, kas noteiktas 8. pantā, ir uzsvērts Tiesas judikatūrā ([4]).

(4) Atbilstīgi Direktīvas 95/46/EK 25. panta 1. punktam dalībvalstīm ir jāparedz, ka personas datu nosūtīšana trešajai valstij var notikt tikai tad, ja attiecīgā trešā valsts nodrošina pienācīgu datu aizsardzības līmeni un ja pirms nosūtīšanas ir ievēroti dalībvalsts tiesību akti, ar kuriem tiek īstenoti citi direktīvas noteikumi. Komisija var konstatēt, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni, pamatojoties uz savu iekšējo tiesisko kārtību vai starptautiskajām saistībām, ko tā uzņēmusies, lai aizsargātu personu tiesības. Tādā gadījumā un neierobežojot atbilstību valsts tiesību normām, kas pieņemtas saskaņā ar citiem Direktīvas noteikumiem, personas datus var pārsūtīt no dalībvalstīm bez nepieciešamām papildu garantijām.

([1]) OV L 281, 23.11.1995., 31. lpp.
([2]) Sk. atzinumu 4/2016 par projektu lēmumam par aizsardzības līmeņa pietiekamību attiecībā uz ES un ASV privātuma vairogu, kas publicēts 2016. gada 30. maijā.
([3]) Lieta C-362/14 *Maximillian Schrems/Data Protection Commissioner ("Schrems")*, EU:C:2015:650, 39. punkts.
([4]) Lieta C-553/07, *Rijkeboer*, EU:C:2009:293, 47. punkts; apvienotās lietas C-293/12 un C-594/12, *Digital Rights Ireland un citi*, EU:C:2014:238, 53. punkts; lieta C-131/12, *Google Spain un Google*, EU:C:2014:317, 53., 66. un 74. punkts.

(5) Atbilstīgi Direktīvas 95/46/EK 25. panta 2. punktam trešās valsts nodrošinātā aizsardzības līmeņa pietiekamība ir jānovērtē, paturot prātā visus ar datu pārsūtīšanas darbību vai datu pārsūtīšanas darbību kopumu cieši saistītos apstākļus, tostarp attiecīgajā trešajā valstī spēkā esošās vispārējās un nozaru tiesību normas.

(6) Komisijas Lēmumā 2000/520/EK ([5]) Direktīvas 95/46/EK 25. panta 2. punkta izpratnē tika uzskatīts, ka "privātuma drošības zonas principi", kas īstenoti saskaņā ar tā sauktajiem "visbiežāk uzdotajiem jautājumiem", kurus izdevusi ASV Tirdzniecības ministrija, nodrošina pienācīgu to personas datu aizsardzības līmeni, kas no Savienības tiek nosūtīti Amerikas Savienoto Valstu organizācijām.

(7) Komisija tās 2013. gada 27. novembra paziņojumos COM(2013) 846 final ([6]) un COM(2013) 847 final ([7]) uzskatīja, ka drošības zonas pamats ir jāpārskata un jāstiprina, ņemot vērā kontekstu, ko rada vairāki faktori, tostarp to datu plūsmu eksponenciāla palielināšanās un to nozīmīgums transatlantiskajai ekonomikai, to ASV uzņēmumu skaita straujā palielināšanās, kuri ir iesaistījušies drošības zonas shēmā, un jaunākā informācija par ASV izlūkošanas programmu mērogu un darbības jomu, kas rada jaunus jautājumus par aizsardzības līmeni, ko tā varētu garantēt. Papildus Komisija norādīja vairākus trūkumus un nepilnības drošības zonas shēmā.

(8) Pamatojoties uz Komisijas savāktajiem pierādījumiem, tostarp informāciju no ES un ASV kontaktgrupas privātuma jautājumos ([8]) un informāciju par ASV izlūkošanas programmām, kas saņemta ES un ASV *ad hoc* darba grupā ([9]), Komisija izstrādāja 13 ieteikumus drošības zonas shēmas pārskatīšanai. Šie ieteikumi bija vērsti uz privātuma materiāltiesisko principu stiprināšanu, pašsertificētu ASV uzņēmumu privātuma politikas pārredzamības palielināšanu, šo principu ievērošanas labāku uzraudzību, pārraudzību un piemērošanu no ASV iestāžu puses, pieejamiem strīdu risināšanas mehānismiem un nepieciešamību nodrošināt, ka Lēmumā 2000/520/EK noteiktais valsts drošības izņēmums tiek izmantots absolūti nepieciešamā un samērīgā apmērā.

(9) Savā 2015. gada 6. oktobra spriedumā lietā C-362/14 *Maximillian Schrems/Data Protection Commissioner* ([10]) Tiesa pasludināja Lēmumu 2000/520/EK par spēkā neesošu. Nepārbaudot drošības zonas privātuma principus pēc būtības, Tiesa pieņēma, ka Komisija šajā lēmumā nebija norādījusi, ka Amerikas Savienotās Valstis tiešām "nodrošināja" pienācīgu aizsardzības līmeni, pamatojoties uz savu iekšējo tiesisko kārtību vai starptautiskajām saistībām, ko tās uzņēmušās ([11]).

(10) Šajā sakarā Tiesa paskaidroja, ka, lai arī Direktīvas 95/46/EK 25. panta 6. punktā minētais jēdziens "pienācīgs aizsardzības līmenis" neapzīmē aizsardzības līmeni, kas ir identisks tam, kas noteikts ES tiesību sistēmā, ar to ir jāsaprot, ka trešajai valstij ir jānodrošina tāds pamattiesību un pamatbrīvību aizsardzības līmenis, kas ir "būtībā ekvivalents" tam, kādu nodrošina Savienība saskaņā ar Direktīvu 95/46/EK, kas interpretēta atbilstoši Pamattiesību hartai. Pat ja līdzekļi, kurus trešā valsts šajā sakarā izmanto, var atšķirties no tiem, kurus izmanto Savienībā, šiem līdzekļiem tik un tā praksē ir jābūt efektīviem ([12]).

(11) Tiesa kritizēja pietiekamu konstatējumu trūkumu Lēmumā 2000/520/EK par to, ka Amerikas Savienotajās Valstīs ir spēkā valsts tiesību akti, kuru mērķis ir ierobežot iespējamo iejaukšanos to personu pamattiesībās, kuru dati no Savienības ir nosūtīti uz ASV, iejaukšanos, ko šīs valsts struktūras ir tiesīgas praktizēt, ja tā kalpo leģitīmam mērķim, tādam kā valsts drošība, un par efektīvas tiesiskās aizsardzības pret šāda veida iejaukšanos esamību ([13]).

([5]) Komisijas 2000. gada 26. jūlija Lēmums 2000/520/EK atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem, un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija (OV L 215, 28.8.2000., 7. lpp.).

([6]) Komisijas paziņojums Eiropas Parlamentam un Padomei "Uzticēšanās atjaunošana datu plūsmām starp ES un ASV", COM(2013) 846 final, 2013. gada 27. novembris.

([7]) Komisijas paziņojums Eiropas Parlamentam un Padomei par "drošības zonas" darbību no ES pilsoņu un uzņēmumu, kas veic uzņēmējdarbību ES, viedokļa, COM(2013) 847 final, 2013. gada 27. novembris.

([8]) Sk., piemēram, Eiropas Savienības Padome, ES un ASV Augsta līmeņa kontaktgrupas galīgais pārskata ziņojums par informācijas apmaiņu un privātumu, un personas datu aizsardzību, Piezīme 9831/08, 2008. gada 28. maijs, pieejams tīmekļa vietnē http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf

([9]) Ziņojums par ES un ASV Datu aizsardzības jautājumu darba grupas ES līdzpriekšsēdētāju konstatējumiem, 2013. gada 27. novembris, pieejams tīmekļa vietnē http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

([10]) Sk. 3. zemsvītras piezīmi.

([11]) *Schrems*, 97. punkts.

([12]) *Schrems*, 73.–74. punkts.

([13]) *Schrems*, 88.–89. punkts.

(12) Komisija 2014. gadā bija uzsākusi sarunas ar ASV iestādēm, lai apspriestu drošības zonas shēmas stiprināšanu atbilstīgi 13 ieteikumiem, kas iekļauti paziņojumā COM(2013) 847 final. Pēc Eiropas Savienības Tiesas sprieduma *Schrems* lietā šīs sarunas tika izvērstas ar mērķi izstrādāt iespējamu jaunu atbilstības lēmumu, kas atbilstu Direktīvas 95/46/EK 25. panta prasībām Tiesas interpretācijā. Šo sarunu rezultāts ir dokumenti, kas ir pievienoti šim lēmumam un tiks publicēti arī ASV Federālajā reģistrā. ES un ASV privātuma vairogu veido privātuma principi (II pielikums) kopā ar dažādu ASV iestāžu oficiālajiem apgalvojumiem un saistībām, kas iekļautas I un III–VII pielikuma dokumentos.

(13) Komisija ir rūpīgi izvērtējusi ASV tiesību aktus un praksi, tostarp oficiālos apgalvojumus un saistības. Pamatojoties uz konstatējumiem, kas izklāstīti 136.–140. apsvērumā, Komisija secina, ka Amerikas Savienotās Valstis nodrošina pienācīgu to personas datu aizsardzības līmeni, kas no Savienības tiek nosūtīti pašsertificētām Amerikas Savienoto Valstu organizācijām.

2. ES UN ASV PRIVĀTUMA VAIROGS

(14) ES un ASV privātuma vairoga pamatā ir pašsertifikācijas sistēma, ar kuru ASV organizācijas uzņemas saistības ievērot privātuma principu kopumu – ES un ASV privātuma vairoga pamatprincipus, tostarp papildprincipus (turpmāk kopā "principi") –, ko izdevusi ASV Tirdzniecības ministrija un kas iekļauti šā lēmuma II pielikumā. Tas attiecas uz pārziņiem un apstrādātājiem (pārstāvjiem), turklāt specifika ir tāda, ka pārstrādātāji ir līgumiski saistīti rīkoties tikai saskaņā ar ES pārziņa norādījumiem un palīdzēt tam sniegt atbildes personām, kas īsteno savas tiesības atbilstoši principiem ([14]).

(15) Neskarot atbilstību valsts noteikumiem, kuri pieņemti saskaņā ar Direktīva 95/46/EK, šā lēmuma rezultātā ir atļauts, ka pārzinis vai apstrādātājs Savienībā nosūta datus organizācijām ASV, kas ir apliecinājušas Tirdzniecības ministrijai savu principialitāti un ir apņēmušās ievērot principus. Šie principi attiecas tikai uz ASV organizāciju veiktu personas datu apstrādi tiktāl, ciktāl apstrāde, ko veic šādas organizācijas neietilpst Savienības tiesību aktu piemērošanas jomā ([15]). Privātuma vairogs neskar to Savienības tiesību aktu piemērošanu, kas reglamentē personas datu apstrādi dalībvalstīs ([16]).

([14]) Sk. II pielikuma III daļas 10. punkta a. apakšpunktu. Saskaņā ar definīciju I daļas 8. punkta c. apakšpunktā ES pārzinis noteiks mērķi un līdzekļus personas datu apstrādei. Turklāt līgumā ar pārstāvi ir skaidri jānorāda, vai ir atļauta datu tālāka nosūtīšana (sk. III daļas 10. punkta a. apakšpunkta ii. punkta 2. apakšpunktu).

([15]) Tas attiecas arī uz gadījumiem, kad cilvēkresursu dati tiek nosūtīti no Savienības saistībā ar darba tiesiskajām attiecībām. Lai arī principos ir uzsvērta ES darba devēja "primārā atbildība" (sk. II pielikumu, III.9.d.i.), tajos vienlaikus ir skaidri pateikts, ka uz viņa rīcību attieksies Savienībā un/vai attiecīgajā dalībvalstī piemērojamie noteikumi, nevis principi. Sk. II pielikumu, III daļas 9. punkta a. apakšpunkta i. punktu, b. apakšpunkta i. punktu, c. apakšpunkta i. punktu, d. apakšpunkta i. punktu.

([16]) Tas attiecas arī uz apstrādi, kas notiek pirms nosūtīšanas uz Amerikas Savienotajām Valstīm, izmantojot iekārtas, kas atrodas Savienībā, bet ko izmanto organizācija, kura neatrodas Savienības (skatīt Direktīvas 95/46/EK 4. panta 1. punkta c) apakšpunktu). No 2018. gada 25. maija Vispārīgo datu aizsardzības regulu (*GDPR*) piemēros personas datu apstrādei i) saistībā ar darbībām, ko veic pārziņa vai apstrādātāja uzņēmējdarbības vietā Savienībā (pat ja apstrāde notiek Amerikas Savienotajās Valstīs), vai ii) Savienībā esošu datu subjektu personas datu apstrādei, ko veic pārzinis vai apstrādātājs, kas neveic uzņēmējdarbību Savienībā, ja apstrādes darbības ir saistītas ar a) preču vai pakalpojumu piedāvāšanu šādiem datu subjektiem Savienībā, neatkarīgi no tā, vai no datu subjekta tiek prasīta samaksa; vai b) viņu uzvedības novērošanu, ciktāl viņu uzvedība notiek Savienībā. Sk. 3. panta 1. un 2. punktu Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

(16) Personas datu aizsardzība, ko nodrošina privātuma vairogs, attiecas uz jebkuru ES datu subjektu ([17]), kura personas dati no Savienības tikuši nosūtīti ASV organizācijām, kas ir apliecinājušas Tirdzniecības ministrijai savu principialitāti.

(17) Principus piemēro uzreiz pēc sertifikācijas. Viens izņēmums attiecas uz atbildības par tālāku nosūtīšanu principu gadījumā, kad privātuma vairogam pašsertificētai organizācijai jau ir iepriekš nodibinātas komercattiecības ar trešām personām. Ņemot vērā to, ka var paiet zināms laiks, lai nodrošinātu minēto komercattiecību atbilstību noteikumiem, ko piemēro saskaņā ar atbildības par tālāku nosūtīšanu principu, organizācijai būs pienākums to darīt pēc iespējas ātrāk un jebkurā gadījumā ne vēlāk kā deviņus mēnešus pēc pašsertifikācijas (ar nosacījumu, ka tas notiek pirmo divu mēnešu laikā pēc dienas, kad privātuma vairogs stājas spēkā). Šajā pārejas posmā organizācijām ir jāpiemēro informēšanas un izvēles princips (tādējādi ļaujot ES datu subjektam atteikties) un gadījumos, kad personas dati tiek nosūtīti trešai personai, kas darbojas kā pārstāvis, ir jānodrošina, ka trešā persona nodrošina vismaz tādu pašu aizsardzības līmeni, kāds tiek prasīts ar principiem ([18]). Šis pārejas periods nodrošina saprātīgu un atbilstošu līdzsvaru starp pamattiesību uz datu aizsardzību ievērošanu un uzņēmumu likumīgajām vajadzībām, lai būtu pietiekami daudz laika pielāgoties jaunajam regulējumam situācijās, kad tas ir atkarīgs arī no viņu komercattiecībām ar trešām personām.

(18) Sistēmu pārvaldīs un uzraudzīs Tirdzniecības ministrija, pamatojoties uz tās saistībām, kas izklāstītas ASV tirdzniecības sekretāra apgalvojumos (šā lēmuma I pielikums). Attiecībā uz principu piemērošanu Federālā tirdzniecības komisija (FTK) un Transporta ministrija ir izteikusi apgalvojumus, kas iekļauti šā lēmuma IV pielikumā un V pielikumā.

2.1. *Privātuma principi*

(19) Pašsertifikācijas ietvaros saskaņā ar ES un ASV privātuma vairogu organizācijām ir jāapņemas ievērot principus ([19]).

(20) Saskaņā ar *informēšanas principu* organizāciju pienākums ir sniegt informāciju datu subjektiem par vairākiem būtiskiem elementiem, kas saistīti ar viņu personas datu apstrādi (piemēram, ievākto datu veids, apstrādes mērķis, piekļuves tiesības un izvēle, nosacījumi tālākai nosūtīšanai un atbildība). Tiek piemēroti arī citi aizsardzības pasākumi, jo īpaši prasība organizācijām publiskot to privātuma politiku (kas atspoguļo principus) un norādīt saites uz Tirdzniecības ministrijas tīmekļa vietni (ar plašāku informāciju par pašsertifikāciju, datu subjektu tiesībām un pieejamajiem tiesību aizsardzības mehānismiem), privātuma vairoga sarakstu (minēts 30. apsvērumā) un atbilstoša alternatīva strīdu izšķiršanas pakalpojumu sniedzēja tīmekļa vietni.

(21) Saskaņā ar *datu integritātes un mērķa ierobežojumu principu* personas dati ir jāierobežo tādā apmērā, lai tie atbilstu apstrādes mērķiem, būtu uzticami to lietošanas paredzētajam mērķim, precīzi, pilnīgi un aktuāli. Organizācija nedrīkst apstrādāt personas datus tādā veidā, kas neatbilst mērķim, kuram tie sākotnēji vākti vai kuram datu subjekts pēc tam atļāvis tos izmantot. Organizācijām ir jānodrošina, ka personas dati saistībā ar paredzētajiem mērķiem ir ticami, precīzi, pilnīgi un aktuāli.

([17]) Šis lēmums attiecas uz EEZ. Līgumā par Eiropas Ekonomikas zonu (EEZ līgums) paredzēta Eiropas Savienības iekšējā tirgus paplašināšana, iekļaujot trīs EBTA valstis: Islandi, Lihtenšteinu un Norvēģiju. Uz Savienības datu aizsardzības tiesību aktiem, tostarp Direktīvu 95/46/EK, attiecas EEZ līgums, un tā ir iekļauta līguma XI pielikumā. EEZ Apvienotā komitejai ir jāpieņem lēmums par šā lēmuma iekļaušana EEZ līgumā. Pēc tam, kad šo lēmumu piemēros Islandei, Lihtenšteinai un Norvēģijai, ES un ASV privātuma vairogs attieksies arī uz šīm trim valstīm, un atsauces privātuma vairoga paketē uz ES un tās dalībvalstīm tiks lasītas kā atsauces, kas attiecas arī uz Islandi, Lihtenšteinu un Norvēģiju.

([18]) Sk. II pielikuma III daļas 6. punkta e. apakšpunktu.

([19]) Īpaši noteikumi, ar kuriem tiek nodrošināti papildu aizsardzības pasākumi, tiek piemēroti cilvēkresursu datiem, kas tiek vākti saistībā ar nodarbinātību, kā norādīts privātuma principu papildprincipā par "cilvēkresursu datiem" (Sk. II pielikuma III daļas 9. punktu). Piemēram, darba devējiem būtu jāievēro darba ņēmēju vēlmes attiecībā uz privātumu, ierobežojot piekļuvi personas datiem, noteiktus datus padarot anonīmus vai piešķirot kodus vai pseidonīmus. Vissvarīgākais ir tas, ka organizācijām ir jāsadarbojas un jāievēro Savienības datu aizsardzības iestāžu ieteikumi attiecībā uz šādiem datiem.

(22) Ja jauns (mainīts) mērķis būtiski atšķiras, bet ir savietojams ar sākotnējo mērķi, *izvēles princips* paredz datu subjektu tiesības iebilst (atteikums). *Izvēles princips* neaizstāj skaidro aizliegumu attiecība uz nesaderīgu apstrādi ([20]). Īpašus noteikumus, kas kopumā ļauj "jebkurā laikā" atteikties no personas datu izmantošanas, piemēro tiešajai tirgvedībai ([21]). Sensitīvu datu gadījumā organizācijām parasti ir jāsaņem datu subjekta skaidra piekrišana (piekrišana).

(23) Vēl saskaņā ar *datu integritātes un mērķa ierobežojuma principu* personas datus var glabāt formā, kas identificē personu vai padara tās identificēšanu iespējamu, (un tādējādi personas datu formā) tikai tik ilgi, kamēr tas nepieciešams mērķim (-iem), kam dati sākotnēji tika vākti vai vēlāk atļauta to izmantošana. Šis pienākums neliedz privātā vairoga organizācijām turpināt apstrādāt personas datus ilgāku laiku, bet tikai tik ilgi un tādā mērā, ciktāl šāda apstrāde ir pamatota viena vai vairāku šādu īpašo mērķu nolūkā: arhivēšana sabiedrības interesēs, žurnālistika, literatūra un māksla, zinātniskā un vēstures pētniecība un statistiskā analīze. Lai viena no minēto mērķu nolūkā personas datus uzglabātu ilgāku laiku, būs nepieciešami principu nodrošinātie aizsardzības pasākumi.

(24) Saskaņā ar *drošības principu* organizācijām, kas rada, uztur, izmanto vai izplata personas datus, ir jāveic "samērīgi un atbilstīgi" drošības pasākumi, ņemot vērā ar apstrādi saistītos riskus un datu veidu. Ja apstrādi veic apakšuzņēmums, organizācijām ir jānoslēdz līgums ar apstrādātāju, kas garantē tādu pašu aizsardzības līmeni, ko nodrošina principi, un jāveic darbības, lai nodrošinātu tā pienācīgu īstenošanu.

(25) Saskaņā ar *piekļuves principu* ([22]) datu subjektiem ir tiesības bez pamatota iemesla un tikai par nepārmērīgu samaksu saņemt no organizācijas apstiprinājumu par to, vai attiecīgā organizācija apstrādā ar viņiem saistītus personas datus, un šie dati ir jāpaziņo saprātīgā termiņā. Šīs tiesības var ierobežot tikai izņēmuma situācijās; jebkādam atteikumam vai ierobežojumam attiecībā uz piekļuves tiesībām ir nepieciešams obligāts un pienācīgs pamatojums, organizācijai uzņemoties slogu, kas saistīts ar šo prasību izpildes apliecināšanu. Datu subjektiem ir jāspēj arī labot, grozīt vai dzēst personisko informāciju, ja tā ir nepareiza vai apstrādāta, pārkāpjot principus. Attiecība uz jomām, kurās uzņēmumi visdrīzāk izmantotu personas datu automatizētu apstrādi, lai pieņemtu lēmumus, kas skar atsevišķu personu (piemēram, aizdevumu izsniegšana, hipotēku piedāvājumi, nodarbinātība), ASV tiesību aktos ir paredzēta īpaša aizsardzība pret nelabvēlīgiem lēmumiem ([23]). Šajos tiesību aktos parasti noteikts, ka personām ir tiesības tikt informētām par īpašiem iemesliem, kas ir lēmuma pamatā (piemēram, atteikums izsniegt kredītu), lai apstrīdētu nepilnīgu vai neprecīzu informāciju (kā arī paļaušanos uz nelikumīgiem elementiem), un prasītu kompensāciju. Šie noteikumi nodrošina aizsardzību tajos (visdrīzāk nedaudzajos) gadījumos, kad automātiskus lēmumus pieņemtu pati privātuma vairoga organizācija ([24]). Tomēr ņemot vērā to, ka modernajā digitālajā ekonomikā automatizētā apstrāde (tostarp profilēšana) arvien plašāk tiek izmantota par pamatu lēmumu pieņemšanā, kas skar atsevišķas personas, šī joma ir cieši jāuzrauga. Lai sekmētu šo uzraudzību, ar ASV iestādēm ir panākta vienošanās, ka dialogs par automatizētu lēmumu pieņemšanu, tostarp informācijas apmaiņa par līdzībām un atšķirībām ES un ASV pieejā šajā ziņā, būs daļa no pirmā gada pārskata, kā arī no turpmākajiem pārskatiem pēc vajadzības.

([20]) Tas attiecas uz visu datu nodošanu saskaņā ar privātuma vairogu, tostarp, ja tiek nodoti dati, kas savākti darba tiesisko attiecību ietvaros. Lai arī pašsertificēta ASV organizācija principā var izmantot cilvēkresursu datus atšķirīgiem mērķiem, kas nav saistīti ar darba tiesiskajām attiecībām, (piemēram, konkrētiem tirgvedības paziņojumiem), tai ir jāievēro nesaderīgas apstrādes aizliegums un organizācija to var darīt tikai saskaņā ar *informēšanas principu* un *izvēles principu*. Aizliegums ASV organizācijai īstenot jebkādu represīvu darbību pret darbinieku, kas izdarījis šādu izvēli, tostarp noteikt jebkādus ierobežojumus attiecībā uz darba iespējām, nodrošinās, ka, neraugoties uz subordinācijas un pakļautības attiecībām, uz darba ņēmēju netiks izdarīts spiediens un tādējādi var izdarīt patiesi brīvu izvēli.

([21]) Sk. II pielikuma III daļas 12. punktu.

([22]) Sk. arī papildprincipu par "piekļuvi" (II pielikuma III daļas 8. punktu).

([23]) Sk., piemēram, *Equal Credit Opportunity Act* (*ECOA, 15 U.S.C. 1691 et seq.*), *Fair Credit Reporting Act* (*FRCA, 15 USC § 1681 et seq.*), vai *Fair Housing Act* (*FHA, 42 U.S.C. 3601 et seq.*).

([24]) Saistībā ar ES vāktu personas datu nosūtīšanu, līgumattiecības ar personu (klientu) vairumā gadījumu būs (un tādējādi jebkuru lēmumu, pamatojoties uz automatizētu apstrādi, parasti pieņems) ES pārzinis, kam jāievēro ES datu aizsardzības noteikumi. Tas ietver gadījumus, kad apstrādi veic privātuma vairoga organizācija, kura darbojas kā pārstāvis ES pārziņa uzdevumā.

(26) Saskaņā ar *tiesību aizsardzības, izpildes un atbildības principu* ([25]) organizācijām, kas līdzdarbojas, ir jānodrošina stabili mehānismi, ar kuriem nodrošināt atbilstību citiem principiem, un to ES datu subjektu tiesību aizsardzība, kuru personas dati ir apstrādāti neatbilstīgā veidā, tostarp efektīvi tiesiskās aizsardzības līdzekļi. Kolīdz organizācija brīvprātīgi nolemj pašsertificēties ([26]) ES un ASV privātuma vairoga ietvaros, tās faktiska atbilstība principiem ir obligāta. Lai varētu turpināt izmantot privātuma vairogu personas datu saņemšanai no Savienības, šādai organizācijai ik gadu ir atkārtoti jāsertificē sava līdzdalība shēmā. Organizācijām arī jāveic pasākumi, lai apliecinātu ([27]), ka to publicētā privātuma politika atbilst principiem un faktiski tiek ievērota. To var izdarīt vai nu caur pašnovērtēšanas sistēmu, kurā jāiekļauj iekšējās procedūras, ar ko tiek nodrošināts, ka darba ņēmēji tiek apmācīti saistībā ar organizācijas privātuma politikas virzieniem un ka atbilstība tiek regulāri objektīvi pārbaudīta, vai arī ārējām atbilstības pārbaudēm, kuru metodes var iekļaut revīzijas vai izlases veida pārbaudes. Turklāt organizācijai ir jāizveido efektīvs tiesiskās aizsardzības mehānisms, lai izskatītu jebkādu sūdzību (šajā sakarā sk. arī 43. apsvērumu), un tai jābūt pakļautai FTK, ASV Transporta ministrijas vai citas ASV pilnvarotas valsts iestādes, kas efektīvi nodrošinās atbilstību principiem, izmeklēšanas un izpildes pilnvarām.

(27) Īpašus noteikumus piemēro tā sauktajai "tālākai nosūtīšanai", proti, organizācijas veiktai personas datu nosūtīšanai trešās personas pārzinim vai apstrādātājam neatkarīgi no tā, vai pēdējais minētais atrodas Amerikas Savienotajās valstīs vai trešā valstī ārpus Amerikas Savienotajām Valstīm (un Savienības). Šo noteikumu mērķis ir nodrošināt, ka ES datu subjektu personas datiem garantētā aizsardzība netiks mazināta un ka tā netiks apieta, to nododot trešām personām. Tas ir īpaši svarīgi sarežģītās ražošanas ķēdēs, kas ir raksturīgas mūsdienu digitālajai ekonomikai.

(28) Saskaņā ar *atbildības par tālāku nosūtīšanu principu* ([28]) jebkura personas datu tālāka nosūtīšana var notikt tikai i) ierobežotos un konkrētos nolūkos, ii) pamatojoties uz līgumu (vai līdzvērtīgu vienošanos uzņēmumu grupas ietvaros ([29])) un iii) vienīgi, ja ar līgumu ir nodrošināts tāds pats aizsardzības līmenis, kādu nodrošina principi, kas ietver prasību, ka principu piemērošana ir ierobežota tiktāl, ciktāl tas nepieciešams, lai tiktu ievērotas valsts drošības, tiesībaizsardzības vai citas sabiedrības intereses ([30]). Tas būtu jālasa kopā ar *informēšanas principu* un gadījumā, kad tiek veikta tālāka nosūtīšana trešās personas pārzinim ([31]) – ar *izvēles principu*, saskaņā ar kuru datu subjekti ir jāinformē (cita starpā) par jebkura saņēmēja – trešās personas tipu/identitāti, tālākas nosūtīšanas mērķi, kā arī par piedāvāto izvēli un iespēju iebilst (atteikums) pret tālāku nosūtīšanu vai, sensitīvu datu gadījumā, nepieciešamību sniegt "skaidru piekrišanu" (piekrišana) tālākai nosūtīšanu. Ņemot vērā *datu integritātes un mērķa ierobežojuma principu*, pienākums nodrošināt tādu pašu aizsardzības līmeni, kādu nodrošina principi, paredz, ka trešā persona drīkst apstrādāt personas datus, kas tai nosūtīti mērķiem, kas nav nesavienojami ar mērķiem, kuriem tie sākotnēji vākti vai kuriem persona pēc tam atļāvusi tos izmantot.

(29) Pienākums nodrošināt tādu pašu aizsardzības līmeni, kādu nosaka principi, attiecas uz visām trešām personām, kas iesaistītas šādi nosūtītu datu apstrādē, neatkarīgi no to atrašanās vietas (ASV vai citā trešā valstī), kā arī uz gadījumiem, kad sākotnējais saņēmējs – trešā persona nosūta minētos datus citam saņēmējam – trešai personai, piemēram, apakšapstrādes nolūkiem. Visos gadījumos līgumā ar saņēmēju – trešo personu ir jānosaka, ka tas informēs privātuma vairoga organizāciju gadījumā, ja tas konstatēs, ka vairs nevar pildīt šo pienākumu. Ja tas tiek

([25]) Sk. arī papildprincipu "Strīdu risināšana un izpilde" (II pielikuma III daļas 11. punktu).
([26]) Sk. arī papildprincipu par "Pašsertifikācija" (II pielikuma III daļas 6. punktu).
([27]) Sk. arī papildprincipu par "Verifikācija" (II pielikuma III daļas 7. punktu).
([28]) Sk. arī papildprincipu "Obligātie līgumi tālākai nosūtīšanai" (II pielikuma III daļas 10. punktu).
([29]) Sk. papildprincipu "Obligātie līgumi tālākai nosūtīšanai" (II pielikuma III daļas 10. punkta b. apakšpunktu). Lai arī šis princips ļauj nosūtīt datus, balstoties arī uz ārpuslīgumiskiem instrumentiem (piemēram, grupas iekšējās atbilstības un kontroles programmas), tekstā ir precizēts, ka šiem instrumentiem vienmēr ir "jānodrošina personas datu aizsardzības nepārtrauktība saskaņā ar principiem". Turklāt, ņemot vērā to, ka pašsertificēta ASV organizācija ir atbildīga par principu ievērošanu, tai būs spēcīgs stimuls izmantot tos instrumentus, kas ir patiešām efektīvi praksē.
([30]) Sk. II pielikuma I daļas 5. punktu.
([31]) Personām nebūs tiesību atteikties, ja personas datus nosūta trešai personai, kas darbojas kā pārstāvis, lai pildītu uzdevumus ASV organizācijas vārdā un saskaņā ar tās norādījumiem. Tomēr, lai to darītu, ir nepieciešams līgums ar pārstāvi, un ASV organizācijas, īstenojot savas pilnvaras sniegt norādījumus, būs atbildīgas par to, lai garantētu aizsardzību saskaņā ar principiem.

konstatēts, trešā persona pārtrauc apstrādi vai ir jāveic citi pamatoti un atbilstoši pasākumi, lai labotu situāciju ([32]). Ja (apakš-)apstrādes ķēdē radīsies atbilstības problēmas, privātuma vairoga organizācijai, kas darbojas kā personas datu pārzinis, būs jāpierāda, ka tā nav atbildīga par notikumu, kura rezultātā radušies zaudējumi, vai kā citādi jāuzņemas atbildība, kā tas precizēts atbilstoši *tiesību aizsardzības, izpildes un atbildības principam*. Papildu aizsardzība ir piemērojama gadījumā, kad tiek veikta tālāka nosūtīšana trešās personas pārstāvim ([33]).

2.2. *ES un ASV privātuma vairoga pārredzamība, pārvaldība un pārraudzība*

(30) ES un ASV privātuma vairogs paredz uzraudzības un izpildes mehānismus, lai pārbaudītu un nodrošinātu, ka pašsertificēti ASV uzņēmumi ievēro principus un ka tiek izskatīts katrs neatbilstības gadījums. Šie mehānismi ir izklāstīti principos (II pielikums) un saistībās, ko uzņēmusies Tirdzniecības ministrija (I pielikums), FTK (IV pielikums) un ASV Transporta ministrija (V pielikums).

(31) Lai nodrošinātu atbilstīgu ES un ASV privātuma vairoga piemērošanu, ieinteresētajām personām, piemēram, datu subjektiem, datu nosūtītājiem un valsts datu aizsardzības iestādēm (DAI) jābūt spējīgām identificēt tās organizācijas, kuras stingri ievēro principus. Tālab ASV Tirdzniecības ministrija ir apņēmusies uzturēt un darīt sabiedrībai zināmu to organizāciju sarakstu, kuras ir apliecinājušas savu principialitāti, un kas ir vismaz vienas no šā lēmuma I un II pielikumā uzskaitīto tiesībaizsardzības iestāžu piekritībā ("privātuma vairoga saraksts") ([34]). Tirdzniecības ministrija atjauninās šo sarakstu, pamatojoties uz organizācijas ikgadējās atkārtotās sertifikācijas iesniegumiem, kā arī tad, kad kāda organizācija izstāsies vai tiks izslēgta no ES un ASV privātuma vairoga. Tā arī darīs sabiedrībai zināmu oficiālu reģistru ar organizācijām, kuras ir dzēstas no saraksta, katrā gadījumā minot dzēšanas iemeslu. Visbeidzot, tā norādīs saiti uz FTK tīmekļa vietnē uzturētu sarakstu ar FTK izpildes lietām, kas saistītas ar privātuma vairogu.

(32) Tirdzniecības ministrija gan privātuma vairoga sarakstu, gan atkārtotās sertifikācijas iesniegumus darīs publiski pieejamus, izmantojot šim nolūkam paredzētu tīmekļa vietni. Savukārt pašsertificētām organizācijām privātuma vairoga sarakstam ir jānorāda ministrijas tīmekļa adresi. Papildus, ja organizācijas paziņojums par privātumu ir pieejams tiešsaistē, tajā ir jāiekļauj hipersaite uz privātuma vairoga tīmekļa vietni, kā arī hipersaite uz neatkarīga tāda tiesību aizsardzības mehānisma tīmekļa vietni vai sūdzības iesniegšanas veidlapu, kas ir pieejams neizskatīto sūdzību atrisināšanai. Tirdzniecības ministrija organizācijas sertifikācijas un atkārtotās sertifikācijas ietvaros regulāri pārbaudīs, vai tās privātuma politikas virzieni atbilst principiem.

(33) Organizācijas, kuras ir pastāvīgi pārkāpušas principus, tiks dzēstas no privātuma vairoga saraksta, un tām būs jānodod atpakaļ vai jāizdzēš ES un ASV privātuma vairoga ietvaros saņemtie personas dati. Citos dzēšanas gadījumos, piemēram, brīvprātīga izstāšanās vai neveikta atkārtota sertifikācija, organizācija var saglabāt šādus datus, ja tā Tirdzniecības ministrijai katru gadu apliecina savas saistības turpināt piemērot principus vai nodrošina pienācīgu personas datu aizsardzību citā atļautā veidā (piemēram, izmantojot līgumu, kurā ir pilnībā atspoguļotas attiecīgo līguma standartklauzulu prasības, kuras apstiprinājusi Komisija). Tādā gadījumā organizācijai ir jānorāda organizācijas kontaktpunkts attiecībā uz visiem ar privātuma vairogu saistītajiem jautājumiem.

(34) Tirdzniecības ministrija arī uzraudzīs organizācijas, kuras vairs nav ES un ASV privātuma vairoga dalībnieces tāpēc, ka ir brīvprātīgi izstājušās vai to sertifikācijai beidzas termiņš, lai pārbaudītu, vai tās nodos atpakaļ, dzēsīs vai saglabās ([35]) iepriekš shēmas ietvaros saņemtos personas datus. Ja tās saglabā šos datus, organizāciju

([32]) Situācija ir atšķirīga atkarībā no tā, vai trešā persona ir pārzinis vai apstrādātājs (pārstāvis). Pirmajā gadījumā līgumā ar trešo personu ir jānosaka, ka šī trešā persona pārtrauc apstrādi vai veic citus pamatotus un atbilstošus pasākumus, lai labotu situāciju. Otrajā gadījumā šie pasākumi jāveic privātuma vairoga organizācijai – jo tā kontrolē apstrādi, saskaņā ar kuras norādēm pārstāvis darbojas.

([33]) Šādā gadījumā ASV organizācijai arī ir jāveic pamatoti un atbilstoši pasākumi, lai i) nodrošinātu, ka pārstāvis efektīvi apstrādā nosūtītos personas datus veidā, kas saskan ar organizācijas saistībām atbilstoši principiem, un ii) lai, saņemot paziņojumu, apturētu un labotu neatļautu apstrādi.

([34]) Informācija par privātuma vairoga saraksts pārvaldību ir atrodama I pielikumā un II pielikumā (I daļas 3. punktu, I daļas 4. punktu, III daļas 6. punkta d. apakšpunktu un III daļas 11. punkta g. apakšpunktu).

([35]) Skatīt, piem., II pielikuma I daļas 3. punktu, III daļas 6. punkta f. apakšpunktu un III daļas 11. punkta g. apakšpunkta i. punktu.

pienākums ir arī turpmāk piemērot principus šiem personas datiem. Gadījumos, kad Tirdzniecības ministrija būs izdzēsusi organizācijas no shēmas saistībā ar pastāvīgu principu neievērošanu, tā nodrošinās, ka minētās organizācijas nodod atpakaļ vai izdzēš personas datus, kurus tās saņēmušas shēmas ietvaros.

(35) Ja kāda organizācija jebkāda iemesla dēļ izstājas no ES un ASV privātuma vairoga, tai ir jāizdzēš visi publiskie apgalvojumi, kuros minēts, ka tā turpina līdzdarboties ES un ASV privātuma vairogā vai ka tai ir tiesības uz priekšrocībām, jo īpaši jebkādas atsauces uz ES un ASV privātuma vairogu tās publicētajā paziņojumā par privātumu. Tirdzniecības ministrija meklēs nepatiesus apgalvojumus, tostarp kādreizējo dalībnieku izteiktus apgalvojumus par līdzdalību sistēmā, un vērsīsies pret tiem ([36]).Uz jebkādiem maldinošiem izteikumiem sabiedrībai, ko maldinošu apgalvojumu vai prakses formā ir izteikusi kāda organizācija par savu principialitāti, attiecas izpildes darbības, ko īsteno FTK, Transporta ministrija vai citas atbilstīgas ASV tiesībaizsardzības iestādes; par Tirdzniecības ministrijai sniegtiem maldinošiem izteikumiem piemēro tiesībaizsardzības darbības saskaņā ar Likumu par nepatiesu ziņu sniegšanu (*False Statements Act*) (18 U.S.C. § 1001) ([37]).

(36) Tirdzniecības ministrija pēc savas iniciatīvas uzraudzīs jebkādus nepatiesus apgalvojumus par līdzdalību privātuma vairoga shēmā vai neatbilstīgu privātuma vairoga sertifikācijas zīmes izmantošanu, un DAI var nodot organizācijas izskatīšanai speciāliem ministrijas kontaktpunktiem. Kad organizācija ir izstājusies no ES un ASV privātuma vairoga shēmas, neveic atkārtotu sertifikāciju vai tiek dzēsta no privātuma vairoga saraksta, Tirdzniecības ministrija pastāvīgi pārbauda, vai tā no sava publicētā paziņojuma par privātumu ir izdzēsusi jebkāda veida atsauces uz privātuma vairogu, kuras liecina par tās turpmāku līdzdalību, un, ja tā turpina izteikt nepatiesus apgalvojumus, nodod lietu FTK, Transporta ministrijai vai citai kompetentai iestādei iespējamu izpildes darbību veikšanai. Tā arī sūtīs aptaujas lapas organizācijām, kuru pašsertifikācijai beidzas termiņš vai kuras ir brīvprātīgi izstājušās no ES un ASV privātuma vairoga shēmas, lai noskaidrotu, vai organizācija nodos atpakaļ, dzēsīs vai turpinās piemērot privātuma principus personas datiem, kurus tā ir saņēmusi, līdzdarbojoties ES un ASV privātuma vairoga shēmā, un, ja personas dati tiks saglabāti, pārbaudīs, kurš organizācijā būs pastāvīgais kontaktpunkts attiecībā uz visiem ar privātuma vairogu saistītajiem jautājumiem.

(37) Tirdzniecības ministrija pēc savas iniciatīvas pastāvīgi veiks pašsertificētu organizāciju atbilstības pārbaudes ([38]), tostarp izsūtot detalizētas aptaujas lapas. Tā arī veiks sistemātiskus pārskatus katru reizi, kad tiks saņemta konkrēta (nozīmīga) sūdzība, ja organizācija nesniegs pienācīgas atbildes uz tās pieprasījumiem vai ja būs ticami pierādījumi, kas liecinās, ka organizācija varētu neievērot principus. Attiecīgos gadījumos Tirdzniecības ministrija par šādām atbilstības pārbaudēm apspriedīsies arī ar DAI.

2.3. *Tiesiskās aizsardzības mehānismi, sūdzību izskatīšana un izpilde*

(38) ES un ASV privātuma vairogs ar *tiesību aizsardzības, izpildes un atbildības principu* nosaka, ka organizācijām ir jānodrošina personām, kuras ir ietekmējusi neatbilstība, iespēja vērsties pēc palīdzības un tādējādi iespēja ES datu subjektiem iesniegt sūdzības par pašsertificētu ASV uzņēmumu neatbilstību un rast risinājumu šīm sūdzībām, nepieciešamības gadījumā ar lēmumu, kas nodrošina efektīvu tiesiskās aizsardzības līdzekli.

(39) Pašsertifikācijas ietvaros organizācijām jāievēro tiesību aizsardzības, izpildes un atbildības principa prasības, paredzot efektīvus un viegli pieejamus neatkarīgus tiesību aizsardzības mehānismus, ar kuriem katras personas sūdzības un strīdus var izmeklēt un efektīvi atrisināt, neradot izmaksas personai.

(40) Organizācijas var izvēlēties neatkarīgu tiesību aizsardzības mehānismu Savienībā vai Amerikas Savienotajās Valstīs. Tas ietver iespēju brīvprātīgi apņemties sadarboties ar ES DAI. Tomēr šādas izvēles nav, ja organizācijas

([36]) Sk. I pielikuma sadaļu "Nepatiesu apgalvojumu par līdzdalību meklēšana un vēršanās pret tiem".
([37]) Sk. II pielikumu, III daļas 6. punkta h. apakšpunktu un III daļas 11. punkta f. apakšpunktu.
([38]) Sk. I pielikumu.

apstrādā cilvēkresursu datus, jo šajā gadījumā sadarbība ar DAI ir obligāta. Citas alternatīvas ietver neatkarīgu alternatīvu strīdu risināšanu (ADR) vai privātajā sektorā izstrādātas *privātuma programmas*, kuru noteikumos iekļauti privātuma principi. Tajā jāietver efektīvi izpildes mehānismi saskaņā ar tiesību aizsardzības, izpildes un atbildības principa prasībām. Organizācijām ir pienākums novērst jebkuras neatbilstības problēmas. Tajos arī jānorāda, ka tās ir pakļautas FTK, Transporta ministrijas vai kādas citas ASV pilnvarotas valsts iestādes izmeklēšanas un izpildes pilnvarām.

(41) Attiecīgi privātuma vairoga regulējums paredz datu subjektiem vairākas iespējas īstenot savas tiesības, iesniegt sūdzības par ASV pašsertificēto uzņēmumu neatbilstību un panākt viņu sūdzību izskatīšanu, ja nepieciešams, pieņemot lēmumu par efektīvu tiesisko aizsardzību. Personas var iesniegt sūdzību tieši organizācijai, neatkarīgai strīdu risināšanas struktūrai, kuru izraudzījusies organizācija, valstu DAI vai FTK.

(42) Gadījumos, kad viņu sūdzības nav atrisinātas, izmantojot jebkuru no šiem tiesībaizsardzības vai izpildes mehānismiem, personām ir arī tiesības pieprasīt saistošu šķīrējtiesu privātuma vairoga komisijas ietvaros (šā lēmuma II pielikuma 1. pielikums). Izņemot šķīrējtiesu, kuras gadījumā vispirms ir jāizmanto daži tiesiskās aizsardzības līdzekļi, pirms var vērsties tiesā, personas pēc savas izvēles var brīvi izvēlēties jebkuru vai visas pārsūdzības mehānismu, un tām nav pienākuma izdarīt izvēli par labu vienam vai otram mehānismam vai ievērojot noteiktu secību. Tomēr pastāv noteikta loģiska secība, ko ir lietderīgi ievērot un kas izklāstīta turpmāk.

(43) Pirmkārt, ES datu subjekti var sekot lietām saistībā ar neatbilstību principiem, tieši sazinoties ar *pašsertificēto ASV uzņēmumu*. Lai sekmētu strīdu risināšanu, organizācijai ir jāievieš efektīvs tiesiskās aizsardzības mehānisms šādu sūdzību izskatīšanai. Tādēļ organizācijas privātuma politikai ir skaidri jāinformē personas par kontaktpunktu organizācijā vai ārpus tās, kas izskatīs sūdzības (tostarp jebkuru atbilstīgu iestādi Savienībā, kura var atbildēt uz pieprasījumiem vai sūdzībām), un par neatkarīgajiem strīdu izskatīšanas mehānismiem.

(44) Saņemot personas sūdzību – gan tieši no pašas personas, gan ar Tirdzniecības ministrijas starpniecību, kad DAI ir nodevusi to izskatīšanai, organizācijai ir jāsniedz atbilde ES datu subjektam 45 dienu laikā. Atbildē ir jābūt sniegtam sūdzības novērtējumam pēc būtības un informācijai par to, kā organizācija atrisinās problēmu. Tāpat organizācijām ir nekavējoties jāatbild uz jautājumiem un citiem informācijas pieprasījumiem no Tirdzniecības ministrijas vai DAI ([39]) (gadījumos, kad organizācija ir uzņēmusies saistības sadarboties ar DAI) attiecībā uz tās principialitāti. Organizācijām ir jāsaglabā sava dokumentācija par to, kā tās īsteno savu privātuma politiku, un pēc pieprasījuma jānodrošina tās pieejamība neatkarīgam tiesību aizsardzības mehānismam vai FTK (vai citai ASV iestādei ar piekritību izmeklēt negodīgu un maldinošu praksi) izmeklēšanas ietvaros vai pēc saņemtas sūdzības par neatbilstību.

(45) Otrkārt, personas var iesniegt sūdzību tieši organizācijas norīkotai *neatkarīgai strīdu risināšanas struktūrai* (Amerikas Savienotajās Valstīs vai Savienībā), kas izmeklē un risina personu sūdzības (ja vien tās nav acīmredzami nepamatotas vai nenozīmīgas) un nodrošina personai atbilstīgu tiesību aizsardzību bez maksas. Šādas struktūras piemērotām sankcijām un tiesiskās aizsardzības līdzekļiem ir jābūt pietiekami stingriem, lai nodrošinātu organizāciju atbilstību principiem, un jāparedz organizācijas veikta neatbilstības ietekmes novēršana vai korekcija un, atkarībā no apstākļiem, tālākas attiecīgo datu apstrādes pārtraukšana un/vai to dzēšana, kā arī neatbilstības konstatējumu publicēšana. Organizācijas norīkotām neatkarīgām strīdu risināšanas struktūrām savās publiskajās tīmekļa vietnēs būs jāiekļauj būtiska informācija par ES un ASV privātuma vairogu un pakalpojumiem tā ietvaros, kurus tās sniedz. Tām katru gadu ir jāpublicē gada ziņojums, kurā sniegta kopējā statistika par šiem pakalpojumiem ([40]).

([39]) Tā ir izskatītāja iestāde, kuru norīkojusi DAI komisija, kas paredzēta papildprincipā par "datu aizsardzības iestāžu lomu" (II pielikuma III daļas 5. punkts).

([40]) Gada ziņojumā ir jāiekļauj: 1) kopējais ar privātuma vairogu saistīto saņemto sūdzību skaits pārskata gadā; 2) saņemto sūdzību veidi; 3) kvalitatīvi strīdu risināšanas pasākumi, piemēram, sūdzību apstrādes ilgums; un 4) saņemto sūdzību rezultāti, īpaši piemēroto tiesiskās aizsardzības līdzekļu vai sankciju skaits un veidi.

(46) Tās atbilstības pārbaudes procedūru ietvaros Tirdzniecības ministrija pārbaudīs, vai pašsertificēti ASV uzņēmumi tiešām ir reģistrējušies neatkarīgajos tiesību aizsardzības mehānismos, kuros, kā tie apgalvo, uzņēmumi ir reģistrējušies. Gan organizācijām, gan atbildīgajiem neatkarīgajiem tiesību aizsardzības mehānismiem ir jāspēj nekavējoties atbildēt uz Tirdzniecības ministrijas jautājumiem un informācijas pieprasījumiem saistībā ar privātuma vairogu.

(47) Gadījumos, kad organizācija neievēro strīdu risināšanas vai pašregulējuma struktūras lēmumu, struktūrai par šādu neievērošanu ir jāinformē Tirdzniecības ministrija un FTK (vai cita ASV iestāde ar piekritību izmeklēt negodīgu vai maldinošu praksi), vai kompetenta tiesa ([41]). Ja organizācija atsakās ievērot jebkuras privātuma pašregulējuma, neatkarīgas strīdu risināšanas vai valdības iestādes galīgo lēmumu vai gadījumā, ja šāda iestāde konstatē, ka organizācija bieži neievēro principus, tas tiks uzskatīts par pastāvīgu neizpildi, kā rezultātā Tirdzniecības ministrija, vispirms informējot organizāciju, kura nav ievērojusi principus, un dodot tai iespēju 30 dienu laikā atbildēt, svītros šo organizāciju no saraksta ([42]). Ja pēc tam, kad organizācija ir svītrota no saraksta, tā turpina apgalvot, ka tai ir privātuma vairoga sertifikācija, ministrija vērsīsies pie FTK vai citas tiesībaizsardzības iestādes ([43]).

(48) Treškārt, personas var arī iesniegt sūdzību valsts *datu aizsardzības iestādei*. Organizācijām ir pienākums sadarboties, kad DAI veic izmeklēšanu un risina sūdzību – gan tad, kad tā attiecas uz cilvēkresursu datu apstrādi, kuri savākti saistībā ar darba tiesiskajām attiecībām, vai ja attiecīgā organizācija ir brīvprātīgi piekritusi DAI uzraudzībai. Jo īpaši organizācijām ir jāatbild uz pieprasījumiem, jāievēro DAI sniegtie ieteikumi, tostarp par tiesiskās aizsardzības vai kompensācijas pasākumiem, un jāsniedz DAI rakstveida apstiprinājums par šādu rīcību.

(49) DAI ieteikumus nodos ar neformālas DAI komisijas starpniecību, kas izveidota Savienības līmenī ([44]) un kas palīdzēs arī nodrošināt saskaņotu un sasaistītu pieeju konkrētai sūdzībai. Ieteikumus sniegs pēc tam, kad abām strīdā iesaistītajām pusēm būs bijusi pienācīga iespēja sniegt komentārus un uzrādīt visus pierādījumus, ko tās vēlas. Attiecīgā komisija sniegs ieteikumus, cik vien drīz to atļaus prasība par pienācīgu izskatīšanu un parasti 60 dienu laikā pēc sūdzības saņemšanas. Ja organizācija 25 dienu laikā pēc ieteikuma sniegšanas to neievēro un nesniedz pienācīgu paskaidrojumu par kavēšanos, komisija paziņo par tās nodomu vai nu iesniegt lietu FTK (vai citai kompetentai ASV tiesībaizsardzības iestādei), vai arī secināt, ka sadarbošanās saistības ir ievērojami pārkāptas. Pirmajā gadījumā rezultāts var būt izpildes darbība saskaņā ar FTK likuma 5. pantu (vai līdzīgu tiesību aktu). Otrajā gadījumā komisija informēs Tirdzniecības ministriju, kas organizācijas atteikumu ievērot DAI komisijas ieteikumu uzskatīs par pastāvīgu pārkāpumu, kā rezultātā organizācija tiks svītrota no privātuma vairoga saraksta.

(50) Ja DAI, kurai sūdzība ir adresēta, sūdzības atrisināšanas nolūkā nav rīkojusies vai ir rīkojusies nepietiekami, attiecīgajam sūdzības iesniedzējam ir iespēja apstrīdēt šādu (bez-)darbību attiecīgās dalībvalsts vietējās tiesās.

(51) Personas var arī iesniegt sūdzību DAI pat tad, ja DAI komisija nav nozīmēta kā organizācijas strīdu risināšanas struktūra. Šādos gadījumos DAI var pārsūtīt šādas sūdzības Tirdzniecības ministrijai vai FTK. Lai sekmētu un palielinātu sadarbību jautājumos saistībā ar personu sūdzībām un privātuma vairoga organizāciju neatbilstību, Tirdzniecības ministrija izveidos speciālu kontaktpunktu, kas darbosies kā koordinators un palīdzēs saistībā ar DAI pieprasījumiem par organizācijas atbilstību principiem ([45]). Tāpat FTK ir apņēmusies izveidot speciālu kontaktpunktu ([46]) un sniegt DAI palīdzību izmeklēšanā saskaņā ar ASV Interneta drošības likumu (*Safe WEb Act*) ([47]).

([41]) Sk. II pielikumu, III daļas 11. punkta e. apakšpunktu.
([42]) Sk. II pielikumu, III daļas 11. punkta g. apakšpunktu, ii. un iii. punktu.
([43]) Sk. I pielikuma sadaļu "Nepatiesu apgalvojumu par līdzdalību meklēšana un vēršanās pret tiem".
([44]) Neformālās DAI komisijas reglamentu pieņem datu aizsardzības iestādes, pamatojoties uz to kompetenci organizēt savu darbu un sadarbojas savā starpā.
([45]) Sk. I pielikuma sadaļas "Palielināta sadarbība ar DAI" un "Sūdzību par neatbilstību atvieglota risināšana" un II pielikuma II daļas 7. punkta e. apakšpunktu.
([46]) Sk. IV pielikuma 6. lpp.
([47]) Turpat.

(52) Ceturtkārt, *Tirdzniecības ministrija* ir uzņēmusies saistības saņemt, izskatīt un darīt visu iespējamo, lai atrisinātu sūdzības par organizācijas neatbilstību principiem. Šajā sakarā Tirdzniecības ministrija nodrošina īpašas procedūras DAI, lai nodotu sūdzības izskatīšanai speciālam kontaktpunktam, izsekotu tās un turpinātu saziņu ar uzņēmumiem, lai sekmētu sūdzību risināšanu. Lai paātrinātu personu sūdzību apstrādi, kontaktpunkts sazināsies tieši ar attiecīgo DAI par atbilstības jautājumiem un īpaši informēs to par sūdzību statusu periodā, kas nepārsniedz 90 dienas pēc nodošanas izskatīšanai. Tas ļauj datu subjektiem iesniegt sūdzības par pašsertificētu ASV uzņēmumu neatbilstību tieši savas valsts DAI un novirzīt tās uz Tirdzniecības ministriju kā ASV iestādi, kas pārvalda ES un ASV privātuma vairogu. Tirdzniecības ministrija ir arī uzņēmusies saistības gada pārskatā par ES un ASV privātuma vairogu sniegt ziņojumu, kurā kopumā analizētas sūdzības, kuras tā saņem katru gadu ([48]).

(53) Ja, pamatojoties uz pārbaudēm, kas veiktas pēc pašas iniciatīvas, sūdzībām vai jebkādu citu informāciju, Tirdzniecības ministrija secinās, ka organizācija ir pastāvīgi pārkāpusi privātuma principus, tā dzēsīs šādu organizāciju no privātuma vairoga saraksta. Atteikums ievērot jebkādas privātuma pašregulējuma, neatkarīgas strīdu risināšanas vai valsts struktūras, tostarp DAI, galīgo lēmumu, tiks uzskatīts par pastāvīgu pārkāpumu.

(54) Piektkārt, privātuma aizsardzības organizācijai ir jābūt pakļautai izmeklēšanas un izpildes pilnvarām, ko īsteno ASV iestādes, jo īpaši *Federālās Tirdzniecības komisija* ([49]), tādējādi efektīvi nodrošinot atbilstību principiem. FTK prioritārā kārtā izskatīs pieprasījumus par neatbilstību privātuma principiem, kuri saņemti no neatkarīgām strīdu risināšanas vai pašregulējuma struktūrām, Tirdzniecības ministrijai un DAI (rīkojoties pēc pašu iniciatīvas vai saskaņā ar sūdzībām) nosakot, vai ir pārkāpts FTK likuma 5. pants ([50]). FTK ir uzņēmusies saistības izstrādāt standartizētu nodošanas izskatīšanai procedūru, norīkot iestādē kontaktpunktu DAI nodoto lietu izskatīšanai un apmainīties ar informāciju par izskatīšanai nodotajām lietām. Tā arī pieņems sūdzības tieši no personām un uzņemsies privātuma vairoga izpēti pēc savas iniciatīvas, jo īpaši plašākas privātuma jautājumu izskatīšanas ietvaros.

(55) FTK var pieprasīt atbilstību ar administratīviem rīkojumiem ("piekrišanas rīkojumi"), un tā sistemātiski uzraudzīs šādu rīkojumu izpildi. Ja organizācijas tos neievēro, FTK var nodot lietu izskatīšanai kompetentajai tiesai, lai piemērotu civiltiesisko atbildību un citus tiesiskās aizsardzības līdzekļus, tostarp par jebkādu kaitējumu prettiesiskas rīcības rezultātā. FTK var arī pieprasīt pagaidu vai pastāvīgu tiesas aizliegumu vai citus tiesiskās aizsardzības līdzekļus federālajā tiesā. Katrā privātuma vairoga organizācijai izsniegtā piekrišanas rīkojumā būs nosacījumi par patstāvīgu ziņošanu ([51]), un organizācijām būs jāpublisko jebkādas būtiskas ar privātuma vairogu saistītas sadaļas jebkurā atbilstības vai novērtējuma ziņojumā, kas iesniegts FTK. Visbeidzot, FTK uzturēs tiešsaistes sarakstu ar uzņēmumiem, kuriem privātuma vairoga lietās piemēroti FTK vai tiesas rīkojumi.

(56) Sestkārt, gadījumā, ja personas sūdzība nav apmierinoši atrisināta ne ar vienu citu pieejamo tiesiskās aizsardzības līdzekli, ES datu subjekts kā galējo tiesību aizsardzības mehānismu var izmantot iespēju pieprasīt saistošu šķīrējtiesu, ko spriež *privātuma vairoga komisija*. Organizācijām ir jāinformē personas par iespēju, ievērojot konkrētus nosacījumus, pieprasīt saistošu šķīrējtiesu, un organizācijām ir pienākums reaģēt, ja persona ir izmantojusi šo iespēju, iesniedzot paziņojumu attiecīgajai organizācijai ([52]).

([48]) Sk. I pielikuma sadaļu "Sūdzību par neatbilstību atvieglota risināšana".

([49]) Privātuma aizsardzības organizācijai ir publiski jāpaziņo par savu apņemšanos ievērot principus, jāpublisko tās privātuma politikas virzieni saskaņā ar šiem principiem un tie pilnībā jāīsteno. To neievērošanas gadījumā piemēro izpildes darbības saskaņā ar FTK likuma 5. pantu, kas aizliedz negodīgas un maldinošas darbības, ko veic tirdzniecībā vai kas to ietekmē.

([50]) Saskaņā ar informāciju, kas saņemta no FTK, tai nav pilnvaru uz vietas veikt pārbaudes privātuma aizsardzības jomā. Tomēr tai ir pilnvaras likt organizācijām iesniegt dokumentus un sniegt liecības (skatīt FTK likuma 20. pantu), un tā var izmantot tiesu sistēmu, lai panāktu šādu rīkojumu izpildi neatbilstības gadījumā.

([51]) FTK vai tiesas rīkojumos var būt prasība uzņēmumiem īstenot privātuma programmas un regulāri darīt FTK zināmus atbilstības ziņojumus vai neatkarīgus šo programmu trešo personu veiktus novērtējumus.

([52]) Sk. II pielikuma II daļas 1. punkta xi. apakšpunktu un III daļas 7. punkta c. apakšpunktu.

(57) Šķīrējtiesas sastāvā ir vismaz 20 šķīrējtiesnešu kopums, kurus iecēlusi Tirdzniecības ministrija un Komisija, pamatojoties uz viņu neatkarību, godīgumu, kā arī pieredzi ASV privātuma un Savienības datu aizsardzības tiesībās. Katram atsevišķam strīdam puses no šī kopuma izvēlēsies vienu vai trīs ([53]) šķīrējtiesnešus. Procedūru regulēs saskaņā ar standarta šķīrējtiesas noteikumiem, par kuriem vienojas Tirdzniecības ministrija un Komisija. Šie noteikumi papildinās jau noslēgto satvaru, kurā ir vairāki elementi, kas pastiprina šā mehānisma pieejamību ES datu subjektiem: i) sagatavojot sūdzību šķīrējtiesai, datu subjektam var palīdzēt tā valsts DAI; ii) lai arī strīda izšķiršana notiks Amerikas Savienotajās Valstīs, ES datu subjekti varēs piedalīties tajā ar videokonferences vai tālruņa konferences starpniecību, kas personai būs jānodrošina bez maksas. iii) lai arī šķīrējtiesā izmantotā valoda parasti būs angļu valoda, taču pēc pamatota pieprasījuma un bez maksas datu subjektam parasti ([54]) tiks nodrošināts šķīrējtiesas lietas izskatīšanas tulkojums; iv) lai arī katrai pusei pašai ir jāuzņemas izdevumi par savu advokātu, ja komisijā to pārstāv advokāts, Tirdzniecības ministrija izveido fondu, kurā tiek iemaksāti ikgadēji privātuma vairoga organizāciju maksājumi, ar kuru var nosegt šķīrējtiesas procedūras attiecināmās izmaksas līdz maksimālajam apmēram, ko noteiks ASV iestādes, konsultējoties ar Komisiju.

(58) Privātuma vairoga komisijai būs tiesības piemērot "personai pielāgotu, taisnīgu nemonetāru palīdzību" ([55]), kas nepieciešams, lai novērstu neatbilstību principiem. Lai arī komisija ņems vērā citus tiesiskās aizsardzības līdzekļus, kas tiek izmantoti citiem privātuma vairoga mehānismiem, personas tik un tā varēs izmantot šķīrējtiesas procedūru, ja tās uzskatīs, ka citi līdzekļi ir bijuši nepietiekami. Tas ļaus ES datu subjektiem pieprasīt šķīrējtiesu visos gadījumos, kad kompetento ASV iestāžu (piemēram, FTK) darbības vai bezdarbības rezultātā sūdzības nebūs izskatītas apmierinoši. Šķīrējtiesu nevar pieprasīt, ja DAI ir likumīgas pilnvaras atrisināt attiecīgo sūdzību attiecībā uz pašsertificētu ASV uzņēmumu, proti, gadījumos, kad organizācijas pienākums ir sadarboties un ievērot DAI ieteikumus par to cilvēkresursu datu apstrādi, kas vākti nodarbinātības ietvaros, vai kad tā ir brīvprātīgi apņēmusies to darīt. Persona var pieprasīt šķīrējtiesas lēmuma izpildi ASV tiesās saskaņā ar Šķīrējtiesas likumu, tādējādi nodrošinot tiesisko aizsardzību gadījumā, ja uzņēmums to nedara.

(59) Septītkārt, ja organizācija nepilda savas saistības ievērot principus un publicētos privātuma politikas virzienus, papildu tiesiskās aizsardzības iespējas var būt pieejamas saskaņā ar ASV tiesībām, kas nodrošina tiesisko aizsardzību saskaņā ar delikta tiesībām un krāpniecisku sagrozījumu, negodīgas vai maldinošas rīcības vai prakses vai līguma saistību neizpildes gadījumā

(60) Turklāt, ja DAI, saņemot ES datu subjekta sūdzību, uzskata, ka personas datu nosūtīšana organizācijai Amerikas Savienotajās Valstīs ir veikta, pārkāpjot ES tiesību aktus datu aizsardzības jomā, tostarp gadījumā, kad ES datu nosūtītājam ir pamats uzskatīt, ka organizācija neievēro principus, DAI var arī izmantot savas pilnvaras attiecībā uz datu nosūtītāju un nepieciešamības gadījumā pieprasīt atcelt datu nosūtīšanu.

(61) Ņemot vērā informāciju šajā sadaļā, Komisija uzskata, ka ASV Tirdzniecības ministrijas izdotie principi kopumā nodrošina tādu personas datu aizsardzības līmeni, kas ir būtībā ekvivalents tam, kādu nodrošina ar Direktīvā 95/46/EK noteiktajiem būtiskajiem pamatprincipiem.

(62) Papildus efektīvu principu piemērošanu garantē pārredzamības prasības un privātuma vairoga pārvaldība un atbilstības pārbaudes, ko veic Tirdzniecības departaments.

(63) Turklāt Komisija uzskata, ka kopumā ar privātuma vairogu nodrošinātā pārraudzība, tiesību aizsardzības un izpildes mehānismi ļauj apzināt un praksē sodīt privātuma vairoga principu pārkāpumus un piedāvāt datu subjektam tiesiskās aizsardzības līdzekļus, kas ļauj piekļūt ar viņu saistītiem personas datiem un galu galā panākt šādu datu labošanu vai dzēšanu.

([53]) Par komisijas šķīrējtiesnešu skaitu ir jāvienojas pusēm.

([54]) Taču komisija var konstatēt, ka konkrētajos strīda izšķiršanas apstākļos tā nodrošināšana var radīt nepamatotas vai nesamērīgas izmaksas.

([55]) Personas nevar pieprasīt zaudējumu atlīdzināšanu šķīrējtiesā, bet šķīrējtiesas pieprasīšana neierobežo iespēju pieprasīt zaudējumu atlīdzināšanu parastās ASV tiesās.

3. PIEKĻUVE ES UN ASV PRIVĀTUMA VAIROGA IETVAROS NOSŪTĪTAJIEM PERSONAS DATIEM UN TO IZMANTOŠANA ASV VALSTS IESTĀDĒS

(64) Kā izriet no II pielikuma I.5. daļas, principialitāte ir ierobežota, ciktāl tas nepieciešams, lai tiktu ievērotas valsts drošības, publisko interešu vai tiesībaizsardzības prasības.

(65) Komisija ir izvērtējusi ierobežojumus un aizsardzības pasākumus, kas pieejami ASV tiesībās attiecībā uz piekļuvi datiem, kuri tiek nosūtīti ES un ASV privātuma vairoga ietvaros, un to izmantošanu ASV valsts iestādēs valsts drošības, tiesībaizsardzības un citu valsts interešu nolūkos. Papildus ASV valdība ar Nacionālās izlūkošanas direktora biroja (NIDB) ([56]) starpniecību ir sniegusi Komisijai detalizētus apgalvojumus un uzņēmusies saistības, kas iekļautas šā lēmuma VI pielikumā. Ar valsts sekretāra parakstītu un šā lēmuma III pielikumā pievienotu vēstuli ASV valdība ir uzņēmusies saistības arī nodrošināt jaunu pārraudzības mehānismu valsts drošības interferencei – privātuma vairoga ombudu, kurš darbojas neatkarīgi no izlūkdienestiem. Visbeidzot, ASV Tieslietu ministrijas apgalvojumos, kas iekļauti šā lēmuma VII pielikumā, ir aprakstīti ierobežojumi un aizsardzības pasākumi, kas piemērojami valsts iestādēm datu piekļuvei un izmantošanai tiesībaizsardzības un citu valsts interešu nolūkos. Lai uzlabotu pārredzamību un atspoguļotu šo saistību tiesisko raksturu, katrs šajā lēmuma uzskaitītais un tam pievienotais dokuments tiks publicēts ASV Federālajā reģistrā.

(66) Komisijas secinājumi par ierobežojumiem attiecībā uz piekļuvi no Eiropas Savienības uz Amerikas Savienotajām Valstīm nosūtītajiem personas datiem un to izmantošanu ASV valsts iestādēs un efektīvu tiesisko aizsardzību ir sīkāk izklāstīti turpmāk.

3.1. *Piekļuve datiem un to izmantošana ASV valsts iestādēs valsts drošības nolūkos*

(67) Komisijas analīze liecina, ka ASV tiesībās ir iekļauti vairāki ierobežojumi ES un ASV privātuma vairoga ietvaros nosūtīto personas datu piekļuvei un izmantošanai valsts drošības nolūkos, kā arī pārraudzības un tiesiskās aizsardzības mehānismi, kas nodrošina pietiekamu aizsardzību, lai šos datus varētu efektīvi pasargāt pret nelikumīgu iejaukšanos un ļaunprātīgas izmantošanas risku ([57]). Kopš 2013. gada, kad Komisija izdeva savus divus paziņojumus (sk. 7. apsvērumu), šis tiesiskais regulējums ir ievērojami stiprināts.

3.1.1. Ierobežojumi

(68) Atbilstīgi ASV Konstitūcijai rūpes par valsts drošību ir prezidenta kompetencē, kurš ir kā virspavēlnieks, galvenā izpildvara un, attiecībā uz ārvalstu izlūkošanu, ASV ārlietu vadītājs ([58]). Lai arī Kongresam ir tiesības piemērot ierobežojumus, un tas ir darīts dažādos aspektos, prezidents šajā kontekstā var pārvaldīt ASV izlūkdienestu darbības, jo īpaši ar izpildrīkojumiem vai prezidenta direktīvām. Tas, protams, attiecas uz tām jomām, kurās nav Kongresa vadības. Šobrīd divi galvenie tiesību akti šajā jomā ir Izpildrīkojums Nr. 12333 ([59]) (*Executive Order, E.O. 12333*) un Prezidenta politikas direktīva Nr. 28 (PPD-28).

([56]) Nacionālās izlūkošanas direktors (NID) darbojas kā izlūkdienestu vadošā struktūrvienība un ir galvenais padomdevējs prezidentam un Nacionālās drošības padomei. Sk. 2004. gada Izlūkošanas reformas un terorisma novēršanas likumu ("Intelligence Reform and Terrorism Prevention Act"), *Pub. L. 108-458, 17.12.2004*. Cita starpā, NIDB nosaka prasības izlūkdienestu veiktiem nacionālās izlūkošanas uzdevumiem, ievākšanai, analīzei, izstrādei un izplatīšanai, kā arī minēto darbību pārvaldībai un norīkošanai, tostarp izstrādājot vadlīnijas par to, kā informācija vai izlūkdati tiek iegūti, izmantoti un koplietoti. Sk. *E.O.* 12333 1.3 (a), (b) sadaļu.

([57]) Sk. *Schrems*, 91. punkts.

([58]) ASV Konstitūcijas II pants. Sk. arī PPD-28 ievadu.

([59]) *E.O.* 12333: Amerikas Savienoto Valstu izlūkošanas darbības, Federālā reģistra 40. sējums, Nr. 235 (1981. gada 8. decembris). Tādā apmērā, kādā izpildrīkojums ir publiski pieejams, tajā ir noteikti ASV izlūkošanas darbību mērķi, virzieni, pienākumi un atbildība (tostarp dažādu izlūkdienestu elementu loma) un izklāstīti vispārīgie parametri izlūkošanas darbību veikšanai (jo īpaši nepieciešamība izsludināt noteiktus procedūras noteikumus). Saskaņā ar *E.O. 12333* 3.2. sadaļu prezidents ar Nacionālās drošības padomes atbalstu un NID izdod atbilstīgas direktīvas, procedūras un vadlīnijas, kas ir nepieciešamas rīkojuma īstenošanai.

(69) Ar 2014. gada 17. janvārī izdoto Prezidenta politikas direktīvu Nr. 28 ("PPD-28") ir noteikti vairāki ierobežojumi "sakaru izlūkošanas" darbībām ([60]). Prezidenta direktīva ir saistoša ASV izlūkošanas iestādēm ([61]) un saglabā spēku līdz ASV valdības maiņai ([62]). PPD-28 ir īpaši svarīga citu valstu personām, tostarp ES datu subjektiem. Cita starpā, ar to nosaka, ka:

a) sakaru izlūkdatu vākšana ir jābalsta uz tiesību aktu vai prezidenta atļauju, un tā jāveic saskaņā ar ASV Konstitūciju (jo īpaši ceturto labojumu) un ASV tiesībām;

b) pret visām personām ir jāizturas ar cieņu un ievērību neatkarīgi no viņu tautības vai dzīvesvietas;

c) visām personām ir likumīgas privātās intereses attiecībā uz viņu personisko informāciju;

d) privātumam un pilsoniskajām brīvībām ir jābūt neatņemamai sastāvdaļai ASV sakaru izlūkošanas darbību plānošanā;

e) tādēļ ASV sakaru izlūkošanas darbībās ir jāiekļauj atbilstīgi aizsardzības pasākumi attiecībā uz visu personu personas datiem neatkarīgi no viņu tautības un dzīvesvietas.

(70) *PPD-28* nosaka, ka sakaru izlūkdatus var vākt tikai valsts un ministriju misiju atbalstam ārvalstu izlūkošanas vai pretizlūkošanas nolūkos un nekādos citos nolūkos (piemēram, lai nodrošinātu konkurences priekšrocību ASV uzņēmumiem). Šajā nolūkā NIDB paskaidro, ka izlūkdienestu elementiem "būtu jānosaka, ka, kad vien iespējams, vākšana būtu jākoncentrē uz specifiskiem ārvalstu izlūkošanas mērķiem vai tematiem, izmantojot diskriminantus (piemēram, specifisku aprīkojumu, atlases nosacījumus un identifikatorus)" ([63]). Turklāt apgalvojumi sniedz pārliecību, ka lēmumi par izlūkdatu vākšanu nav atstāti atsevišķu izlūkošanas aģentu ziņā, bet tiem piemēro politikas virzienus un procedūras, kuras ir jāievieš dažādiem ASV izlūkdienestu elementiem (aģentūrām), lai īstenotu PPD-28 ([64]). Attiecīgi pētniecība un piemērotu izraudzītāju atlase notiek vispārējā "Nacionālās izlūkošanas prioritāšu satvara" (NIPS) ietvaros, kas nodrošina, ka izlūkošanas prioritātes nosaka augsta līmeņa politikas veidotāji un tās tiek regulāri pārskatītas, lai spētu reaģēt uz aktuālajiem draudiem valsts drošībai, un ņemot vērā iespējamos riskus, tostarp privātuma riskus ([65]). Pamatojoties uz to, aģentūras personāls pēta un identificē specifiskus atlases nosacījumus, lai vāktu ārvalstu izlūkdatus atbilstoši prioritātēm ([66]). Izraudzīšanas noteikumi jeb "izraudzītāji" ir regulāri jāpārbauda, lai pārliecinātos, ka tie joprojām sniedz vērtīgus izlūkdatus saskaņā ar prioritātēm ([67]).

([60]) Saskaņā ar *E.O. 12333* Nacionālās drošības aģentūras (NDA) direktors ir sakaru izlūkošanas funkcionālais vadītājs, un viņam jānodrošina vienota sakaru izlūkošanas darbību organizēšana.

([61]) Termina "izlūkdienesti" definīciju skatīt *E.O. 12333* 3.5 (h) sadaļā kopā ar PPD-28 Nr. 1.

([62]) Sk. Tieslietu ministrijas Juridisko konsultāciju biroja 2000. gada 29. janvāra memorandu prezidentam Klintonam. Saskaņā ar šo juridisko atzinumu prezidenta direktīvām ir "tāds pats neatkarīgs juridiskais spēks kā izpildrīkojumam".

([63]) NIDB apgalvojumi (VI pielikums), 3. lpp.

([64]) Sk. PPD-28 4. panta b) un c) apakšpunktu. Saskaņā ar publiski pieejamo informāciju 2015. gada ziņojumā tika apstiprināti seši pastāvoši mērķi. Sk. NIDB, "Sakaru izlūkošanas reforma" (*Signals Intelligence Reform*), 2016. gada progresa ziņojums.

([65]) NIDB apgalvojumi (VI pielikums), 6. lpp. (ar atsauci uz izlūkdienestu (ID) direktīvu Nr. 204). Sk. arī PPD-28 3. panta b) un c) apakšpunktu.

([66]) NIDB apgalvojumi (VI pielikums), 6. lpp. Sk., piemēram, NDA Pilsonisko brīvību un privātuma birojs (NDA PBPB), NDA Pilsonisko brīvību un privātuma aizsardzība mērķtiecīgām sakaru izlūkošanas darbībām saskaņā ar *E.O. 12333*, 2014. gada 7. oktobris. Skatīt arī ODNI 2014. gada situācijas ziņojumu. Piekļuves pieprasījumiem saskaņā ar ĀIUL 702. sadaļu jautājumi tiek pārvaldīti ar ĀIUT apstiprinātām minimizācijas procedūrām. Sk. NDA PBPB, Ārvalstu izlūkošanas uzraudzības likuma (*Foreign Intelligence Surveillance Act*) 702. panta īstenošana, ko veic NDA, 2014. gada 16. aprīlis.

([67]) Sk. 2015. gada jubilejas ziņojumu "Sakaru izlūkošanas reforma" (*Signals Intelligence Reform*). Sk. arī NIDB apgalvojumus (VI pielikums), 6., 8.–9., 11. lpp.

(71) Turklāt PPD-28 noteiktās prasības, ka izlūkdatu vākšanai vienmēr ([68]) jābūt "cik vien iespējams pielāgotai", un ka izlūkdienestiem par prioritāru jāpieņem citas informācijas pieejamība un piemērotas un iespējamas alternatīvas ([69]), atspoguļo vispārēju noteikumu par prioritāti izvirzīt datu mērķtiecīgu, nevis lielapjoma vākšanu. Saskaņā ar NIDB pausto apliecinājumu tie nodrošina jo īpaši to, ka datu lielapjoma vākšana nenozīmē nedz "masveidā", nedz "nekritiski", un ka izņēmums neaizēno noteikumu ([70]).

(72) Lai arī PPD-28 paskaidrots, ka izlūkdienestu elementiem dažkārt konkrētos apstākļos ir lielapjomā jāvāc sakaru izlūkdati, piemēram, lai identificētu un izvērtētu jaunus vai radušos draudus, direktīva norāda šiem elementiem, ka ir jānosaka prioritāras alternatīvas, kas ļautu veikt mērķtiecīgu sakaru izlūkošanu ([71]). No tā izriet, ka datiu lielapjoma vākšana notiks tikai tad, kad "tehnisku vai ar ekspluatāciju saistītu apsvērumu dēļ" nav iespējama mērķtiecīgu vākšana, izmantojot diskriminantus – proti, identifikatorus, kas saistīti ar konkrētu mērķi (piemēram, mērķa e-pasta adrese vai tālruņa numurs) ([72]). Tas attiecas gan uz veidu, kādā sakaru izlūkdati tiek vākti, gan uz to, kas faktiski tiek vākts ([72]).

(73) Saskaņā ar NIDB apgalvojumiem pat gadījumos, kad izlūkdienesti nevar izmantot konkrētus identifikatorus mērķtiecīgai vākšanai mērķa, tā centīsies "cik vien iespējams" sašaurināt vākšanu. Lai to nodrošinātu, tā "piemēro filtrus vai citus tehniskus rīkus, lai koncentrētu vākšanu uz tām iekārtām, kurās varētu būt saziņa ar ārvalstu izlūkošanas vērtība" (un tādējādi būtu reaģēts uz prasībām, ko formulējuši ASV politikas veidotāji saskaņā ar iepriekš 70. apsvērumā aprakstīto procedūru). Tādējādi pret datu lielapjoma vākšanu vērstos vismaz divos veidos: pirmkārt, tā vienmēr attiektos uz konkrētiem ārvalstu izlūkošanas mērķiem (piemēram, lai iegūtu sakaru izlūkdatus par kādas teroristu grupas darbībām, kas darbojas konkrētā reģionā) un koncentrētu vākšanu uz paziņojumiem, kuros ir šāda saikne. Saskaņā ar NIDB pausto apliecinājumu tas atspoguļojas apstāklī, ka "Amerikas Savienoto Valstu sakaru izlūkošanas darbības skar tikai daļu no paziņojumiem, kas atrodami internetā. ([73])" Otrkārt, NIDB apgalvojumos paskaidrots, ka izmantotie filtri un citi tehniskie rīki tiks izstrādāti tā, lai koncentrētu vākšanu "maksimāli precīzi", lai nodrošinātu, ka tiek samazināts savāktās "nederīgās informācijas" apjoms.

(74) Visbeidzot, pat ja ASV uzskata, ka sakaru izlūkdatus ir nepieciešams lielapjoma vākt saskaņā ar 70.–73. apsvērumā izklāstītajiem nosacījumiem, PPD-28 ierobežo šādas informācijas izmantošanu līdz sešiem valsts drošības mērķiem ar nolūku aizsargāt visu personu privātumu un pilsoniskās brīvības neatkarīgi no viņu tautības un dzīvesvietas ([74]). Šie pieļaujamie mērķi aptver pasākumus, ar kuriem apzināt un apkarot draudus

([68]) Sk. 63. zemsvītras piezīmi.

([69]) Būtu jāatzīmē arī tas, ka saskaņā ar *E.O. 12333* 2.4. sadaļu IK elementos "ir jāizmanto visneuzbāzīgākās vākšanas metodes, kādas iespējamas Amerikas Savienotajās Valstīs". Attiecībā uz ierobežojumiem visu datu lielapjoma vākšanas aizstāšanai ar mērķtiecīgu vākšanu, skatīt Nacionālās Pētniecības padomes izvērtējuma rezultātus, ko paziņojusi Eiropas Savienības Pamattiesību aģentūra – Izlūkošanas dienestu uzraudzība: pamattiesības, aizsardzības pasākumi un tiesiskās aizsardzības līdzekļi ES (2015), 18. lpp.

([70]) NIDB apgalvojumi (VI pielikums), 4. lpp.

([71]) Sk. arī PPD-28 5.(d) sadaļu, kurā noteikts, ka nacionālās izlūkošanas direktoram sadarbībā ar attiecīgo izlūkdienestu elementu vadītājiem un Zinātnes un tehnoloģijas politikas biroju ir jāsniedz prezidentam "ziņojums, kurā izvērtēta tādas programmatūras izveides iespējamība, kas ļautu izlūkdienestiem vieglāk veikt mērķtiecīgu informācijas iegūšanu, nevis datu lielapjoma vākšanu". Saskaņā ar publiski pieejamo informāciju šā ziņojuma secinājums bija tāds, ka "nav uz programmatūru balstītas alternatīvas, kas pilnībā aizstās datu lielapjoma vākšanu dažu draudu valsts drošībai atklāšanai". Sk. 2015. gada jubilejas ziņojumu "Sakaru izlūkošanas reforma" (*Signals Intelligence Reform*).

([72]) Sk. 63. zemsvītras piezīmi.

([73]) NIDB apgalvojumi (VI pielikums). Tas jo īpaši attiecas uz bažām, ko izteikušas valsts datu aizsardzības iestādes savā atzinumā par atbilstību lēmuma projektu. Sk. 29. panta Datu aizsardzības darba grupas Atzinumu 01/2016 par ES un ASV privātuma vairoga atbilstību lēmuma projektu (pieņemts 2016. gada 13. aprīlī), 38. lpp. ar Nr. 47.

([74]) Sk. PPD-28 2. pantu.

bruņotajiem spēkiem vai militārajam personālam, ko veicina spiegošana, terorisms, masu iznīcināšanas ieroči, draudus kiberdrošībai, kā arī transnacionālus kriminālos draudus, kas saistīti ar pārējiem pieciem mērķiem, un tie tiks pārskatīti vismaz reizi gadā. Saskaņā ar ASV valdības apgalvojumiem izlūkdienestu elementi ir stiprinājuši savu analītisko praksi un standartus nenovērtētu sakaru izlūkdatu vērtēšanai, lai ievērotu šīs prasības; mērķtiecīgas meklēšanas izmantošana "nodrošina, ka analītiķiem izpētei tiek uzrādīta tikai tā informācija, kurai ir potenciāla izlūkošanas vērtība" ([75]).

(75) Šie ierobežojumi īpaši attiecas uz personas datiem, kas tiek nosūtīti ES un ASV privātuma vairoga ietvaros, īpaši gadījumā, ja personas datus vāc ārpus Amerikas Savienotajām Valstīm, tostarp to pārsūtīšanas laikā pa transatlantiskajiem kabeļiem no Savienības uz Amerikas Savienotajām Valstīm. Kā ASV iestādes apstiprinājušas NIDB apgalvojumos, tajos izklāstītie ierobežojumi un aizsardzības pasākumi – tostarp PPD-28 – attiecas uz šādu vākšanu ([76]).

(76) Lai arī tas nav noformulēts šajos juridiskajos noteikumos, šie principi iemieso nepieciešamības un proporcionalitātes principu būtību. Mērķtiecīga ievākšana ir skaidra prioritāte, savukārt apjomīga ievākšana aprobežojas ar (izņēmuma) situācijām, kurās mērķtiecīga ievākšana nav iespējama tehnisku vai operatīvu iemeslu dēļ. Pat tad, ja no *datu lielapjoma vākšanas* nav iespējams izvairīties, tālāka šādu datu "izmantošana", tiem piekļūstot, ir *strikti ierobežota* konkrētiem, likumīgiem valsts drošības mērķiem ([77]).

(77) Tā kā prasības ir iekļautas direktīvā, ko izdevis prezidents kā galvenā izpildvara, tās ir saistošas visiem izlūkdienestiem un ir tālāk īstenotas ar aģentūru noteikumiem un procedūrām, ar kurām vispārējos principus transponē konkrētos virzienos ikdienas darbībām. Turklāt, lai arī Kongresam pašam PPD-28 nav saistoša, tas arī ir veicis darbības, lai nodrošinātu, ka personas datu ievākšana un piekļuve tiem Amerikas Savienotajās Valstīs ir mērķtiecīga, nevis tiek veikta "vispārīgi".

(78) No pieejamās informācijas, tostarp no ASV valdības saņemtajiem apgalvojumiem, izriet, ka, kad dati tiek nosūtīti organizācijai, kas atrodas ASV un ir pašsertificējusies ES un ASV privātuma vairoga ietvaros, ASV izlūkošanas aģentūras drīkst pieprasīt personas datus tikai tad ([78]), ja pieprasījums atbilst Ārvalstu izlūkošanas uzraudzības likumam (ĀIUL) vai to ir iesniedzis Federālais izmeklēšanas birojs (FIB), pamatojoties uz tā dēvēto nacionālās drošības vēstuli (NDV) ([79]). Saskaņā ar ĀIUL pastāv vairāki juridiskie pamati, kurus var izmantot, lai vāktu (un pēc tam apstrādātu) ES datu subjektu personas datus, kuri tiek pārsūtīti ES un ASV privātuma vairoga ietvaros.

([75]) NIDB apgalvojumi (VI pielikums), 4. lpp. Skatīt arī izlūkdienestu direktīvu 203.

([76]) NIDB apgalvojumi (VI pielikums), 2. lpp. Līdzīgi *E.O. 12333* noteiktie ierobežojumi (piemēram, nepieciešamība pēc ievāktas informācijas, lai reaģētu uz prezidenta noteiktajām izlūkošanas prioritātēm).

([77]) Sk. *Schrems*, 93. punkts.

([78]) Papildus FIB datu ievākšanu var balstīt uz tiesībaizsardzības atļauju (sk. šā lēmuma 3.2. punktu).

([79]) Tālākiem skaidrojumiem par NDV izmantošanu sk. NIDB apgalvojumus (VI pielikums), 13.–14. lpp., Nr. 38. Saskaņā ar tajos norādīto FIB var izmantot NDV tikai ar saturu nesaistītas informācijas pieprasīšanai attiecībā uz atļautu valsts drošības izmeklēšanu, lai aizsargātu no starptautiskā terorisma vai slepenām izlūkošanas darbībām. Attiecībā uz datu nosūtīšanu ES un ASV privātuma vairoga ietvaros vispiemērotākā likumīgā atļauja šķiet Elektroniskās saziņas privātuma likums (*Electronic Communications Privacy Act*) (*18 U.S.C. § 2709*), kurā noteikts, ka jebkādā abonenta informācijas vai darījumu uzskaites pieprasījumā ir jāizmanto "nosacījums, kas īpaši identificē personu, uzņēmumu, tālruņa numuru vai kontu".

Papildus tradicionālajai individualizētajai elektroniskajai uzraudzībai saskaņā ar ĀIUL 104. pantu ([80]) un zvanīto numuru reģistrētāju un uztveršanas un trasēšanas ierīču uzstādīšanai saskaņā ar ĀIUL 402. pantu ([81]) divi galvenie instrumenti ir ĀIUL 501. pants (*USA Patriot Act* bij. 215. pants) un ĀIUL 702. pants ([82]).

(79) Šajā ziņā ar ASV Brīvības likumu (*USA FREEDOM Act*), kas stājās spēkā 2015. gada 2. jūnijā, ir aizliegta apjomīga dokumentācijas ievākšana, pamatojoties uz ĀIUL 402. pantu (tiesības izmantot zvanīto numuru reģistrētāju un uztveršanas un trasēšanas ierīces) un ĀIUL 501. pantu (*USA Patriot Act* bij. 215. pants) ([83]) un izmantojot NDV, un tās vietā ir noteikta specifisku "atlases nosacījumu" izmantošana ([84]).

(80) Lai arī ĀIUL ietver citas likumīgas atļaujas veikt nacionālās izlūkošanas darbības, tostarp sakaru izlūkošanu, Komisijas novērtējums ir apliecinājis, ka attiecībā uz personas datiem, kas pārsūtāmi ES un ASV privātuma vairoga ietvaros, šīs atļaujas vienlīdz ierobežo publisko iestāžu iejaukšanos līdz mērķtiecīgai ievākšanai un piekļuvei.

(81) Tas ir skaidrs attiecībā uz individualizētu elektronisko uzraudzību saskaņā ar ĀIUL 104. pantu ([85]). Attiecībā uz ĀIUL 702. pantu, kas nodrošina pamatu divām svarīgām izlūkošanas programmām, kuras vada ASV izlūkošanas aģentūras (*PRISM, UPSTREAM*), meklēšana tiek veikta mērķtiecīgā veidā, izmantojot individuālus izraudzītājus, kuri identificē konkrētus sakaru līdzekļus, piemēram, e-pasta adresi vai tālruņa numuru, nevis atslēgvārdus vai pat interesējošo personu vārdus ([86]). Tādēļ, kā atzīmējusi Privātuma un pilsonisko brīvību pārraudzības padome

([80]) *50 U.S.C. § 1804*. Lai arī šai likumīgajai pilnvarai ir nepieciešams "faktu un apstākļu izklāsts, uz ko balstās pieteicējs, lai pamatotu savu uzskatu, ka A) elektroniskās uzraudzības mērķis ir ārvalstu vara vai ārvalstu varas pārstāvis", pēdējais var būt citu valstu personas, kuras iesaistās starptautiskajā terorismā vai starptautiskajā masu iznīcināšanas ieroču izplatīšanā (tostarp sagatavošanās darbībās) (*50 U.S.C. § 1801 (b)(1)*). Tomēr saikne ar personas datiem, kuri tiek pārsūtīti ES un ASV privātuma vairoga ietvaros, ir tikai teorētiska, ņemot vērā, ka faktu izklāstā ir jāpamato arī uzskats, ka "visas telpas un vietas, pret ko ir vērsta elektroniskā uzraudzība, izmanto vai plāno izmantot ārvalstu vara vai ārvalstu varas pārstāvis". Jebkurā gadījumā šādas pilnvaras izmantošanai ir nepieciešams pieteikums ĀIUT, kurā novērtēts, cita starpā, vai, pamatojoties uz iesniegtajiem faktiem, ir ticams iemesls, ka šis tiešām ir tas gadījums.

([81]) *50 U.S.C. § 1842* ar *§ 1841(2), Sec. 3127 of Title 18*. Šī pilnvara nav saistīta ar paziņojumu saturu, bet drīzāk ir ar mērķi informēt par klientu vai abonentu, kas izmanto pakalpojumu (piemēram, vārds, adrese, abonenta numurs, saņemtā pakalpojuma ilgums/veids, maksājuma avots/līdzeklis). Tam nepieciešams pieteikums ĀIUT (vai ASV izmeklēšanas tiesneša (*magistrate judge*)) rīkojumam un specifiska atlases nosacījuma izmantošana 1841. panta 4. punkta izpratnē, t. i., nosacījums, kas konkrēti identificē personu, kontu utt. un tiek izmantots, lai maksimāli ierobežotu pieprasītās informācijas apmēru.

([82]) Lai arī ĀIUL 501. pantu (*USA Patriot Act* bij. 215. pants) FIB ir ļauts pieprasīt tiesas rīkojumu attiecībā uz "taustāmu lietu" (jo īpaši tālruņa metadatu, bet arī uzņēmējdarbības dokumentācijas) uzrādīšanu ārvalstu izlūkošanas nolūkos, ĀIUL 702. pants ļauj ASV izlūkdienestu elementiem pieprasīt piekļuvi informācijai, tostarp interneta sakaru saturam, no Amerikas Savienotajām Valstīm, attiecībā uz noteiktām citu valstu personām, kuras atrodas ārpus Amerikas Savienotajām Valstīm.

([83]) Pamatojoties uz šo nosacījumu, FIB var pieprasīt "taustāmas lietas" (piemēram, reģistrus, papīrus, dokumentus), pamatojoties uz liecībām Ārvalstu izlūkošanas uzraudzības tiesai (ĀIUT) par to, ka ir pamats uzskatīt, ka tie ir būtiski attiecīgajai FIB izmeklēšanai. Veicot meklēšanu, FIB ir jāizmanto ĀIUT apstiprināti atlases nosacījumi, attiecībā uz kuriem ir "pamatotas, skaidri formulētas aizdomas" par to, ka šāds nosacījums ir saistīts ar vienu vai vairākām ārvalstu varām vai to pārstāvjiem, kas iesaistījušies starptautiskajā terorismā vai tā sagatavošanās darbībās. Sk. PPBPP ziņojuma 215. sadaļu, 59. lpp.; NDA PBPB pārredzamības ziņojums: *The USA Freedom Act Business Records FISA Implementation*, 2016. gada 15. janvāris, 4.–6. lpp.

([84]) NIDB apgalvojumi (VI pielikums), 13. lpp. (Nr. 38).

([85]) Sk. 81. zemsvītras piezīmi.

([86]) PPBPP, 702. panta ziņojums, 32.–33. lpp. ar turpmākām atsaucēm. NDA saskaņā ar tās privātuma biroju ir jāapstiprina, ka starp mērķi un izraudzītāju ir saikne, jādokumentē ārvalstu izlūkošanas informācija, kuru paredzēts iegūt, šī informācija ir jāpārbauda un jāapstiprina diviem NDA vecākajiem analītiķiem, un vispārējā procesā tiks sekots turpmākām atbilstības pārbaudēm, ko veiks NIDB un Tieslietu ministrija. Sk. NDA PBPB, Ārvalstu izlūkošanas likuma 702. panta īstenošana, ko veic NDA, 2014. gada 16. aprīlis.

(PPBPP), 702. panta uzraudzība "pilnībā sastāv no mērķtiecīgām darbībām pret konkrētām [citu valstu] personām, par kurām ir veikta individuāla analīze" ([87]). Turpināmības klauzulas dēļ ĀIUL 702. pants 2017. gadā būs jāpārskata, un tajā laikā Komisijai būs atkārtoti jāizvērtē ES datu subjektiem pieejamie aizsardzības pasākumi.

(82) Turklāt ASV valdība savos apgalvojumos ir nepārprotami apliecinājusi Eiropas Komisijai, ka ASV izlūkdienesti "neiesaistās neviena cilvēka, tostarp parastu Eiropas pilsoņu, nekritiskā uzraudzībā" ([88]). Attiecībā uz personas datiem, kas tiek vākti Amerikas Savienotajās Valstīs, šo apgalvojumu apstiprina empīriski pierādījumi, kas apliecina, ka *piekļuves pieprasījumi* caur NDV un saskaņā ar ĀIUL gan atsevišķi, gan kopā attiecas tikai uz relatīvi nelielu skaitu mērķēto personu salīdzinājumā ar vispārējo datu plūsmu internetā ([89]).

(83) Attiecībā uz piekļuvi ievāktajiem datiem un *datu drošību* PPD-28 nosaka, ka piekļuve "ir pieejama tikai pilnvarotiem darbiniekiem, kuriem jāzina informācija, lai veiktu savu uzdevumu," un ka personiskā informācija "tiek apstrādāta un uzglabāta apstākļos, kuros tiek nodrošināta pienācīga aizsardzība un liegta piekļuve nepiederošām personām atbilstoši sensitīvai informācijai piemērojamajiem drošības pasākumiem". Izlūkošanas personāls saņem atbilstošu un pienācīgu apmācību attiecībā uz PPD-28 izklāstītajiem principiem ([90]).

(84) Visbeidzot, attiecībā uz to personisko datu *glabāšanu* un tālāku *izplatīšanu*, kuri iegūti no ES datu subjektiem un kurus vāc ASV izlūkošanas iestādes, PPD-28 nosaka, ka pret visām personām (tostarp citu valstu personām) ir jāizturas ar cieņu un ievērību, ka visām personām ir likumīgas privātās intereses attiecībā uz apiešanos ar viņu personas datiem un ka tādējādi izlūkdienestu elementiem ir jāizveido politikas virzieni, ar kuriem tiek nodrošināti pienācīgi šādu datu aizsardzības pasākumi, kas ir "saprātīgi izstrādāti, lai samazinātu (to) izplatīšanu un saglabāšanu ([91])."

([87]) PPBPP ziņojuma 702. sadaļa, 111. lpp. Skat arī NIDB apgalvojumus (VI pielikums), 9. lpp. ("vākšana saskaņā ar [ĀIUL] 702. pantu nav "masveida un nekritiska", bet tā ir šauri koncentrēta uz ārvalstu izlūkdatu vākšanu no individuāli identificētiem likumīgiem mērķiem") un 13. lpp., Nr. 36 (ar atsauci uz 2014. gada ĀIUT atzinumu); NDA PBPB, Ārvalstu izlūkošanas likuma 702. panta īstenošana, ko veic NDA, 2014. gada 16. aprīlis. Pat *UPSTREAM* gadījumā NDA var pieprasīt tikai elektronisko sakaru pārtveršanu norīkotiem izraudzītājiem, no tiem vai par tiem.

([88]) NIDB apgalvojumi (VI pielikums), 18. lpp. Sk. arī 6. lpp., saskaņā ar kuru piemērojamās procedūras "apliecina nepārprotamu apņemšanos novērst patvaļīgu un nekritisku sakaru izlūkdatu vākšanu un īstenot – valdības augstākajos līmeņos – saprātīguma principu".

([89]) Sk. Statistisko pārredzamības ziņojumu par nacionālās drošības iestāžu izmantošanu (*Statistical Transparency Report Regarding Use of National Security Authorities*), 2015. gada 22. aprīlis. Attiecībā uz vispārējo datu plūsmu internetā sk., piemēram, Pamattiesību aģentūras ziņojuma *Surveillance by Intelligence Services*: pamattiesības, aizsardzības pasākumi un tiesiskās aizsardzības līdzekļi ES (2015), 15.–16. lpp. Attiecībā uz *UPSTREAM* programmu saskaņā ar deklasificēto 2011. gada ĀIUT atzinumu vairāk nekā 90 % elektronisko sakaru, kas saņemti atbilstīgi ĀIUL 702. pantam, ir iegūti no *PRISM* programmas, bet mazāk nekā 10 % no *UPSTREAM*. Sk. ĀIUT, Memoranda atzinums, 2011 WL 10945618 (ĀIUL tiesa, 3.10.2011.), Nr. 21 (pieejams: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Sk. PPD-28 4.(a)(ii) sadaļu. Skat arī NIDB, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28* (Situācijas pārskats par procedūru izstrādi un īstenošanu saskaņā ar Prezidenta politikas direktīvu 28), 2014. gada jūlijs, 5. lpp., saskaņā ar kuru "izlūkdienestu elementu politikas virzieniem būtu jāstiprina esošā analītiskā prakse un standarti, tādējādi analītiķiem ir jāizmanto strukturāla meklēšana vai citi meklēšanas nosacījumi un tehnikas, ar kurām identificēt izlūkošanas informāciju, kas attiecas uz likumīgu izlūkošanas vai tiesībaizsardzības uzdevumu, meklējumi par personām jākoncentrē uz izlūkošanas informācijas kategorijām, kuras atbilst izlūkošanas vai tiesībaizsardzības prasībai, un jāsamazina personiskās informācijas pārskatīšana, kas neatbilst izlūkošanas vai tiesībaizsardzības prasībām". Sk., piemēram, CIP, "Sakaru izlūkošanas darbības" (*Signals Intelligence Activities*), 5. lpp.; FIB, *Presidential Policy Directive 28 Policies and Procedures*, 3. punkts. Saskaņā ar 2016. gada progresa ziņojumu par sakaru izlūkošanas reformu IK elementi (tostarp FIB, CIP un NDA) ir veikuši pasākumus, lai informētu savus darbiniekus par PPD-28 prasībām, izstrādājot jaunus vai grozot esošos apmācību politikas virzienus.

([91]) Saskaņā ar NIDB apgalvojumiem šos ierobežojumus piemēro neatkarīgi no tā, vai notikusi informācijas lielapjoma vai mērķtiecīga vākšana, un neatkarīgi no personas pilsonības.

(85) ASV valdība ir paskaidrojusi, ka šī saprātīguma prasība nozīmē, ka izlūkdienestu elementiem nebūs jāpieņem "neviens teorētiski iespējams pasākums", bet būs "jālīdzsvaro savi centieni aizsargāt likumīgas privātuma un pilsoniskās brīvības intereses ar sakaru izlūkošanas darbību praktiskajām vajadzībām" ([92]). Šajā ziņā pret citu valstu personām izturēsies tāpat kā pret ASV piederīgām personām, pamatojoties uz procedūrām, kuras apstiprinājis ģenerālprokurors. ([93])

(86) Saskaņā ar šiem noteikumiem glabāšanas termiņš parasti ir ierobežots līdz pieciem gadiem, ja vien likumā nav īpašs noteikums vai nacionālās izlūkošanas direktors pēc rūpīgas privātuma jautājumu novērtēšanas – ņemot vērā NIDB pilsonisko brīvību un privātuma inspektora, kā arī aģentūru privātuma un pilsonisko brīvību inspektoru viedokļus – nenosaka, ka turpmāka glabāšana ir valsts drošības interesēs. ([94]) Izplatīšana ir ierobežota līdz gadījumiem, kuros informācija ir būtiska vākšanas pamatmērķim un tādējādi atbilst sankcionētai ārvalstu izlūkošanas vai tiesībaizsardzības prasībai. ([95])

(87) Saskaņā ar ASV valdības apgalvojumiem personas datus nedrīkst izplatīt tikai tāpēc, ka attiecīgā persona nav ASV piederīga persona, un "sakaru izlūkošana attiecībā uz ārvalstu personas ikdienas darbībām nebūtu izskatāma par ārvalstu izlūkdatiem, kurus var pastāvīgi izplatīt vai saglabāt tikai šā fakta dēļ, ja vien pretējā gadījumā tas neatbilst sankcionētai ārvalstu izlūkošanas prasībai" ([96]).

(88) Pamatojoties uz iepriekš minēto, Komisija secina, ka Amerikas Savienotajās Valstīs ir noteikumi, kas paredzēti, lai ierobežotu iejaukšanos valsts drošības nolūkos to personu pamattiesībās, kuru personas dati tiek nosūtīti no Savienības uz Amerikas Savienotajām Valstīm ES un ASV privātuma vairoga ietvaros, līdz tādam līmenim, kas ir absolūti nepieciešams, lai sasniegtu attiecīgo likumīgo mērķi.

(89) Kā liecina minētā analīze liecina, ASV tiesību akti nodrošina, ka uzraudzības pasākumi tiks izmantoti vienīgi ārvalstu izlūkdatu iegūšanai – kas ir likumīgs politikas mērķis ([97]) – un tie būs pēc iespējas mērķtiecīgi. Jo īpaši,

([92]) Sk. NIDB apgalvojumus (VI pielikums).

([93]) Sk. PPD-28 4(a)(i) sadaļu kopā ar *E.O.* 12333 2.3. sadaļu.

([94]) PPD-28 4.(a)(i) sadaļa; NIDB apgalvojumi (VI pielikums), 7. lpp. Piemēram, attiecībā uz personisko informāciju, kas ievākta saskaņā ar ĀIUL 702. pantu, NDA minimizācijas procedūrās, kuras apstiprinājusi ĀIUT, ir paredzēts, ka metadati un nenovērtētais saturs PRISM tiek saglabāts ne ilgāk kā piecus gadus, savukārt *UPSTREAM* dati tiek glabāti ne ilgāk kā divus gadus. NDA ievēro šos uzglabāšanas ierobežojumus, izmantojot automatizētu procesu, kurā attiecīgā uzglabāšanas termiņa beigās ievāktie dati tiek izdzēsti. Sk. NDA ĀIUL 702. panta minimizācijas procedūras, 7. sadaļa kopā ar 6.(a)(1). sadaļu; NDA PBPB, Ārvalstu izlūkošanas uzraudzības likuma 702. panta īstenošana, ko veic NDA, 2014. gada 16. aprīlis. Tāpat saglabāšanas termiņš saskaņā ar ĀIUL 501. pantu (*USA Patriot Act* bij. 215. pants) ir ierobežots līdz pieciem gadiem, ja vien personas dati nav daļa no atbilstīgi apstiprinātas ārvalstu izlūkošanas informācijas izplatīšanas vai ja Tieslietu ministrija rakstveidā nenorāda NDA, ka ierakstiem ir piemērots saglabāšanas nosacījums nepabeigtā vai gaidāmā tiesvedībā. Skat arī NDA PBPB pārredzamības ziņojumu: NDA PBPB pārskatāmības ziņojums "The USA Freedom Act Business Records FISA Implementation", 2016. gada 15. janvāris.

([95]) Konkrēti, ĀIUL 501. panta (*USA Patriot Act* bij. 215. pants) gadījumā personisku informāciju drīkst izplatīt tikai pretterorisma nolūkos vai kā nozieguma pierādījumu, bet ĀIUL 702. panta gadījumā tikai tad, ja ir likumīgs ārvalstu izlūkošanas vai tiesībaizsardzības mērķis. Sk. NDA PBPB, Ārvalstu izlūkošanas uzraudzības likuma 702. panta īstenošana, ko veic NDA, 2014. gada 16. aprīlis; Pārredzamības ziņojums: *The USA Freedom Act Business Records FISA Implementation*, 2016. gada 15. janvāris. Sk. arī NDA Pilsonisko brīvību un privātuma aizsardzība mērķtiecīgām sakaru izlūkošanas darbībām saskaņā ar izpildrīkojumu Nr. 12333, 2014. gada 7. oktobris.

([96]) NIDB apgalvojumi (VI pielikums), 7. lpp. (attiecībā uz izlūkdienestu direktīvu (IDD) Nr. 203).

([97]) Tiesa ir izskaidrojusi, ka valsts drošība ir likumīgs politikas mērķis. Sk. *Schrems*, 88. punkts. Skatīt arī lietu *Digital Rights Ireland and Others*, 42.–44. un 51. punktu, kurā Tiesa atzina, ka cīņa pret smagiem noziegumiem, jo īpaši organizēto noziedzību un terorismu, var lielā mērā būt atkarīga no moderno izmeklēšanas tehniku izmantošanas. Turklāt atšķirībā no kriminālizmeklēšanas, kas parasti attiecas uz retrospektīvu atbildību un vainas noteikšanu par jau veiktām notikušām, izlūkošanas darbības bieži ir koncentrētas uz draudu valsts drošībai novēršanu vēl pirms ir nodarīts kaitējums. Tādēļ šādā izmeklēšanā bieži var nākties aptvert plašāks iespējamo dalībnieku ("mērķu") loks un plašāku ģeogrāfisko apgabalu. Sk. ECT spriedumu lietā *Weber and Saravia v. Germany*, 2006. gada 29. jūnijs, pieteikums Nr. 54934/00, 105.–118. punkts (par tā saukto "stratēģisko uzraudzību").

datu vākšana vākšana tiks atļauta tikai izņēmuma kārtā gadījumos, kad nav iespējama mērķtiecīga vākšana, un to papildinās ar papildu drošības pasākumiem, lai samazinātu ievākto datu apjomu un turpmāko piekļuvi tiem (kurai jābūt mērķtiecīgai un atļautai tikai konkrētos nolūkos).

(90) Komisijas izvērtējumā tas saskan ar Tiesas noteikto standartu *Schrems* spriedumā, saskaņā ar kuru tiesiskajā regulējumā, kurā ir ietverta iejaukšanās Pamattiesību hartas 7. un 8. pantā garantētajās pamattiesībās, ir jānosaka "minimālās prasības" ([98]) un ka "līdz absolūti nepieciešamajam nav ierobežots tiesiskais regulējums, saskaņā ar kuru vispārīgi tiek pieļauta visu to personu personas datu saglabāšana, kuru dati no Savienības ir pārsūtīti uz ASV – nešķirojot, bez ierobežojumiem vai izņēmumiem saistībā ar mērķi, kam tie kalpo, vai neparedzot objektīvus kritērijus, kas valsts iestāžu piekļuvi datiem un to vēlāku izmantošanu ļauj ierobežot precīziem, strikti ierobežotiem un tādiem mērķiem, kas pamato gan piekļuvi šiem datiem, gan arī to izmantošanu." ([99]) Tāpat nenotiks neierobežota visu personu datu vākšana un glabāšana un netiks pieļauta neierobežota piekļuve. Turklāt Komisijai sniegtie apliecinājumi, tostarp apliecinājums, ka ASV sakaru izlūkošanas darbības skar tikai daļu no paziņojumiem, kas atrodami internetā, izslēdz iespēju, ka varētu būt "vispārēja" piekļuve elektronisko sakaru saturam ([100]).

3.1.2. Efektīva tiesiskā aizsardzība

(91) Komisija ir izvērtējusi gan Amerikas Savienotajās Valstīs pastāvošos pārraudzības mehānismus attiecībā uz ASV izlūkošanas iestāžu iejaukšanos personas datos, kas tiek pārsūtīti uz Amerikas Savienotajām Valstīm, gan ES datu subjektiem pieejamās iespējas pieprasīt individuālu tiesisko aizsardzību.

Pārraudzība

(92) Uz ASV izlūkdienestiem attiecas dažādi pārbaudes un pārraudzības mehānismi, kas ietilpst valsts varas trīs pīlaros. Tie ietver iekšējās un ārējās izpildvaras struktūras, vairākas Kongresa komitejas, kā arī tiesas uzraudzību – jo īpaši pār darbībām, uz kurām attiecas Ārvalstu izlūkošanas uzraudzības likums.

(93) Pirmkārt, ASV iestāžu izlūkošanas darbības rūpīgi pārrauga izpildvara.

(94) Saskaņā ar PPD-28 4. panta a) apakšpunkta iv) punktu izlūkdienestu elementu politikas virzieni un procedūras "ietver pienācīgus pasākumus, ar kuriem sekmēt personiskās informācijas aizsardzības mehānismu īstenošanas pārraudzību"; šajos pasākumos būtu jāiekļauj periodiskas revīzijas ([101]).

([98]) *Schrems*, 91. punkts, ar turpmākām atsaucēm.
([99]) *Schrems*, 93. punkts.
([100]) Sal. *Schrems*, 94. punkts.
([101]) NIDB, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, 7. lpp. Sk., piemēram, CIP, *Signals Intelligence Activities*, 6. p. ("Atbilstība"); FIB, *Presidential Policy Directive 28 Policies and Procedures*, III nodaļas A daļas 4. punkts, B daļas 4. punkts; NDA, PPD-28 4. panta procedūras, 2015. gada 12. janvāris, 8.1. punkts, 8.6. punkta c) apakšpunkts.

(95) Šajā ziņā ir ieviesti vairāki pārraudzības slāņi, tostarp pilsonisko brīvību vai privātuma inspektori, ģenerālinspektori, NIDB Pilsonisko brīvību un privātuma birojs, PPBPP un Prezidenta izlūkošanas pārraudzības padome. Šīs pārraudzības funkcijas nodrošina atbilstības darbinieki visās aģentūrās ([102]).

(96) Kā skaidro ASV valdība ([103]), *pilsonisko brīvību vai privātuma inspektori* ar pārraudzības pienākumiem ir vairākās ministrijās ar izlūkošanas funkcijām un izlūkošanas aģentūrās ([104]). Lai arī šo inspektoru konkrētās pilnvaras zināmā mērā var atšķirties atkarībā no pilnvarojošā tiesību akta, parasti tās ietver tādu procedūru uzraudzību, ar kurām nodrošināt, ka attiecīgā ministrija/aģentūra adekvāti izskata privātuma un pilsonisko brīvību jautājumus un ir ieviesusi atbilstošas procedūras, ar kurām risināt sūdzības no personām, kas uzskata, ka viņu privātums un pilsoniskās brīvības ir aizskartas (un atsevišķos gadījumos, piemēram, NIDB, pašiem ir tiesības izskatīt sūdzības ([105])). Savukārt ministrijas/aģentūras vadītājam ir jānodrošina, ka inspektors saņem visu informāciju un tam ir piekļuve visiem materiāliem, kas nepieciešami, lai pildītu savas funkcijas. Pilsonisko brīvību un privātuma inspektori periodiski atskaitās Kongresam un PPBPP, tostarp norādot ministrijas/aģentūras saņemto sūdzību skaitu un veidu un sniedzot kopsavilkumu par šādu sūdzību izvietojumu, veiktajiem ziņojumiem un izmeklēšanām un inspektora veikto darbību ietekmi ([106]). Saskaņā ar valsts datu aizsardzības iestāžu novērtējumu iekšējo pārraudzību, ko veic pilsonisko brīvību vai privātuma inspektori, var uzskatīt par "vidēji spēcīgu", lai gan pēc iestāžu domām inspektoriam nav nepieciešamā neatkarības līmeņa ([107]).

(97) Papildus katram izlūkdienestu elementam ir pašam savs *ģenerālinspektors*, kura pienākums, cita starpā, ir pārraudzīt ārvalstu izlūkošanas darbības ([108]). NIDB tas ir Ģenerālinspektora birojs, kam ir visaptveroša kompetence visā izlūkdienestā un pilnvaras izskatīt sūdzības vai informāciju saistībā ar apgalvojumiem par nelikumīgu rīcību vai ļaunprātīgu varas izmantošanu saistībā ar NIDB un/vai izlūkošanas kopienas programmām un darbībām ([109]). Ģenerālinspektori ir likumiski neatkarīgas ([110]) vienības, kas ir atbildīgas par revīziju un izmeklēšanas veikšanu attiecībā uz programmām un darbībām, kuras īsteno attiecīgā aģentūra nacionālās izlūkošanas nolūkos, tostarp saistībā ar likuma ļaunprātīgu izmantošanu un pārkāpšanu ([111]). Tiem ir tiesības piekļūt visiem ierakstiem, atskaitēm, revīziju materiāliem, pārskatiem, dokumentiem, materiāliem, ieteikumiem un

([102]) Piemēram, NDA Atbilstības direktorātā strādā vairāk nekā 300 atbilstības darbinieki. Sk. NIDB apgalvojumus (VI pielikums), 7. lpp.
([103]) Sk. Ombuda mehānisma (III pielikums) 6(b)(i) līdz (iii) sadaļu.
([104]) Sk. *42 U.S.C. § 2000ee-1*. To vidū ir, piemēram, Valsts departaments, Tieslietu ministrija (tostarp FIB), Tēvzemes drošības departaments, Aizsardzības ministrija, NDA, CIP un NIDB.
([105]) Ka apgalvo ASV valdība, ja NIDB Pilsonisko brīvību un privātuma birojs saņem sūdzību, tas ar citiem izlūkdienestu elementiem arī saskaņos to, kā šo sūdzību IK būtu turpmāk jāapstrādā. Sk. Ombuda mehānisma (III pielikums) 6(b)(ii) sadaļu.
([106]) Sk. *42 U.S.C. § 2000ee-1 (f)(1),(2)*.
([107]) Sk. 29. panta Datu aizsardzības darba grupas Atzinumu 01/2016 par ES un ASV privātuma vairoga atbilstību lēmuma projektu (pieņemts 2016. gada 13. aprīlī), 41. lpp.
([108]) NIDB apgalvojumi (VI pielikums), 7. lpp. Sk., piemēram, NDA, PPD-28 4. sadaļu "Procedūras", 2015. gada 12. janvāris, 8.1. sadaļa; CIP, "Sakaru izlūkošanas darbības" (*Signals Intelligence Activities*), 7. lpp. ("Pienākumi").
([109]) Šo ģenerālinspektoru (ĢI) (kura amats izveidots 2010. gada oktobrī) ieceļ prezidents, viņu apstiprina Senāts un viņu var atstādināt tikai prezidents, nevis NID.
([110]) Ģenerālinspektoriem ir noteikts laiks amatā, un tos var atstādināt tikai prezidents, kuram rakstveidā jāpaziņo Kongresam šādas atstādināšanas iemesli. Tas nebūt nenozīmē, ka uz tiem pilnībā neattiecas norādījumi. Dažos gadījumos departamenta vadītājs var aizliegt ģenerālinspektoram uzsākt, veikt vai pabeigt revīziju vai izmeklēšanu, ja tas tiek uzskatīts par nepieciešamu, lai ievērotu svarīgas nacionālās (drošības) intereses. Taču Kongress ir jāinformē par šādas pilnvaras izmantošanu, un, pamatojoties uz to, tas var saukt pie atbildības attiecīgo vadītāju. Sk., piemēram, 1978. gada Ģenerālinspektoru likuma 8. pantu (Aizsardzības ministrijas ģenerālinspektors); *§ 8E* (Tieslietu ministrijas ģenerālinspektors), *§ 8G (d)(2)(A),(B)* (NDA ģenerālinspektors); *50. U.S.C.* 403q. sadaļas b) daļu (CIP ģenerāldirektors); 2010. fiskālā gada Izlūkošanas atļaujas likuma 405. panta f) punktu (izlūkdienesta ģenerālinspektors). Saskaņā ar valsts datu aizsardzības iestāžu novērtējumu ģenerālinspektori *"visdrīzāk izpilda organizatoriskās neatkarīgas kritērijus, kā tos definējusi Eiropas Savienības Tiesa un Eiropas Cilvēktiesību tiesa (ECT), vismaz no brīža, kad jaunā iecelšanas kārtība tiek piemērota visiem."* Sk. 29. panta Datu aizsardzības darba grupas Atzinumu 01/2016 par ES un ASV privātuma vairoga atbilstību lēmuma projektu (pieņemts 2016. gada 13. aprīlī), 40. lpp.
([111]) Sk. NIDB apgalvojumus (VI pielikums), 7. lpp. Skat arī. 1978. gada Ģenerālinspektoru likumu ar grozījumiem, publicēts L. 113–126, 2014. gada 7. jūlijs.

citiem būtiskiem materiāliem, vajadzības gadījumā ar tiesas pavēsti, un iegūt liecības nopratināšanā ([112]). Lai arī ģenerālinspektori var izdot tikai nesaistošus ieteikumus koriģējošai rīcībai, to atskaites, tostarp par turpmāku rīcību (vai tās trūkumu), tiek publicētas un nosūtītas Kongresam, kas, pamatojoties uz to, var izmantot savu pārraudzības funkciju ([113]).

(98) Turklāt *Privātuma un pilsonisko brīvību pārraudzības padomei* – neatkarīga izpildvaras aģentūra ([114]), ko veido divu pušu izvirzīti pieci locekļi ([115]), kurus uz sešu gadu laikposmu ieceļ prezidents ar Senāta apstiprinājumu – ir uzticēti pienākumi pretterorisma politikas virzienu jomā un to īstenošanā ar mērķi aizsargāt privātumu un pilsoniskās brīvības. Pārbaudot izlūkdienestu darbības, tā var piekļūt visiem attiecīgo aģentūru ierakstiem, atskaitēm, revīziju materiāliem, pārskatiem, dokumentiem, materiāliem un ieteikumiem, tostarp klasificētai informācijai, veikt nopratināšanu un uzklausīt liecības. Tā saņem ziņojumus no dažādu federālo departamentu/aģentūru pilsonisko brīvību un privātuma inspektoriem ([116]), var izdot tiem ieteikumus un regulāri atskaitās Kongresa komitejām un prezidentam ([117]). PPBPP ir uzdots tās kompetences ietvaros sagatavot ziņojumu, kurā ir novērtēta PPD-28 īstenošana.

(99) Visbeidzot, iepriekš minētos pārraudzības mehānismus papildina *Izlūkošanas pārraudzības padome*, ko ieceļ Prezidenta izlūkošanas pārraudzības padomes ietvaros, kura pārrauga to, kā ASV izlūkošanas iestādes ievēro Konstitūciju un visus piemērojamos noteikumus.

(100) Lai sekmētu pārraudzību, izlūkdienestu elementi tiek mudināti izstrādāt informācijas sistēmas, lai varētu uzraudzīt, reģistrēt un pārskatīt prasījumus vai cita veida personiskās informācijas meklējumus ([118]). Pārraudzības un atbilstības struktūras periodiski pārbaudīs izlūkdienestu elementu praksi attiecībā uz tādas personiskās informācijas aizsardzību, kas iekļauta sakaru izlūkošanā, un to atbilstību šīm procedūrām ([119]).

(101) Turklāt šīs pārraudzības funkcijas stiprina apjomīgas ziņošanas prasības attiecībā uz neatbilstību. Konkrēti, ar aģentūras procedūrām ir jānodrošina, ka, rodoties ievērojamai atbilstības problēmai, kas saistīta ar jebkuras personas, neatkarīgi no pilsonības, personisko informāciju, kas vākta sakaru izlūkošanas ietvaros, par šādu problēmu nekavējoties ziņo izlūkdienestu elementa vadītājam, kurš savukārt informē nacionālās izlūkošanas direktoru, kuram saskaņā ar *PPD-28* ir jānosaka, vai ir nepieciešamas koriģējošas darbības ([120]). Turklāt saskaņā ar *E.O. 12333* visiem izlūkdienestu elementiem ir noteikta prasība ziņot par neatbilstības gadījumiem Izlūkošanas pārraudzības padomei ([121]). Šie mehānismi nodrošina, ka problēma tiks risināta augstākajā izlūkdienestu līmenī. Ja

([112]) Sk. 1978. gada Ģenerālinspektoru likumu 6. pantu.
([113]) Sk. NIDB apgalvojumus (VI pielikums), 7. lpp. Skat arī. 1978. gada Ģenerālinspektoru likuma 4. panta 5. punktu, 5. pantu. Saskaņā ar 2010. fiskālā gada Izlūkošanas atļaujas likuma 405. panta b) punkta 3. un 4. daļu, publicets L. 111–259, 2010. gada 7. oktobris, izlūkdienesta ģenerālinspektors pastāvīgi informē NID, kā arī Kongresu par koriģējošu darbību nepieciešamību un progresu.
([114]) Saskaņā ar valsts datu aizsardzības iestāžu novērtējumu PPBPP līdz ir šim ir "demonstrējusi savu neatkarību". Sk. 29. panta Datu aizsardzības darba grupas Atzinumu 01/2016 par ES un ASV privātuma vairoga atbilstību lēmuma projektu (pieņemts 2016. gada 13. aprīlī), 42. lpp.
([115]) Papildus PPBPP strādā aptuveni 20 pastāvīgo darbinieku. Sk. https://www.pclob.gov/about-us/staff.html
([116]) To vidū ir vismaz Tieslietu ministrija, Aizsardzības ministrija, Tēvzemes drošības departaments, nacionālās izlūkošanas direktors un Centrālā izlūkošanas pārvalde, kā arī jebkurš cits izpildvaras departaments, aģentūra vai elements, kuru PPBPP atzinusi par piemērotu.
([117]) Sk. *42 U.S.C. § 2000ee*. Sk. Ombuda mehānisma (III pielikums) 6. punkta b) apakšpunkta iv) punktu. Cita starpā PPBPP ir jāziņo par gadījumiem, kad izpildvaras aģentūra atsakās ņemt vērā tās ieteikumus.
([118]) NIDB, *Safeguarding the Personal Information of all People*: *A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, 7.–8. lpp.
([119]) Turpat, 8. lpp. Sk. arī NIDB apgalvojumus (VI pielikums), 9. lpp.
([120]) NIDB, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, 7. lpp. Sk., piemēram, NDA, PPD-28 4. sadaļu "Procedūras", 2015. gada 12. janvāris, 7.3, 8.7(c),(d) sadaļa; FIB, *Presidential Policy Directive 28 Policies and Procedures*, III nodaļas A daļas 4. punkts, B daļas 4. punkts; CIP, "Sakaru izlūkošanas darbības" (*Signals Intelligence Activities*), 6. p. ("Atbilstība") un 8. p. ("Pienākumi").
([121]) Sk. *E.O. 12333* 1.6(c) sadaļu.

ir iesaistīta citu valstu persona, nacionālās izlūkošanas direktors, konsultējoties ar valsts sekretāru un ziņojošā departamenta vai aģentūras vadītāju, nosaka, vai ir jāveic kādas darbības, lai informētu attiecīgo ārvalstu valdību atbilstoši avotu un metožu, kā arī ASV personāla aizsardzībai ([122]).

(102) Otrkārt, papildus šiem izpildvaras pārraudzības mehānismiem ASV Kongresam, konkrēti *Parlamenta un Senāta izlūkošanas un tieslietu komitejām*, ir pārraudzības pienākumi attiecībā uz visām ASV ārvalstu izlūkošanas darbībām, tostarp ASV sakaru izlūkošanu. Saskaņā ar Nacionālās drošības likumu "prezidents nodrošina, ka kongresa izlūkošanas komitejas tiek pilnībā un vienmēr informētas par Amerikas Savienoto Valstu izlūkošanas darbībām, tostarp jebkādu nozīmīgu gaidāmu izlūkošanas darbību saskaņā ar šo apakšnodaļu" ([123]). Tāpat "prezidents nodrošina, ka kongresa izlūkošanas komitejām nekavējoties tiek ziņots par jebkādu izlūkošanas darbību, kā arī jebkādu koriģējošu darbību, kas ir veikta vai tiek plānota saistībā ar šādu nelegālu rīcību" ([124]). Šo komiteju locekļiem ir piekļuve klasificētai informācijai, kā arī izlūkošanas metodēm un programmām ([125]).

(103) Ar turpmākiem tiesību aktiem ziņošanas prasības ir paplašinātas un pilnveidotas gan attiecībā uz izlūkdienestu elementiem, attiecīgajiem ģenerālinspektoriem, gan uz ģenerālprokuroru. Piemēram, ĀIUL nosaka, ka ģenerālprokuroram ir "pilnībā jāinformē" Senāta un Parlamenta izlūkošanas un tieslietu komitejas par valdības darbībām saskaņā ar atsevišķiem ĀIUL pantiem ([126]). Tas arī nosaka, ka valdībai ir jāiesniedz Kongresa komitejām "kopijas visiem lēmumiem, rīkojumiem vai atzinumiem, ko izdevusi Ārvalstu izlūkošanas uzraudzības tiesa vai Ārvalstu izlūkošanas uzraudzības apelācijas tiesa un kas ietver" ĀIUL noteikumu "būtisku izskaidrojumu vai interpretāciju". Konkrēti, attiecībā uz pārraudzību saskaņā ar ĀIUL 702. pantu pārraudzību veic ar likumā noteiktiem ziņojumiem Izlūkošanas un Tieslietu komitejām, kā arī regulārām instruktāžām un pārrunām. Tajā skaitā ir ģenerālprokurora pusgada ziņojums, kurā aprakstīta ĀIUL 702. panta izmantošana, pievienoti apliecinoši dokumenti, tostarp jo īpaši Tieslietu ministrijas un NIDB atbilstības ziņojumi un jebkādu neatbilstības gadījumu apraksts, ([127]) kā arī atsevišķs ģenerālprokurora un NID pusgada novērtējums, kurā dokumentēta atbilstība mērķēšanas un minimizācijas procedūrām, tostarp atbilstība procedūrām, kas paredzētas, lai nodrošinātu, ka ievākšana tiek veikta likumīgā ārvalstu izlūkošanas nolūkā ([128]). Kongress saņem arī ziņojumus no ģenerālinspektoriem, kuriem ir tiesības novērtēt aģentūru atbilstību mērķēšanas un minimizācijas procedūrām un ģenerālprokurora pamatnostādnēm.

(104) Saskaņā ar 2015. gada ASV Brīvības likumu ASV valdībai katru gadu ir jāatklāj Kongresam (un sabiedrībai) ĀIUL pieprasīto un saņemto rīkojumu un direktīvu skaits, kā arī, cita starpā, to ASV piederīgo un citu valstu personu skaita aplēses, pret kurām vērsta uzraudzība ([129]). Ar likumu ir noteikta papildu publiska ziņošana par izdoto

([122]) PPD-28 4(a)(iv) sadaļa.
([123]) Sk. 501(a)(1) sadaļu (*50 U.S.C. § 413(a)(1)*). Šajā noteikumā ir iekļautas vispārīgas prasības attiecībā uz Kongresa pārraudzību valsts drošības jomā.
([124]) Sk. 501(b) sadaļu (*50 U.S.C. § 413(b)*).
([125]) Sal. 501(d) sadaļu (*50 U.S.C. § 413(d)*).
([126]) Sk. *50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.*
([127]) Sk. *50 U.S.C. § 1881f.*
([128]) Sk. *50 U.S.C. § 1881a(l)(1).*
([129]) Sk. 2015. gada ASV Brīvības likums, publicēts L. Nr. 114-23, 602.(a) sadaļa. Papildus saskaņā ar 402. pantu "nacionālās izlūkošanas direktors, konsultējoties ar ģenerālprokuroru, veic katra Ārvalstu izlūkošanas uzraudzības tiesas vai Ārvalstu izlūkošanas uzraudzības revīzijas tiesas izdota lēmuma, rīkojuma vai atzinuma deklasificēšanas pārskatu (kā noteikts 601. panta e) daļā), kurā iekļauta jebkura likuma noteikuma būtiska interpretācija, tostarp jebkāda jauna vai būtiska termina "specifisks atlases nosacījums" interpretācija, un atbilstīgi šim pārskatam katru lēmumu, rīkojumu vai atzinumu publisko pēc iespējas plašākā mērogā".

NDV skaitu, atkal attiecībā gan uz ASV, gan citu valstu personām (vienlaikus atļaujot ĀIUL rīkojumu un apliecinājumu, kā arī NDV pieprasījumu saņēmējiem noteiktos apstākļos izdot pārredzamības ziņojumus) ([130]).

(105) Treškārt, ASV valsts iestāžu izlūkošanas darbības, pamatojoties uz ĀIUL, ļauj *ĀIUL tiesai* (ĀIUT) ([131]), kas ir neatkarīga tiesa ([132]), kuras lēmumus var apstrīdēt Ārvalstu izlūkošanas apelācijas tiesā (ĀIAT) ([133]), un galu galā Amerikas Savienoto Valstu Augstākajai tiesai ([134]) pārskatīt un atsevišķos gadījumos iepriekš apstiprināt pasākumus. Iepriekšējas apstiprināšanas gadījumā pieprasījumu iesniegušajām iestādēm (FIB, NDA, CIP utt.) būs jāiesniedz pieteikuma projekts Tieslietu ministrijas Valsts drošības departamenta juristiem, kuri to rūpīgi pārbaudīs un, ja nepieciešams, pieprasīs papildu informāciju ([135]). Kad pieteikums būs pabeigts, nacionālās drošības ģenerālprokuroram, ģenerālprokurora vietniekam vai ģenerālprokurora palīgam tas būs jāapstiprina ([136]). Pēc tam Tieslietu ministrija iesniegs pieteikumu ĀIUT, kas to izvērtēs un pieņems pagaidu lēmumu par tālāko rīcību ([137]). Ja notiek lietas izskatīšana, ĀIUT ir tiesības uzklausīt liecības, kas var ietvert ekspertu ieteikumus ([138]).

(106) ĀIUT (un ĀIAT) strādā pastāvīga piecu personu grupa ar zinātību valsts drošības, kā arī pilsonisko brīvību jautājumos ([139]). No šīs grupas tiesa ieceļ personu, kas darbojas kā *amicus curiae*, lai palīdzētu izskatīt jebkuru pieteikumu rīkojumam vai pārskatīšanai, kas pēc tiesas ieskatiem sniedz jaunu vai būtisku likuma interpretāciju, ja vien tiesa nesecina, ka šāda iecelšana nav atbilstīga ([140]). Tam jo īpaši jānodrošina, ka tiesas novērtējumā ir pienācīgi atspoguļoti privātuma apsvērumi. Tiesa var iecelt arī personu vai organizāciju, kas darbojas kā *amicus curiae*, tostarp sniedzot tehnisko ekspertīzi, kad vien uzskata to par nepieciešamu, vai arī, pamatojoties uz pieprasījumu, ļaut personai vai organizācijai pagarināt *amicus curiae* darbības termiņu ([141]).

([130]) ASV Brīvības likums, 602(a), 603(a) sadaļa.

([131]) Noteiktu veidu uzraudzības gadījumos kā alternatīvai ASV izmeklēšanas tiesnesim, ko publiski iecēlis Amerikas Savienoto Valstu galvenais tiesnesis, ir tiesības arī uzklausīt pieteikumus un izdot rīkojumus.

([132]) ĀIUT sastāvā ir vienpadsmit tiesneši, kurus Amerikas Savienoto Valstu galvenais tiesnesis ieceļ no esošajiem ASV apgabaltiesu tiesnešiem, kurus iepriekš nozīmējis prezidents un apstiprinājis Senāts. Tiesneši saglabā amatu uz mūžu, viņus var atcelt tikai pamatota iemesla dēļ, un viņi ĀIUL mainās rotācijas kārtībā ir pēc septiņiem gadiem. ĀIUL nosaka, ka tiesnešiem jābūt no vismaz septiņiem dažādiem ASV tiesu apgabaliem. Sk. *Sec 103 FISA (50 U.S.C. 1803 (a));* PPBPP ziņojuma 215. sadaļa, 174.–187. lpp. Tiesnešiem palīdz pieredzējuši tiesas ierēdņi, kas ir tiesas juridiskie darbinieki un sagatavo ievākšanas pieprasījumu juridisko analīzi. Sk. PPBPP ziņojuma 215. sadaļu, 178. lpp.; godājamā ĀSV Ārvalstu izlūkošanas uzraudzības tiesas galvenā tiesneša god. Regija B. Valtona (*Reggie B. Walton*) vēstule ASV Senāta Tieslietu komitejas priekšsēdētājam god. Patrikam Dž. Leihī (*Patrick J. Leahy*) (2013. gada 29. jūlijs) ("Valtona vēstule"), 2.–3. lpp.

([133]) ĀIAT sastāvā ir trīs tiesneši, kurus ieceļ Amerikas Savienoto Valstu galvenais tiesnesis un kurus pieaicina no ASV apgabaltiesām vai apelācijas tiesām un viņi mainās rotācijas kārtībā ir pēc septiņiem gadiem. Sk. *Sec. 103 FISA (50 U.S.C. § 1803 (b)).*

([134]) Sk. *50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).*

([135]) Piemēram, papildu fakti par izlūkošanas mērķi, tehniska informācija par izlūkošanas metodiku vai apgalvojumi par to, kā iegūtā informācija tiks izmantota un izplatīta. Sk. PPBPP ziņojuma 215. sadaļu, 177. lpp.;

([136]) *50 U.S.C. §§ 1804 (a), 1801 (g).*

([137]) ĀIUL var apstiprināt pieteikumu, pieprasīt papildu informāciju, noteikt nepieciešamību veikt nopratināšanu vai norādīt iespējamu pieteikuma noraidījumu. Balstoties uz šo pagaidu lēmumu, valdība izstrādās galīgo pieteikumu. Tajā var būt iekļautas būtiskas izmaiņas salīdzinājumā ar sākotnējo pieteikumu, pamatojoties uz tiesneša provizoriskiem komentāriem. Lai arī lielu daļu galīgo pieteikumu apstiprina ĀIUT, ievērojama to daļa satur būtiskas izmaiņas salīdzinājumā ar sākotnējo pieteikumu, piemēram, 24 % apstiprināto pieteikumu periodā no 2013. gada jūlija līdz septembrim. Sk. PPBPP ziņojuma 215. sadaļu, 179. lpp.; Valtona vēstules 3. lpp.

([138]) PPBPP ziņojuma 215. sadaļu, 179. lpp., Nr. 619.

([139]) *50 U.S.C. § 1803 (i)(1),(3)(A).* Ar šo jauno likumu tika īstenoti PPBPP ieteikumi izveidot privātuma un pilsonisko brīvību ekspertu grupu, kas var darboties kā *amicus curiae*, lai sniegtu tiesai juridiskus argumentus par progresu privātuma un pilsonisko brīvību jomā. Sk. PPBPP ziņojuma 215. sadaļu, 183.–187. lpp.

([140]) *50 U.S.C. § 1803 (i)(2)(A).* Saskaņā ar NIDB sniegto informāciju šāda iecelšana jau ir notikusi. Sk. Sakaru izlūkošanas reformas (*Signals Intelligence Reform*) 2016. gada progresa ziņojumu.

([141]) *50 U.S.C. § 1803 (i)(2)(B).*

(107) Attiecībā uz divām likumīgajām uzraudzības atļaujām saskaņā ar ĀIUL, kuras ir vissvarīgākās datu pārsūtīšanai ES un ASV privātuma vairoga ietvaros, ĀIUT pārraudzība ir atšķirīga.

(108) Saskaņā ar ĀIUL 501. pantu ([142]), ar kuru ir atļauts ievākt "jebkādas taustāmas lietas (tostarp grāmatas, ierakstus, papīrus, dokumentus un citas lietas)", pieteikumā ĀIUT ir jāiekļauj faktu izklāsts, apliecinot, ka ir pamatots iemesls ticēt, ka pieprasītās taustāmās lietas ir būtiskas attiecībā uz atļauto izmeklēšanu (izņemot apdraudējumu novērtējumu), kas veikta, lai iegūtu ārvalstu izlūkošanas informāciju, kas nav saistīta ar ASV piederīgu personu, vai aizsardzību pret starptautisko terorismu vai slepenām izlūkošanas darbībām. Tāpat pieteikumā ir jāiekļauj ģenerālprokurora apstiprināts minimizācijas procedūru saraksts ievākto izlūkdatu saglabāšanai un izplatīšanai. ([143])

(109) Turpretī saskaņā ar ĀIUL 702. pantu ([144]) ĀIUT neapstiprina individuālus uzraudzības pasākumus, bet gan uzraudzības programmas (piemēram, *PRISM, UPSTREAM*), pamatojoties uz ikgadējām sertifikācijām, kuras sagatavo ģenerālprokurors un nacionālās izlūkošanas direktors. Ar ĀIUL 702. pantu ir atļauts izsekot personas, attiecībā uz kurām ir pamats uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām Valstīm, lai iegūtu ārvalstu izlūkošanas informāciju ([145]). Šādu izsekošanu NDA veic divos posmos. Pirmajā NDA analītiķi identificē ārvalstīs esošas citu valstu personas, kuru uzraudzība, pamatojoties uz analītiķu novērtējumu, ļaus nonākt līdz attiecīgajai ārvalstu izlūkošanai, kas norādīta sertifikācijā. Otrajā, kad ir identificētas atsevišķas personas un to izsekošana ir apstiprināta ar plašu pārskatīšanas mehānismu NDA ([146]), izraudzītājiem, kas identificē izsekoto personu sakaru līdzekļus (piemēram, e-pasta adreses), tiks dots uzdevums (t.i. izstrādāts un piemērots) ([147]). Kā norādīts, sertifikācijas, kuras jāapstiprina ĀIUT, nesatur informāciju par atsevišķām personām, kuras jāizseko, bet gan identificē ārvalstu izlūkošanas informācijas kategorijas ([148]). Lai arī ĀIUT nevērtē – pamatojoties uz ticamu iemeslu vai kādu citu standartu –, vai personas ir atbilstīgi izsekotas, lai iegūtu ārvalstu izlūkošanas informāciju ([149]), tās kontrole ietver nosacījumu, ka "būtisks iegūšanas mērķis ir iegūt ārvalstu izlūkošanas informāciju" ([150]). Saskaņā ar ĀIUL 702. pantu NDA patiešām ir ļauts ievākt ārpus ASV esošu citu valstu personu sakarus tikai tad, ja ir pamats uzskatīt, ka attiecīgais sakaru līdzeklis tiek izmantots, lai izplatītu ārvalstu izlūkošanas informāciju (piemēram, saistībā ar starptautisko terorismu, kodolieroču izplatīšanu vai nelabvēlīgām kiberdarbībām). Lēmumi šajā saistībā ir apstrīdami tiesā ([151]). Sertifikācijās ir jāparedz arī mērķēšanas un minimizācijas procedūras ([152]).

([142]) *50 U.S.C. § 1861*
([143]) *50 U. S. C. § 1861(b)*
([144]) *50 U.S.C. § 1881.*
([145]) *50 U.S.C. § 1881a (a).*
([146]) PPBPP ziņojuma 702. sadaļa, 46. lpp.
([147]) *50 U.S.C. § 1881a (h).*
([148]) *50 U.S.C. § 1881a (g).* Saskaņā ar PPBPP šīs kategorijas līdz šim galvenokārt bijušas saistītas ar starptautisko terorismu un tādām tēmām kā masu iznīcināšanas ieroču iegūšana. Sk. PPBPP ziņojuma 702. sadaļu, 25. lpp.;
([149]) PPBPP ziņojuma 702. sadaļu, 27. lpp.
([150]) *50 U.S.C. § 1881a.*
([151]) *Liberty and Security in a Changing World* ("Brīvība un drošība mainīgā pasaulē"), Prezidenta izlūkošanas un sakaru tehnoloģijas pārskatīšanas grupas ziņojums un ieteikumi, 2013. gada 12. decembris, 152. lpp. U.S.C.
([152]) 50. sadaļas 1881a. iedaļas i) daļa.

Ģenerālprokurors un nacionālās izlūkošanas direktors pārbauda atbilstību, un aģentūru pienākums ir par jebkādiem neatbilstības gadījumiem ziņot ĀIUL ([153]) (kā arī Kongresam un Prezidenta izlūkošanas pārraudzības padomei), kas, pamatojoties uz to, var grozīt atļauju ([154]).

(110) Turklāt, lai palielinātu ĀIUT pārraudzības efektivitāti, ASV valdība ir piekritusi īstenot PPBPP ieteikumu sniegt ĀIUT dokumentāciju saistībā ar 702. panta mērķēšanas lēmumiem, tostarp nejauši izvēlētu uzdevumu lapu paraugu, lai ĀIUT varētu novērtēt, kā ārvalstu izlūkošanas nolūka prasība tiek izpildīta praksē ([155]). Tajā pašā laikā ASV valdība piekrita pārskatīt NDA mērķēšanas procedūras un ir veikusi attiecīgas darbības, lai labāk dokumentētu ārvalstu izlūkošanas iemeslus mērķēšanas lēmumiem ([156]).

Individuāla tiesiskā aizsardzība

(111) ES datu subjektiem saskaņā ar ASV tiesībām ir vairākas iespējas, ja tie bažījas par to, vai viņu personas datus ir apstrādājuši (ievākuši, izvērtējuši utt.) ASV izlūkdienestu elementi, un, ja tā, vai ir ievēroti ierobežojumi, kas piemēroti ASV tiesībās. Tie galvenokārt attiecas uz trīs jomām: iejaukšanos saskaņā ar ĀIUL; nelikumīgu, tīšu valsts amatpersonu piekļuvi personas datiem; un piekļuvi informācijai saskaņā ar Likumu par informācijas brīvību (*Freedom of Information Act*) (LIB) ([157]).

(112) Pirmkārt, Ārvalstu izlūkošanas uzraudzības likums paredz vairākus tiesiskās aizsardzības līdzekļus, pieejamus arī c personām, ar kuriem apstrīdēt nelikumīgu elektronisko uzraudzību ([158]). To vidū ir iespēja personām celt civilprasību pret Amerikas Savienotajām Valstīm par finansiāliem zaudējumiem, ja informācija par šīm personām ir nelikumīgi un tīši izmantota vai izpausta ([159]); iesūdzēt tiesā ASV valsts amatpersonas kā privātpersonas (kas nelikumīgi veic likumīgu darbību) par finansiāliem zaudējumiem ([160]); un apstrīdēt uzraudzības likumību (un pieprasīt noklusēt informāciju) gadījumā, ja ASV valdība plāno izmantot vai izpaust jebkādu informāciju, kas iegūta vai atvasināta no elektroniskās uzraudzības attiecībā uz personu, tiesā vai administratīvajā kārtībā Amerikas Savienotajās Valstīs ([161]).

(113) Otrkārt, ASV valdība norādīja Komisijai vairākas papildu iespējas, kuras ES datu subjekti var izmantot, lai pieprasītu tiesību aizsardzību pret valdības amatpersonām attiecībā uz nelikumīgu valdības piekļuvi personas

([153]) ĀIUT procedūras noteikumu 13.b noteikumā ir prasība valdībai nekavējoties iesniegt tiesai rakstveida paziņojumu, kolīdz tiek atklāts, ka kāda tiesas atļauja vai apstiprinājums ir īstenots veidā, kas neatbilst tiesas atļaujai vai apstiprinājumam, vai piemērojamajam likumam. Tas arī nosaka, ka valdībai rakstveidā jāinformē tiesa par faktiem un apstākļiem, kas attiecas uz šādu neatbilstību. Parasti valdība iesniedz 13.a noteikuma paziņojumu, kad attiecīgie fakti ir zināmi un visi neatļauti ievāktie dati ir iznīcināti. Sk. Valtona vēstules 10. lpp.

([154]) *50 U.S.C. § 1881 (l)*. Sk. arī PPBPP ziņojuma 702. sadaļu, 66.–76. lpp.; NDA PBPB, Ārvalstu izlūkošanas uzraudzības likuma 702. panta īstenošana, ko veic NDA, 16.4.2014. Personas datu ievākšanai izlūkošanas nolūkos saskaņā ar ĀIUL 702. pantu piemēro gan iekšējo, gan ārējo izpildvaras pārraudzību. Cita starpā, iekšējā uzraudzība ietver iekšējās atbilstības programmas, ar kurām novērtēt un pārraudzīt atbilstību mērķēšanas un minimizācijas procedūrām; ziņošanu NIDB, Tieslietu ministrijai, Kongresam un ĀIUL par iekšējiem un ārējiem neatbilstības gadījumiem, un ikgadējus pārskatus, kas tiek sūtīti šīm pašām struktūrām. Kas attiecas uz ārējo pārraudzību, tā galvenokārt ietver mērķēšanas un minimizācijas pārskatus, kurus veic NIDB, Tieslietu ministrija un ģenerālinspektors, kas savukārt ziņo Kongresam un ĀIUT, tostarp par neatbilstības gadījumiem. Par būtiskiem neatbilstības gadījumiem ir jāziņo ĀIUT nekavējoties, par pārējiem – ceturkšņa ziņojumā. Sk. PPBPP ziņojuma 702. sadaļu, 66.–77. lpp.

([155]) PPBPP, Ieteikumu novērtēšanas ziņojums, 2015. gada 29. janvāris, 20. lpp.

([156]) PPBPP, Ieteikumu novērtēšanas ziņojums, 2015. gada 29. janvāris, 16. lpp.

([157]) Turklāt Likuma par klasificētas informācijas procedūrām 10. pantā ir paredzēts, ka jebkurā apsūdzībā, kurā Amerikas Savienotajām Valstīm jānosaka, ka materiāls ir uzskatāms par klasificētu informāciju (piemēram, tāpēc, ka tam ir nepieciešama aizsardzība pret neatļautu izpaušanu nacionālās drošības dēļ), Amerikas Savienotās Valstis informē apsūdzēto par materiāla daļām, uz kurām tā pamatoti paredz paļauties, lai noteiktu nodarījuma klasificētās informācijas elementu.

([158]) Sk. šādus NIDB apgalvojumus (VI pielikums), 16. lpp.

([159]) *18 U.S.C. § 2712*.

([160]) *50 U.S.C. § 1810*.

([161]) *50 U.S.C. § 1806*.

datiem vai to izmantošanu, tostarp paredzētos nacionālās drošības nolūkos (t. i., Likums par krāpniecību ar datora starpniecību un tā ļaunprātīgu izmantošanu (*Computer Fraud and Abuse Act*) ([162]), Elektroniskās saziņas privātuma likums ([163]); Likums par tiesībām uz finanšu datu aizsardzību (*Right to Financial Privacy Act*) ([164]). Visi šie prasības pamati ir saistīti ar specifiskiem datiem, mērķiem un/vai piekļuves veidiem (piemēram, piekļuve datoram ar tālvadību caur internetu) un ir pieejami noteiktos apstākļos (piemēram, apzināta/tīša rīcība, rīcība ārpus dienesta pilnvarām, ciestie zaudējumi) ([165]). Vispārīgi tiesiskās aizsardzības iespēja ir paredzēta saskaņā ar Administratīvā procesa likumu (*5 U.S.C. § 702*), saskaņā ar kuru "jebkurai personai, kam nodarīta juridiska netaisnība aģentūras darbības rezultātā vai ko nelabvēlīgi ietekmē vai neapmierina aģentūras darbība", ir tiesības vērsties tiesā. Tas ietver iespēju lūgt tiesu "apturēt nelikumību un atcelt aģentūras darbību, konstatējumus un secinājumus, kas atzīti par […] patvaļīgiem, nepamatotiem, pieņemtiem, ļaunprātīgi izmantojot dienesta stāvokli, vai citādi pretrunā ar tiesību aktiem" ([166]).

(114) Visbeidzot, ASV valdība ir norādījusi uz LIB kā līdzekli citu valstu personām, ar kuru pieprasīt piekļuvi esošajiem federālās aģentūras ierakstiem, tostarp tad, ja tie satur attiecīgās privātpersonas personas datus ([167]). Ņemot vērā tvērumu, uz ko vērsts LIB, tas neparedz individuālu tiesību aizsardzību pret iejaukšanos personas datos, lai arī principā tas ļautu personām iegūt piekļuvi būtiskai informācijai, kuru glabā nacionālās izlūkošanas aģentūras. Pat šajā ziņā iespējas šķiet ierobežotas, jo aģentūras var neizpaust informāciju, uz kuru attiecas noteikti uzskaitīti izņēmumi, tostarp piekļuve klasificētai nacionālās drošības informācijai un informācijai saistībā ar tiesībaizsardzības izmeklēšanām ([168]). Tomēr, ja nacionālās izlūkošanas aģentūras izmanto šādus izņēmumus, personas var to apstrīdēt, pieprasot gan administratīvu izskatīšanu, gan izskatīšanu tiesā.

(115) Lai arī tādējādi personām, tostarp ES datu subjektiem, ir vairākas tiesiskās aizsardzības iespējas, ja tās ir pakļautas nelikumīgai (elektroniskajai) uzraudzībai nacionālās drošības nolūkos, tikpat skaidrs ir tas, ka nav iekļauti atsevišķi juridiskie pamatojumi (piemēram, *E.O. 12333*), kurus var izmantot ASV izlūkošanas iestādes. Turklāt, ja tiesiskās aizsardzības iespējas principā ir citu valstu personām, piemēram, uzraudzībai saskaņā ar ĀIUL, pieejamie rīcības pamatojumi ir ierobežoti ([169]), un personu (tostarp ASV piederīgu personu) prasības tiks atzītas par nepieņemamām, ja tās nevar pierādīt "tiesībspēju" ([170]), un tas ierobežo piekļuvi parastajām tiesām ([171]).

(116) Lai paredzētu papildu tiesiskās aizsardzības iespējas, kas pieejamas visiem ES datu subjektiem, ASV valdība ir nolēmusi izveidot jaunu ombuda mehānismu, kā izklāstīts ASV valsts sekretāra vēstulē Komisijai, vēstule ir pievienota šā lēmuma III pielikumā. Šā mehānismā pamatā ir vecākā koordinatora (valsts sekretāra vietnieka līmenī) iecelšana Valsts departamentā saskaņā ar PPD-28, kurš darbosies kā kontaktpunkts ārvalstu valdībām, lai tās varētu izteikt bažas saistībā ar ASV sakaru izlūkošanas darbībām, taču tā darbības joma ir daudz plašāka par sākotnējo konceptu.

([162]) *18 U.S.C. § 1030*.
([163]) *18 U.S.C. §§ 2701-2712*.
([164]) *12 U.S.C. § 3417*.
([165]) NIDB apgalvojumi (VI pielikums), 17. lpp.
([166]) *5 U.S.C. § 706(2)(A)*.
([167]) *5 U.S.C. § 552*. Līdzīgi likumi pastāv štatu līmenī.
([168]) Tādā gadījumā persona parasti saņem tikai standarta atbildi, ar kuru aģentūra atsakās apstiprināt vai noliegt jebkādu ierakstu esību. Sk. *ACLU v. CIA, 710 F.3d 422 (D.C. Cir. 2014)*.
([169]) Sk. NIDB apgalvojumus (VI pielikums), 16. lpp. Saskaņā ar sniegtajiem skaidrojumiem pieejamajiem rīcības veidiem ir nepieciešama *zaudējumu* esība (*18 U.S.C. § 2712*; *50 U.S.C. § 1810*) vai apliecinājums par to, ka *valdība plāno izmantot vai izpaust informāciju*, kas iegūta vai atvasināta no attiecīgās personas elektroniskās uzraudzības, *tiesvedībā vai administratīvajā procesā* Amerikas Savienotajās Valstīs (*50 U.S.C. § 1806*). Taču, kā Tiesa vairākkārt uzsvērusi, lai konstatētu iejaukšanos pamattiesībās uz privātumu, nav svarīgi, vai attiecīgā persona ir izjutusi negatīvas sekas saistībā ar šādu iejaukšanos. Sk. *Schrems*, 89. punkts ar turpmākām atsaucēm.
([170]) Pieņemamības kritērija pamats ir "lietas vai strīda" prasība ASV Konstitūcijas III pantā.
([171]) Sk. *Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138, 1144 (2013)*. Attiecībā uz NDV izmantošanu ASV Brīvības likums (502. panta f) daļa) līdz 503. pantam) paredz, ka neizpaušanas prasības ir periodiski jāpārskata un ka NDV *saņēmēji* ir jāinformē, kad fakti vairs neapstiprina neizpaušanas prasību (sk. NIDB apgalvojumus (VI pielikums), 13. lpp.). Taču tas nenodrošina, ka ES datu subjekts tiek informēts par to, ka viņš (viņa) ir izmeklēšanas mērķis.

(117) Konkrēti, saskaņā ar ASV valdības saistībām ombuda mehānisms nodrošinās, ka personu sūdzības tiek atbilstoši izskatītas un personas saņem neatkarīgi apstiprinājumu tam, ka ir ievēroti ASV tiesību akti vai, šādu tiesību aktu pārkāpuma gadījumā, ir novērsti neatbilstība ([172]). Mehānismā ir ietverts "privātuma vairoga ombuds", proti, valsts sekretāra vietnieks un citi darbinieki, kā arī citas pārraudzības iestādes, kas ir kompetentas pārraudzīt izlūkdienestu dažādos elementus, un izskatot sūdzības, privātuma vairoga ombuds balstīsies uz sadarbību izlūkdienestiem. Jo īpaši, ja personas pieprasījums ir saistīts ar uzraudzības atbilstību ASV tiesību aktiem, privātuma vairoga ombuds varēs paļauties uz neatkarīgām pārraudzības struktūrām, kam ir izmeklēšanas pilnvaras (piemēram, PPBPP ģenerālinspektori). Katrā lietā valsts sekretārs nodrošina, ka ombudam būs nepieciešamie līdzekļi, lai nodrošinātu, ka tā atbildes uz individuāliem pieprasījumiem ir pamatotas ar visu vajadzīgo informāciju.

(118) Ar šo "kompozīto" struktūru ombuda mehānisms nodrošina neatkarīgu pārraudzību un personas tiesību aizsardzību. Turklāt sadarbība ar citām pārraudzības iestādēm nodrošina piekļuvi nepieciešamajai zinātībai. Visbeidzot, privātuma aizsardzību ombudam uzliekot pienākumu apstiprināt atbilstību vai labot jebkādu neatbilstību, mehānisms atspoguļo ASV valdības apņemšanos kopumā uzklausīt un risināt ES iedzīvotāju sūdzības.

(119) Pirmkārt, atšķirībā no starpvaldību mehānisma, privātuma vairoga ombuds saņems personu sūdzības un atbildēs uz tām. Šādas sūdzības var adresēt dalībvalstu uzraudzības struktūrām, kurām ir kompetence valsts drošības dienestu pārraudzībā un/vai to, kā valsts iestādes apstrādā personas datus, kuras šīs sūdzības iesniegs centralizētai ES struktūrai, kas pārsūtīs tās privātuma vairoga ombudam ([173]). Tā nudien būs priekšrocība ES personām, kuras varēs vērsties valsts iestādē "tuvu mājām" un to savā valodā. Šādas iestādes uzdevums būs palīdzēt personai, iesniedzot privātuma vairoga ombudam pieprasījumu, kurā būs iekļauta pamatinformācija un kurš tādējādi būs uzskatāms par "pilnīgu". Personai nebūs jāpierāda, ka ASV valdība tiešām ir piekļuvusi tās personas datiem, veicot sakaru izlūkošanas darbības.

(120) Otrkārt, ASV valdība apņemas nodrošināt, ka, veicot savas funkcijas, privātuma aizsardzību ombuds varēs paļauties uz sadarbību no citiem pārraudzības un atbilstības pārbaudes mehānismiem, kuri pieejami ASV tiesību aktos. Tādēļ dažkārt tiks iesaistītas valsts tiesībaizsardzības iestādes, jo īpaši gadījumos, kad pieprasījums ir jāinterpretē kā pieprasījums par piekļuvi dokumentiem saskaņā ar Likumu par informācijas brīvību. Citos gadījumos, jo īpaši, ja pieprasījumi ir saistīti ar uzraudzības atbilstību ASV tiesību aktiem, šāda sadarbība ietvers neatkarīgas pārraudzības struktūras (piemēram, ģenerālinspektorus) ar atbildību un pilnvarām veikt rūpīgu izmeklēšanu (jo īpaši, izmantojot piekļuvi visiem attiecīgajiem dokumentiem un pilnvaras pieprasīt informāciju un paziņojumus) un vērsties pret neatbilstību ([174]). Tāpat privātuma vairoga ombuds varēs nodot lietas izskatīšanai PPBPP ([175]). Ja viena no šīm pārraudzības iestādēm ir konstatējusi neatbilstību, attiecīgajam izlūkdienestu elementam (piemēram, izlūkošanas aģentūrai) būs jānovērš neatbilstība, jo tikai šādi ombuds varēs

([172]) Gadījumos, kad sūdzības iesniedzējs pieprasa piekļuvi dokumentiem, kas ir ASV valsts iestāžu rīcībā, piemēro Likumā par informācijas brīvību izklāstītos noteikumus un procedūras. Saskaņā ar LIB izklāstītajiem nosacījumiem tas ietver iespēju vērsties pēc tiesiskās aizsardzības (nevis neatkarīgas pārraudzības) gadījumā, ja pieprasījums ir noraidīts.

([173]) Saskaņā ar Ombuda mehānisma (III pielikums) 4. punkta f) apakšpunktu privātuma vairoga ombuds sazināsies tieši ar ES personu sūdzību izskatīšanas struktūru, kas savukārt būs atbildīga par saziņu ar personu, kura iesniegusi pieprasījumu. Ja tieša saziņa ir daļa no "saistītajiem procesiem", kas var nodrošināt pieprasīto palīdzību (piemēram, LIB piekļuves pieprasījums, sk. 5. pantu), šī saziņa notiek saskaņā ar piemērojamajām procedūrām.

([174]) Sk. Ombuda mehānisma (III pielikums) 2. punkta a) apakšpunktu. Sk. arī 96.–97. apsvērumu.

([175]) Sk. Ombuda mehānisma (III pielikums) 2. punkta c) apakšpunktu. Saskaņā ar ASV valdības sniegtajiem skaidrojumiem PPBPP nepārtraukti jāpārskata par pretterorismu atbildīgo ASV iestāžu politikas virzieni un procedūras, kā arī to īstenošana, lai noteiktu, vai ar to darbībām "tiek pienācīgi aizsargāts privātums un pilsoniskās brīvības un tās atbilst likumiem, tiesību aktiem un politikas virzieniem, ar kuriem regulē privātumu un pilsoniskās brīvības". Tai arī būs "jāsaņem no privātuma inspektoriem un pilsonisko brīvību inspektoriem ziņojumi un cita informācija un jāpārskata tā un, ja nepieciešams, jāsniedz viņiem ieteikumi attiecībā uz viņu darbību".

sniegt personai pozitīvu atbildi (t.i., ka jebkāda neatbilstība ir novērsta) – kā ASV valdība ir to apņēmusies. Tāpat, īstenojot sadarbību, privātuma aizsardzību ombuds tiks informēts par izmeklēšanas iznākumu, un ombudam būs nepieciešamie līdzekļi, lai nodrošinātu, ka tas saņem visu informāciju, kas vajadzīga atbildes sagatavošanai.

(121) Visbeidzot, privātuma vairoga ombuds būs neatkarīgs, tādēļ uz viņu neattieksies ASV izlūkdienestu norādījumi ([176]). Tam ir liela nozīme, ņemot vērā to, ka ombudam būs "jāapstiprina", ka i) sūdzība ir pienācīgi izmeklēta un ka ii) ir ievēroti attiecīgie ASV tiesību akti – tostarp jo īpaši ierobežojumi un aizsardzības pasākumi, kas izklāstīti VI pielikumā – vai ir novērsts pārkāpums neatbilstības gadījumā. Lai varētu sniegt šādu neatkarīgu apstiprinājumu, privātuma vairoga ombudam būs jāiegūst nepieciešamā informācija par izmeklēšanu, lai izvērtētu atbildes uz sūdzību precizitāti. Turklāt valsts sekretārs ir apņēmies nodrošināt, ka privātuma aizsardzību ombuda funkcijas valsts sekretāra vietnieks veiks objektīvi un neatkarīgi no jebkādas neatbilstošas ietekmes, kas varētu ietekmēt sniedzamo atbildi.

(122) Kopumā šis mehānisms nodrošina, ka personu sūdzības tiks rūpīgi izmeklētas un atrisinātas un ka vismaz novērošanas jomā tiks iesaistītas neatkarīgas pārraudzības struktūras, kam ir nepieciešamā zinātība un izmeklēšanas pilnvaras, un ombuds, kas spēs pildīt savas funkcijas, būdams brīvs no neatbilstošas un jo īpaši politiskās ietekmes. Turklāt personas varēs iesniegt sūdzības un tām nebūs jāpierāda vai būs tikai jāsniedz norādes par to, ka tās ir bijušas novērošanas objekts ([177]). Ņemot vērā šos elementus, Komisija uzskata, ka pastāv atbilstīgas un efektīvas garantijas pret ļaunprātīgu izmantošanu.

(123) Pamatojoties uz iepriekš minēto, Komisija secina, ka Amerikas Savienotās Valstis nodrošina efektīvu tiesisko aizsardzību pret tās izlūkošanas iestāžu iejaukšanos to personu pamattiesībās, kuru dati ES un ASV privātuma vairoga ietvaros tiek nosūtīti no Savienības uz Amerikas Savienotajām Valstīm.

(124) Šajā sakarā Komisija ņem vērā Tiesas spriedumu *Schrems* lietā, saskaņā ar kuru "tiesiskajā regulējumā, kurā indivīdiem nav paredzētas nekādas iespējas likt lietā tiesību aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panākt šādu datu labošanu vai dzēšanu, nav ņemta vērā Pamattiesību hartas 47. pantā iedibināto pamattiesību uz efektīvu aizsardzību tiesā būtība." ([178]) Komisijas izvērtējumā ir apstiprināts, ka Amerikas Savienotajās Valstīs ir nodrošināti šādi tiesiskās aizsardzības līdzekļi, tostarp ieviešot ombuda mehānismu. Ombuda mehānisms paredz neatkarīgas pārraudzības un izmeklēšanas pilnvaras. Tā kā Komisija pastāvīgi uzraudzīs privātuma vairogu, tostarp sagatavojot ikgadēju kopēju pārskatu, kurā vērtēs arī obmudu, arī šā mehānisma efektivitāte tiks vērtēta no jauna.

3.2. *Piekļuve datiem un to izmantošana ASV valsts iestādēs tiesībaizsardzības un valsts interešu nolūkos*

(125) Attiecībā uz iejaukšanos ES un ASV privātuma vairoga ietvaros pārsūtītajos personas datos tiesībaizsardzības nolūkos, ASV valdība (Tieslietu ministrijas vārdā) ir sniegusi apstiprinājumu par piemērojamajiem ierobežojumiem un aizsardzības pasākumiem, kas Komisijas izvērtējumā liecina par pienācīgu aizsardzības līmeni.

([176]) Sk. lietu *Roman Zakharov v. Russia*, 2015. gada 4. decembra spriedums (virspalāta), pieteikums Nr. 47143/06, 275. punkts ("lai gan principā ir vēlams pārraudzības kontroli uzticēt tiesnesim, iestāžu, kas nav tiesas, īstenotu pārraudzību var uzskatīt par saderīgu ar Konvenciju, ar nosacījumu, ka pārraudzības iestāde ir neatkarīga no iestādes, kas veic novērošanu, un tai ir piešķirtas pietiekamas un efektīvas pārraudzības pilnvaras.").

([177]) Sk. *Kennedy v. the United Kingdom*, 2010. gada 18. maija spriedums, pieteikums Nr. 26839/05, 167. punkts.

([178]) *Schrems*, 95. punkts Kā izriet no sprieduma 91., 96., punkta, 95. punkts attiecas uz aizsardzības līmeni, kas garantēts Savienības tiesību sistēmā, kam "būtībā līdzvērtīgam" ir jābūt aizsardzības līmenim trešā valstī. Saskaņā ar sprieduma 73. un 74. punktā, tas nepieprasa, ka aizsardzības līmenim vai līdzekļiem, ko trešā valsts izmanto, jābūt identiskiem, lai gan izmantojamiem līdzekļiem praksē ir jāizrādās efektīviem.

(126) Saskaņā ar šo informāciju atbilstīgi ASV Konstitūcijas ceturtajam labojumam ([179]) tiesībaizsardzības iestāžu veiktām kratīšanām un mantas arestam principā ([180]) ir nepieciešams tiesas rīkojums, norādot "ticamu iemeslu". Dažos īpaši noteiktos izņēmuma gadījumos, kad rīkojuma prasība netiek piemērota ([181]), tiesībaizsardzībai piemēro "saprātīguma" pārbaudi ([182]). To, vai kratīšana un mantas arests ir saprātīgs, "nosaka, izvērtējot, no vienas puses, kādā mērā tas pārkāpj personas privātumu, un, no otras puses, kādā mērā tas ir nepieciešams, lai sekmētu likumīgas valdības intereses" ([183]). Runājot plašākā kontekstā, ceturtais labojums garantē privātumu, cieņu un aizsargā pret valdības amatpersonu patvaļīgu un uzbrūkošu rīcību ([184]). Šīs koncepcijas iemieso ideju par Savienības tiesību nepieciešamību un proporcionalitāti. Pēc tam, kad tiesībaizsardzības iestādēm vairs nav nepieciešams izmantot izņemtās lietas kā pierādījumu, tās būtu jāatdod ([185]).

(127) Lai arī ceturtā labojuma tiesības neattiecas uz citu valstu personām, kas nedzīvo Amerikas Savienotajās Valstīs, tomēr šīs personas netieši gūst labumu no minētā grozījuma aizsardzības, ņemot vērā to, ka personas datus glabā ASV uzņēmumi, tādējādi tiesībaizsardzības iestādēm jebkurā gadījumā ir jāsaņem tiesas atļauja (vai vismaz jāievēro uz saprātīguma prasība) ([186]). Papildu aizsardzību nodrošina īpašas ar likumu noteiktas iestādes, kā arī Tieslietu ministrijas pamatnostādnes, kas ierobežo tiesībaizsardzības iestāžu piekļuvi datiem, pamatojoties uz nepieciešamību un proporcionalitāti (piemēram, pieprasot FIB izmantot visneuzbāzīgākās iespējamās izmeklēšanas metodes, ņemot vērā ietekmi uz privāto dzīvi un pilsoniskajām brīvībām) ([187]). Saskaņā ar ASV valdības apgalvojumiem tāda pati vai lielāka aizsardzība ir piemērojama tiesībaizsardzības iestāžu veiktai izmeklēšanai štata līmenī (attiecībā uz izmeklēšanu, ko veic saskaņā ar štata likumiem) ([188]).

(128) Lai arī iepriekšēja tiesas vai zvērināto (personu grupa tiesā [pierādījumu] izvērtēšanai, kuru ieceļ tiesnesis vai izmeklēšanas tiesnesis) atļauja nav nepieciešama visos gadījumos ([189]), administratīvās pavēstes var sūtīt tikai konkrētās lietās un tām būs nepieciešama neatkarīga pārbaude tiesā vismaz tajos gadījumos, kad tiesā prasītājs ir valdība ([190]).

([179]) Saskaņā ar ceturto labojumu "[n]av pārkāpjamas cilvēku tiesības uz personas aizsardzību, viņu māju, dokumentu un īpašuma aizsardzību no nepamatotām kratīšanām un aresta. Kratīšanas un aresta orderi var izdot tikai pietiekami pamatotā gadījumā, ko apstiprina zvērests vai svinīgs solījums. Šādā orderī jābūt kratīšanas vietas un arestējamās personas vai mantas sīkam aprakstam." Kratīšanas orderus var izdot tikai izmeklēšanas tiesneši. Federālos orderus par elektroniski uzglabātas informācijas kopēšanu sīkāk reglamentē Federālā krimināprocesa 41. noteikums.

([180]) Augstākā Tiesa atkārtoti ir uzsvērusi, ka pārmeklējumi bez ordera ir "izņēmums". Sk., piemēram, *Johnson v. United States, 333 U.S. 10, 14 (1948)*; *McDonald v. United States, 335 U.S. 451, 453 (1948)*; *Camara v. Municipal Court, 387 U.S. 523, 528-29 (1967)*; *G.M. Leasing Corp. v. United States, 429 U.S. 338, 352-53, 355 (1977)*. Tāpat Augstākā Tiesa regulāri uzsver, ka "šajā jomā galvenais konstitucionālais noteikums ir tāds, ka kratīšanas, kas nav veiktas tiesvedības ietvaros un īstenotas bez tiesneša vai izmeklēšanas tiesneša iepriekšēja apstiprinājuma, saskaņā ar ceturto labojumu – pašas par sevi ir nepamatotas, un pastāv tikai daži konkrēti noteikti un precīzi aprakstīti izņēmumi." Sk., piemēram, *Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971)*; *G.M. Leasing Corp. v. United States, 429 U.S. 338, 352-53, 358 (1977)*.

([181]) *City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010)*.

([182]) PPPBPP, ziņojuma 215. sadaļa, 107. lpp., attiecībā uz*Maryland/King, 133 S. Ct. 1958, 1970 (2013)*.

([183]) PPPBPP, ziņojuma 215. sadaļa, 107. lpp., attiecībā uz*Samson v. California, 547 U.S. 843, 848 (2006)*.

([184]) *City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010), 2627*.

([185]) Sk., piemēram, *United Sates v Wilson, 540 F.2d 1100 (D.C. Cir. 1976)*.

([186]) Sk. lietu *Roman Zakharov v. Russia*, 2015. gada 4. decembra spriedums (virspalāta), pieteikums Nr. 47143/06, 269. punkts, saskaņā ar kuru "prasība, ka [tiesībaizsardzības iestādei] ir jāuzrāda pārtveršanas atļauja sakaru pakalpojumu sniedzējam, pirms tiek saņemta piekļuve personas saziņai, ir viens no būtiskajiem aizsardzības līdzekļiem pret ļaunprātīgu izmantošanu no tiesībaizsardzības iestāžu puses, tādējādi nodrošinot, ka tiek saņemta atbilstoša atļauja visos [datu] pārtveršanas gadījumos."

([187]) Tieslietu ministrijas apgalvojumi (VII pielikums), 4. lpp. ar turpmākām atsaucēm.

([188]) Tieslietu ministrijas apgalvojumi (VII pielikums), 2. lpp.

([189]) Saskaņā ar Komisijas saņemto informāciju, un neņemot vērā atsevišķas jomas, kas visdrīzāk neattiecas uz datu pārsūtīšanu ES un ASV privātuma vairoga ietvaros (piemēram, izmeklēšana lietās saistībā ar krāpniecību veselības aprūpes nozarē, vardarbīgu izturēšanās pret bērnu vai kontrolējamām vielām), tas galvenokārt attiecas uz konkrētām iestādēm atbilstīgi Elektroniskās saziņas privātuma likumam (LESP), proti, pamatinformācijas par abonentiem, savienojumiem un rēķiniem (*18 U.S.C. § 2703(c)(1), (2)*, piem., adrese, pakalpojuma veids/ilgums) pieprasījumiem un elektronisko vēstuļu, kas vecākas par 180 dienām, satura pieprasījumiem (*18 U.S.C. § 2703(a), (b)*). Taču pēdējā gadījumā attiecīgajai personai ir jābūt informētai, tādēļ tai ir iespēja apstrīdēt pieprasījumu tiesā. Sk. arī Tieslietu ministrijas pārskatu *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 3. nodaļa: *The Stored Communications Act*, 115.–138. lpp.

([190]) Saskaņā ar ASV valdības apgalvojumiem administratīvo pavēstu saņēmēji var apstrīdēt tās tiesā kā nepamatotas, t. i., pārmērīgas, represīvas vai apgrūtinošas. Sk. Tieslietu ministrijas apgalvojumus (VII pielikums), 2. lpp.

(129) Tas pats attiecas uz administratīvo pavēstu izmantošanu valsts interešu nolūkos. Turklāt saskaņā ar AS valdības apgalvojumiem līdzīgi būtiski ierobežojumi ir piemērojami tam, ka aģentūras var pieprasīt piekļuvi datiem, kas attiecas uz lietām to kompetencē, un tām ir jāievēro saprātīguma standarts.

(130) Turklāt ASV tiesību aktos personām ir paredzētas vairākas tiesiskās aizsardzības iespējas, lai vērstos pret valsts iestādi vai kādu no tās ierēdņiem, ja šīs iestādes apstrādā personas datus. Šie risinājumi, jo īpaši Administratīvā procesa likums (APA), Likums par informācijas brīvību (LIB) un Elektroniskās saziņas privātuma likums (LESP), ir pieejami visām personām neatkarīgi no viņu valstspiederības un ievērojot visus piemērojamos nosacījumus.

(131) Parasti ar Administratīvā procesa likumu ([191])"jebkurai personai, kam nodarīta juridiska netaisnība aģentūras darbības rezultātā vai ko nelabvēlīgi ietekmē vai neapmierina aģentūras darbība", ir tiesības vērsties tiesā ([192]). Tas ietver iespēju lūgt tiesu "apturēt nelikumību un atcelt aģentūras darbību, konstatējumus un secinājumus, kas atzīti par […] patvaļīgiem, nepamatotiem, pieņemtiem, ļaunprātīgi izmantojot dienesta stāvokli, vai citādi pretrunā ar tiesību aktiem" ([193]).

(132) Konkrēti, Elektroniskās saziņas privātuma likuma ([194]) II sadaļā ir izklāstīta obligāto privātuma tiesību sistēma un tādējādi reglamentēta tiesībaizsardzības iestāžu piekļuve pa vadiem pārraidītas, mutiskas vai elektroniskas saziņas saturam, kura ierakstus glabā pakalpojumu sniedzēji – trešās personas ([195]). Tajā paredzēta krimināltiesību pārkāpums par nelikumīgu (t. i., bez tiesas atļaujas vai kā citādi neatļautu) piekļuvi šādai saziņai un noteikti tiesību aizsardzības iespējas skartajai personai: pret valdības amatpersonu, kas ir apzināti izdarījusi šādas nelikumīgas darbības, vai pret Amerikas Savienotajām Valstīm iesniegt ASV federālajā tiesā civilprasību par faktisko zaudējumu atlīdzināšanu un zaudējumu atlīdzību ar sodošu raksturu, kā arī par taisnīgu vai skaidrojošu spriedumu.

(133) Tāpat saskaņā ar Likumu par informācijas brīvību (LIB) (*5 U.S.C. § 552*) ikvienai personai ir tiesības iegūt piekļuvi federālās aģentūras reģistriem, un pēc administratīvo līdzekļu izmantošanas, pieprasīt šādu tiesību īstenošanu tiesā, izņemot gadījumus, kad šādi ieraksti ir aizsargāti pret izpaušanu sabiedrībai izņēmuma kārtā vai ar īpašu izslēgšanu tiesībaizsardzības nolūkos ([196]).

([191]) 5. sadaļas 702. iedaļa.

([192]) Parasti tiesā var vērsties tikai par aģentūras "galīgo darbību", nevis "iepriekšēju, procesuālu vai starpposma" aģentūras darbību. Sk. *5 U.S.C. § 704*.

([193]) *5 U.S.C. § 706(2)(A)*.

([194]) *18 U.S.C. §§ 2701-2712*.

([195]) ECPA aizsargā saziņu, ko nodrošina divu definētu kategoriju pakalpojumu sniedzēji, proti, kas sniedz: i) elektronisko komunikāciju pakalpojumus, piemēram, telefonija vai e-pasts; ii) attālinātos datošanas pakalpojumus, piemēram, elektronisko informācijas nesēju vai apstrādes pakalpojumi.

([196]) Šāda izslēgšana tomēr ir regulēta. Piemēram, saskaņā ar 5 U.S.C. § 552 (b)(7) LIB tiesības ir izslēgtas attiecībā uz "tiesībaizsardzības nolūkos apkopotu dokumentāciju vai informāciju, taču tikai tiktāl, ciktāl šādas tiesībaizsardzības nolūkos apkopotu dokumentācijas vai informācijas sagatavošanu A) varētu būt pamatoti uzskatāma par izpildes procedūru traucējumu, B) atņemtu personai tiesības uz taisnīgu tiesu vai objektīvu iztiesāšanu, C) varētu būt pamatoti uzskatāma par nelikumīgu iejaukšanos personas privātajā dzīvē, D) varētu būt pamatoti uzskatāma par konfidenciāla avota (tostarp valsts, vietējas vai ārvalstu aģentūras vai iestādes vai jebkuras privātas iestādes, kas sniegusi informāciju kā konfidenciālu) identitātes atklāšanu, un gadījumā, kad dokumentāciju vai informāciju apkopojusi krimināltiesību aizsardzības iestāde, veicot izziņu kriminālprocesā, vai aģentūra, kas veic izlūkošanas valsts drošības nolūkos likumīgu izmeklēšanu – konfidenciāla avota sniegtas informācijas izpaušanu, E) izpaustu tiesībaizsardzības iestāžu izmeklēšanas vai kriminālprocesa virzītāju metodes procedūras, vai izpaustu tiesībaizsardzības iestāžu izmeklēšanas vai kriminālprocesa virzītāju pamatnostādnes, ja šāda izpaušana varētu būt pamatoti uzskatāma par tādu, kas rada risku likuma apiešanai, vai F) varētu būt pamatoti uzskatāma par apdraudējumu jebkuras personas dzīvībai vai fiziskai drošībai." Tāpat "[k]atru reizi, kas tiek iesniegts pieprasījums saistībā ar piekļuvi dokumentācijai, [kā sagatavošana varētu būt pamatoti uzskatāma par izpildes procedūru traucējumu] un – A) izmeklēšana vai process ir saistīts ar iespējamu krimināltiesību pārkāpumu; un B) ir iemesls uzskatīt, ka i) izmeklēšanas vai procesa subjekts nav informēts par to norisi, un ii) dokumentācijas esamības izpaušana varētu būt pamatoti uzskatāma par izpildes procedūru traucējumu, aģentūra var tikai laikposmā, kamēr turpinās minētie apstākļi, rīkoties ar dokumentāciju tā, it kā uz to neattiecas šīs sadaļas prasības." (*5 U.S.C. § 552 (c)(1)*).

(134) Turklāt vairākos tiesību aktos personām ir piešķirtas tiesības celt tiesā prasību pret ASV valsts iestādi vai amatpersonu attiecībā uz personas datu apstrādi, piemēram, Likumā par telefona sarunu noklausīšanos (*Wiretap Act*) ([197]), Likumā par datorkrāpšanu un ļaunprātīgu izmantošanu (*Computer Fraud and Abuse Act*) ([198]), Federālajā likumā par noteiktiem atlīdzināmiem kaitējumiem (*Federal Torts Claim Act*) ([199]), Likumā par tiesībām uz finanšu datu aizsardzību (*Right to Financial Privacy Act*) ([200]), un Likumā par godīgu kredītinformāciju (*Fair Credit Reporting Act*) ([201]).

(135) Tādēļ Komisija secina, ka Amerikas Savienotajās Valstīs ir noteikumi, kas paredzēti, lai ierobežotu iejaukšanos tiesībaizsardzības ([202]) vai citu valsts interešu nolūkos to personu pamattiesībās, kuru personas dati tiek nosūtīti no Savienības uz Amerikas Savienotajām Valstīm ES un ASV privātuma vairoga ietvaros, līdz tādam līmenim, kas ir absolūti nepieciešams, lai sasniegtu attiecīgo likumīgo mērķi, un tādējādi tie nodrošina efektīvu tiesisko aizsardzību pret šādu iejaukšanos.

4. PIENĀCĪGS AIZSARDZĪBAS LĪMENIS ES UN ASV PRIVĀTUMA VAIROGA IETVAROS

(136) Ņemot vērā minētos konstatējumus, Komisija uzskata, ka Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni personas datiem, kas ES un ASV privātuma vairoga ietvaros no Savienības tiek nosūtīti organizācijām Amerikas Savienotajās Valstīs.

(137) Jo īpaši Komisija uzskata, ka ASV Tirdzniecības ministrijas izdotie principi kopumā nodrošina tādu personas datu aizsardzības līmeni, kas ir būtībā ekvivalents tam, kādu nodrošina ar Direktīvā 95/46/EK noteiktajiem būtiskajiem pamatprincipiem.

(138) Turklāt efektīvu principu piemērošanu garantē pārredzamības prasības un privātuma vairoga pārvaldība, ko veic Tirdzniecības ministrija.

(139) Turklāt Komisija uzskata, ka kopumā ar privātuma vairogu nodrošinātā pārraudzība un tiesību aizsardzības mehānismi ļauj apzināt un praksē sodīt privātuma vairoga principu pārkāpumus un piedāvāt datu subjektam tiesiskās aizsardzības līdzekļus, kas ļauj piekļūt ar viņu saistītiem personas datiem un galu galā panākt šādu datu labošanu vai dzēšanu.

(140) Visbeidzot, pamatojoties uz pieejamo informāciju par ASV tiesību sistēmu, tostarp ASV valdības apgalvojumiem un saistībām, Komisija uzskata, ka jebkāda ASV valsts iestāžu iejaukšanās to personu pamattiesībās, kuru dati privātuma vairoga ietvaros no Savienības tiek nosūtīti uz Amerikas Savienotajām Valstīm, ja tas notiek valsts drošības, tiesībaizsardzības vai citu valsts interešu nolūkos, un sekojošie ierobežojumi, kas piemēroti pašsertificētām organizācijām attiecībā uz to principialitāti, būs ierobežoti līdz tādam apmēram, kas ir absolūti nepieciešams, lai sasniegtu attiecīgo likumīgo mērķi, un tādējādi tie nodrošina efektīvu tiesisko aizsardzību pret šādu iejaukšanos.

([197]) *18 U.S.C. §§ 2510* un turpm. Saskaņā ar Likumu par telefona sarunu noklausīšanos (*18 U.S.C. § 2520*) persona, kuras pa vadiem pārraidīta, mutiska vai elektroniska saziņa ir pārtverta, izpausta vai ar nolūku izmantota, var celt prasību par Likuma par telefona sarunu noklausīšanos pārkāpšanu, tostarp konkrētos apstākļos pret atsevišķu valsts amatpersonu vai Amerikas Savienotajām Valstīm. Adrešu un citas ar saturu nesaistītas informācijas (piem., IP adrese, saņēmēja/sūtītāja e-pasta adrese) vākšanai, skatīt arī 18. nodaļas sadaļu "Zvanīto numuru reģistrētāji un uztveršanas un trasēšanas ierīces" (*Pen Registers and Trap and Trace Devices*) (*18 U.S.C. §§ 3121-3127 un civilprasībai – § 2707*).

([198]) *18 U.S.C. § 1030*. Saskaņā ar Likumu par datorkrāpšanu un ļaunprātīgu izmantošanu, persona var celt prasību pret jebkuru personu par tīšu neatļautu piekļuvi (vai pārsniegtu atļauto piekļuvi), lai iegūtu informāciju no finanšu iestādes, ASV valdības datorsistēmas vai cita konkrēti noteikta datora, tostarp konkrētos apstākļos prasību var celt pret atsevišķu valsts amatpersonu.

([199]) *28 U.S.C. §§ 2671* un turpm. Saskaņā ar Federālo likumu par noteiktiem atlīdzināmiem kaitējumiem, persona konkrētos apstākļos var celt prasību pret Amerikas Savienotajām Valstīm attiecībā uz "jebkura valsts iestādes darbinieka nolaidīgu vai nelikumīgu darbību vai bezdarbību, pildot amata vai darba pienākumus."

([200]) *12 U.S.C. §§ 3401* un turpm. Saskaņā ar Likumu par tiesībām uz finanšu datu aizsardzību, persona konkrētos apstākļos var celt prasību pret Amerikas Savienotajām Valstīm attiecībā uz aizsargātu finanšu datu pretlikumīgu iegūšanu vai izpaušanu. Valdības piekļuve aizsargātiem finanšu datiem parasti ir aizliegta, izņemot gadījumu, kad valdība iesniedz pieprasījumu saskaņā ar likumīgu tiesas pavēsti vai kratīšanas orderi vai – ar ierobežojumiem – oficiālu rakstveida pieprasījumu, un persona, kuras informācija ir pieprasīta, saņem paziņojumu par šādu pieprasījumu.

([201]) *15 U.S.C. §§ 1681-1681x*. Saskaņā ar Likumu par godīgu kredītinformāciju persona var celt prasību pret jebkuru personu, kas neizpilda prasības (jo īpaši attiecībā uz likumīgu atļauju), attiecībā uz patērētāja kredītinformācijas izplatīšanu un izmantošanu, vai arī konkrētos apstākļos prasību var celt pret valdības aģentūru.

([202]) Tiesa ir atzinusi, ka tiesībaizsardzība ir likumīgs politikas mērķis. Sk. apvienotās lietas C-293/12 un C-594/12, *Digital Rights Ireland un citi*, EU:C:2014:238, 42. punkts. Sk. arī Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas (ECTK) 8. panta 2. punktu un Eiropas Cilvektiesību tiesas spriedumu lietā *Weber and Saravia v. Germany*, Pieteikums Nr. 54934/00, 104. punkts

(141) Komisija secina, ka tas atbilst Direktīvas 95/46/EK 25. panta standartiem, kas interpretēti atbilstoši Eiropas Savienības Pamattiesību hartai, kā to skaidrojusi Tiesa jo īpaši spriedumā *Schrems* lietā.

5. DATU AIZSARDZĪBAS IESTĀŽU RĪCĪBA UN INFORMĀCIJA KOMISIJAI

(142) Spriedumā *Schrems* lietā Tiesa precizēja, ka Komisijas kompetencē nav ierobežot DAI pilnvaras, kas noteiktas Direktīvas 95/46/EK 28. pantā (tostarp pilnvaras pārtraukt datu pārsūtīšanu), ja persona, ceļot prasību saistībā ar šo nosacījumu, apšauba Komisijas atbilstības lēmuma saderību ar pamattiesību aizsardzību attiecībā uz privātumu un datu aizsardzību ([203]).

(143) Lai efektīvi pārraudzītu privātuma vairoga darbību, dalībvalstīm būtu jāinformē Komisija par attiecīgo DAI rīcību.

(144) Turklāt Tiesa uzskatīja, ka saskaņā ar Direktīvas 95/46/EK 25. panta 6. punkta otro daļu dalībvalstis un to iestādes veic nepieciešamos pasākumus, lai izpildītu Savienības institūciju tiesību aktus, jo tie principā tiek uzskatīti par likumīgiem un attiecīgi paredz tiesiskās sekas līdz brīdim, kad tiek atcelti, anulēti saskaņā ar prasību atcelt tiesību aktu vai pasludināti par spēkā neesošiem pēc lūguma sniegt prejudiciālu nolēmumu vai iebildes par prettiesiskumu. Tādējādi Komisijas atbilstības lēmums, kas pieņemts saskaņā ar Direktīvas 95/46/EK 25. panta 6. punktu, ir saistošs visām dalībvalstu iestādēm, kurām tas ir adresēts, tostarp to neatkarīgajām uzraudzības iestādēm ([204]). Ja šāda iestāde ir saņēmusi sūdzību, ar kuru tiek apšaubīta Komisijas atbilstības lēmuma saderība ar pamattiesību aizsardzību attiecībā uz privātumu un datu aizsardzību un kurā izvirzītie iebildumi ir labi pamatoti, valsts tiesībās ir jāparedz tiesiskā aizsardzība, lai šos iebildumus virzītu izskatīšanai valsts tiesā, kurai šaubu gadījumā jāaptur tiesvedība un jāatsaucas uz Tiesas prejudiciālu nolēmumu ([205]).

6. KONSTATĒJUMA PAR ATBILSTĪBU PERIODISKA PĀRSKATĪŠANA

(145) Ņemot vērā faktu, ka ar ASV tiesību sistēmu nodrošinātais aizsardzības līmenis var mainīties, Komisija pēc šā lēmuma pieņemšanas periodiski pārbaudīs, vai konstatējumi par aizsardzības līmeņa atbilstību, ko nodrošina ES un ASV privātuma vairogs, joprojām ir faktiski un juridiski pamatoti. Šāda pārbaude ir nepieciešama katru reizi, kad Komisija saņem jebkādu informāciju, kas rada pamatotas bažas par to ([206]).

(146) Tādēļ Komisija nepārtraukti pārraudzīs vispārējo sistēmu personas datu pārsūtīšanai, kas izveidota ES un ASV privātuma vairoga ietvaros, kā arī to, vai ASV iestādes ievēro apgalvojumus un saistības, kas iekļautas šim lēmumam pievienotajos dokumentos. Lai atvieglotu šo procesu, ASV ir apņēmušās informēt Komisiju par būtiskām izmaiņām ASV tiesību aktos, kad tas attieksies uz privātuma vairogu datu aizsardzības jomā, un ierobežojumiem un aizsardzības pasākumiem attiecībā uz valsts iestāžu piekļuvi personas datiem. Turklāt par šo lēmumu veiks ikgadēju kopēju pārskatu, kas aptvers visus ES un ASV privātuma vairoga darbības aspektus, tostarp principu valsts drošības un tiesībaizsardzības izņēmumu darbību. Turklāt, tā kā konstatējumu par atbilstību var ietekmēt arī juridiskās izmaiņas Savienības tiesību aktos, Komisija izvērtēs privātuma vairoga sniegto aizsardzības līmeni pēc tam, kad stāsies spēkā vispārīgā datu aizsardzības regula.

(147) Lai izstrādātu I, II un VI pielikumā minēto ikgadējo kopējo pārskatu, Komisija tiksies ar Tirdzniecības ministriju un FTK, piedaloties, ja nepieciešams, citiem departamentiem un aģentūrām, kas iesaistījušās privātuma vairoga pasākumu īstenošanā, kā arī, attiecībā uz jautājumiem saistībā ar valsts drošību – NIDB pārstāvjiem, citiem izlūkdienestu elementu pārstāvjiem un ombudu. Šo tikšanos varēs apmeklēt ES DAI un 29. panta darba grupa.

([203]) *Schrems*, 40. un turpmākie punkti, 101.–103. punkts.
([204]) *Schrems*, 51., 52. un 62. punkts.
([205]) *Schrems*, 65. punkts.
([206]) *Schrems*, 76. punkts.

(148) Ikgadējā kopējā pārskata ietvaros Komisija pieprasīs Tirdzniecības ministrijai sniegt visaptverošu informāciju par visiem būtiskajiem aspektiem saistībā ar ES un ASV privātuma vairoga darbību, tostarp Tirdzniecības ministrijas no DAI saņemtās lietas izskatīšanai un pēc ministrijas iniciatīvas veikto atbilstības pārbaužu rezultātus. Komisija arī pieprasīs skaidrojumus saistībā ar jebkādiem jautājumiem vai lietām attiecībā uz ES un ASV privātuma vairogu un tā darbību, kas izriet no pieejamās informācijas, tostarp pārredzamības ziņojumiem, kuri atļauti saskaņā ar ASV Brīvības likumu, ASV nacionālās izlūkošanas iestāžu, DAI, privātuma grupu publiskajiem ziņojumiem, plašsaziņas līdzekļu ziņojumiem vai jebkura cita iespējama avota. Turklāt, lai sekmētu Komisijas uzdevumu šajā sakarā, dalībvalstīm būtu jāinformē Komisija par gadījumiem, kad tādu struktūru rīcība, kuras atbildīgas par privātuma principu ievērošanu Amerikas Savienotajās Valstīs, nenodrošina atbilstību, un par jebkādām norādēm uz to, ka par valsts drošību vai kriminālpārkāpumu novēršanu, izmeklēšanu, atklāšanu un sodīšanu atbildīgo ASV valsts iestāžu rīcība nenodrošina nepieciešamo aizsardzības līmeni.

(149) Pamatojoties uz ikgadējo kopējo pārskatu, Komisija sagatavos publisku ziņojumu, kas jāiesniedz Eiropas Parlamentam un Padomei.

7. **ATBILSTĪBAS LĒMUMA APTURĒŠANA**

(150) Ja, pamatojoties uz pārbaudēm vai jebkādu citu pieejamo informāciju, Komisija secina, ka privātuma vairoga sniegto aizsardzības līmeni vairs nevar uzskatīt par būtiski līdzvērtīgu Savienības sniegtajam aizsardzības līmenim, vai ja ir skaidras norādes uz to, ka Amerikas Savienotajās Valstīs vairs nav iespējams nodrošināt efektīvu privātuma principu ievērošanu vai ka par valsts drošību vai kriminālpārkāpumu novēršanu, izmeklēšanu, atklāšanu un sodīšanu atbildīgu ASV valsts iestāžu rīcība nenodrošina nepieciešamo aizsardzības līmeni, tā informē par to Tirdzniecības ministriju un pieprasa attiecīgu pasākumu īstenošanu, lai noteiktā, saprātīgā laikā ātri atrisinātu jebkādu iespējamu neatbilstību privātuma principiem. Ja pēc noteiktā laika ASV iestādes nespēj apmierinoši nodemonstrēt, ka ES un ASV privātuma vairogs turpina nodrošināt efektīvu atbilstību un pienācīgu aizsardzības līmeni, Komisija uzsāk procedūru, kuras rezultātā šīs lēmums tiek pilnībā vai daļēji apturēts vai atcelts ([207]). Komisija var arī ierosināt grozīt šo lēmumu, piemēram, ierobežojot konstatējuma par atbilstību tvērumu tikai attiecībā uz tādu datu nosūtīšanu, kurai piemēro papildu nosacījumus.

(151) Konkrēti, Komisija uzsāks apturēšanas vai atcelšanas procedūru, ja:

a) būs norādes par to, ka ASV iestādes neievēro apgalvojumus un saistības, kas iekļautas dokumentos, kuri pievienoti šim lēmumam, tostarp attiecībā uz nosacījumiem un ierobežojumiem ASV valsts iestāžu piekļuvei privātuma vairoga ietvaros pārsūtītajiem personas datiem tiesībaizsardzības, valsts drošības un citu valsts interešu nolūkos;

b) netiks efektīvi risinātas ES datu subjektu sūdzības; šajā ziņā Komisija ņems vērā visus apstākļus, kas ietekmēs iespēju ES datu subjektiem īstenot savas tiesības, tostarp, jo īpaši, pašsertificētu ASV uzņēmumu brīvprātīgu apņemšanos sadarboties ar DAI un ievērot to ieteikumus; vai

c) privātuma vairoga ombuds laikus un pienācīgi neatbildēs uz ES datu subjektu pieprasījumiem.

(152) Komisija izskatīs iespēju arī uzsākt procedūru, kā rezultātā šis lēmums tiks grozīts, apturēts vai atcelts, ja ES un ASV privātuma vairoga darbības ikgadējā kopīgā pārskata ietvaros vai citā veidā Tirdzniecības ministrija vai citi departamenti vai aģentūras, kas iesaistījušās privātuma vairoga īstenošanā, vai – attiecībā uz valsts drošības jautājumiem – ASV izlūkdienestu pārstāvji vai ombuds nesniegs informāciju vai skaidrojumus, kas nepieciešami, lai novērtētu atbilstību privātuma principiem, sūdzību izskatīšanas procedūru efektivitāti vai jebkādu

([207]) Ar Vispārīgās datu aizsardzības regulas piemērošanas dienu Komisija izmantos savas pilnvaras, lai, pamatojoties uz pienācīgi pamatotiem, nenovēršamiem steidzamības iemesliem, pieņemtu īstenošanas aktu, ar kuru apturēs esošo lēmumu un kurš stāsies spēkā nekavējoties, iepriekš neiesniedzot to attiecīgajai komitoloģijas komitejai, un būs spēkā ne ilgāk kā sešus mēnešus.

nepieciešamā aizsardzības līmeņa pazemināšanos saistībā ar ASV nacionālās izlūkošanas iestāžu rīcību, jo īpaši saistībā ar personas datu vākšanu un/vai piekļuvi tiem tādā apmērā, kas pārsniedz absolūti nepieciešamu un samērīgu. Šajā sakarā Komisija ņems vērā apmēru, kādā attiecīgo informāciju var iegūt no citiem avotiem, tostarp pašsertificētu ASV uzņēmumu ziņojumiem, kas atļauts ar ASV Brīvības likumu.

(153) Darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi, kas ir izveidota ar Direktīvas 95/46/EK 29. pantu, ir sniegusi atzinumus par aizsardzības līmeni, ko nodrošina ES un ASV privātuma vairogs ([208]), un tie ir ņemti vērā, sagatavojot šo lēmumu.

(154) Eiropas Parlaments pieņēma rezolūciju par transatlantiskajām datu plūsmām ([209]).

(155) Šajā lēmumā paredzētie pasākumi atbilst atzinumam, ko sniegusi komiteja, kura izveidota saskaņā ar Direktīvas 95/46/EK 31. panta 1. punktu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

1. Direktīvas 95/46/EK 25. panta 2. punkta izpratnē Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni personas datiem, kas ES un ASV privātuma vairoga ietvaros no Savienības tiek nosūtīti organizācijām Amerikas Savienotajās Valstīs.

2. ES un ASV privātuma vairogu veido principi, kurus ASV Tirdzniecības ministrija izdevusi 2016. gada 7. jūlijā, kas izklāstīti II pielikumā, un oficiālie apgalvojumi un saistības, kas iekļautas dokumentos I un III–VII pielikumā.

3. Šā panta 1. punkta īstenošanai personas dati tiek pārsūtīti ES un ASV privātuma vairoga ietvaros, ja tos no Savienības pārsūta Amerikas Savienoto Valstu organizācijām, kuras ir iekļautas "Privātuma vairoga sarakstā", ko uztur un publicē ASV Tirdzniecības ministrija saskaņā ar II pielikumā izklāstīto principu I un III sadaļu.

2. pants

Šis lēmums neietekmē to, kā tiek piemēroti Direktīvas 95/46/EK noteikumi, izņemot 25. panta 1. punktu, kas attiecas uz personas datu apstrādi dalībvalstīs, un jo īpaši tās 4. pants.

3. pants

Kad kompetentas iestādes dalībvalstī, lai pasargātu personas attiecībā uz viņu personas datu apstrādi, izmanto savas pilnvaras atbilstīgi Direktīvas 95/46/EK 28. panta 3. punktam, kā rezultātā tiek apturētas vai pilnībā aizliegtas datu plūsmas uz tādu organizāciju Amerikas Savienotajās Valstīs, kas ir iekļauta privātuma vairoga sarakstā saskaņā ar II pielikumā izklāstīto principu I un III sadaļu, attiecīgā dalībvalsts nekavējoties informē Komisiju.

4. pants

1. Komisija nepārtraukti uzraudzīs ES un ASV privātuma vairoga darbību ar mērķi novērtēt, vai Amerikas Savienotās Valstis tā ietvaros turpina nodrošināt no Savienības Amerikas Savienoto Valstu organizācijām pārsūtīto datu aizsardzību.

([208]) Atzinumu 01/2016 par projektu lēmumam par aizsardzības līmeņa pietiekamību attiecībā uz ES un ASV privātuma vairogu, pieņemts 2016. gada 13. aprīlī.
([209]) Eiropas Parlamenta 2016. gada 26. maija rezolūcija par transatlantiskajām datu plūsmām (2016/2727 (RSP)).

2. Dalībvalstis un Komisija informē viena otru par gadījumiem, kad tiek konstatēts, ka Amerikas Savienoto Valstu valdības struktūras ar likumā noteiktām pilnvarām nodrošināt atbilstību II pielikumā izklāstītajiem principiem nenodrošina efektīvus atklāšanas un uzraudzības mehānismus, kas ļauj apzināt un praksē sodīt principu pārkāpumus.

3. Dalībvalstis un Komisija informē viena otru par jebkādu norādi, kas liecina par to, ka ASV valsts iestāžu, kuras atbildīgas par valsts drošību, tiesībaizsardzību vai citām valsts interesēm, iejaukšanās personu tiesībās attiecībā uz personas datu aizsardzību pārsniedz absolūti nepieciešamo un/vai ka pret šādu iejaukšanos nav efektīvas tiesiskās aizsardzības.

4. Viena gada laikā pēc šā lēmuma paziņošanas dalībvalstīm un pēc tam reizi gadā Komisija novērtēs konstatējumu 1. panta 1. punktā, pamatojoties uz visu pieejamo informāciju, tostarp informāciju, kas saņemta I, II un VI pielikumā minētā ikgadējā kopīgā pārskata ietvaros.

5. Komisija par piemērotiem konstatējumiem ziņos komitejai, kas izveidota saskaņā ar Direktīvas 95/46/EK 31. pantu.

6. Komisija iesniegs pasākumu projektu saskaņā ar Direktīvas 95/46/EK 31. panta 2. punktā izklāstīto procedūru ar mērķi apturēt, grozīt vai atcelt šo lēmumu, vai ierobežot tā darbības jomu, ja, cita starpā, būs norādes:

— uz to, ka ASV valsts iestādes neievēro apgalvojumus un saistības, kas iekļautas šim lēmumam pievienotajos dokumentos, tostarp attiecībā uz nosacījumiem un ierobežojumiem ASV valsts iestāžu piekļuvei tiesībaizsardzības, valsts drošības un citu valsts interešu nolūkos ES un ASV privātuma vairoga ietvaros nosūtītajiem personas datiem,

— uz sistemātisku nespēju efektīvi risināt ES datu subjektu sūdzības, vai

— uz sistemātisku privātuma vairoga ombuda nespēju laikus un pienācīgi atbildēt uz ES datu subjektu pieprasījumiem saskaņā ar tā funkcijām, kas izklāstītas III pielikuma 4. punkta e) apakšpunktā.

Komisija iesniegs šādu pasākumu projektu arī tad, ja sadarbības trūkums starp struktūrām, kuras iesaistītas ES un ASV privātuma vairoga darbības Amerikas Savienotajās Valstīs nodrošināšanā, neļaus Komisijai noteikt, vai ir ietekmēts 1. panta 1. punkta konstatējums.

5. pants

Dalībvalstis veic nepieciešamos pasākumus, lai izpildītu šo lēmumu.

6. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2016. gada 12. jūlijā

Komisijas vārdā –
Komisijas locekle
Věra JOUROVÁ

I PIELIKUMS

Vēstule no ASV tirdzniecības ministres *Penny Pritzker*

2016. gada 7. jūlijs

Verai Jourovai,
tieslietu, patērētāju un dzimumu līdztiesības komisārei
Eiropas Komisija
Rue de la Loi/Westraat 200
1049 Brisele
Beļģija

Cienījamā komisāres kundze!

Amerikas Savienoto Valstu vārdā ar gandarījumu pārsūtu Jums ES un ASV privātuma vairoga materiālu paketi, kas ir izstrādāta divus gadus ilgās un rezultatīvās mūsu darba grupu apspriedēs. Kopā ar citiem materiāliem, kas Komisijai pieejami no publiskiem avotiem, šis materiālu kopums veido ļoti spēcīgu pamatu jaunam Eiropas Komisijas konstatējumam par aizsardzības līmeņa pietiekamību ([1]).

Mēs abas varam lepoties ar regulējuma uzlabojumiem. Privātuma vairoga pamatā ir principi, ko vienlīdz spēcīgi atbalsta abās Atlantijas okeāna pusēs, un mēs esam nostiprinājušas to darbību. Mums ir reāla iespēja, kopīgi strādājot uzlabot privātuma aizsardzību visā pasaulē.

Privātuma vairoga paketē ir izklāstīti vairoga principi un iekļauta vēstule (pievienota kā 1. pielikums) no Tirdzniecības ministrijas Starptautiskās tirdzniecības pārvaldes (STP), kas pārvalda programmas īstenošanu. Vēstulē ir aprakstītas saistības, ko mūsu ministrija uzņēmusies, lai nodrošinātu rezultatīvu privātuma vairoga darbību. Paketei ir arī 2. pielikums, kurā uzskaitītas citas Tirdzniecības ministrijas saistības attiecībā uz jauno privātuma vairoga satvarā pieejamo šķīrējtiesas modeli.

Esmu likusi saviem darbiniekiem veltīt visus resursus, kas vajadzīgi, lai ātri un pilnīgi īstenotu privātuma vairoga regulējumu un nodrošinātu 1. un 2. pielikumā uzskaitīto saistību savlaicīgu izpildi.

Privātuma vairoga paketē ietilpst arī citu ASV aģentūru sagatavoti dokumenti, piemēram:

— vēstule no Federālās tirdzniecības komisijas (FTK), kurā aprakstīts, kā tā panāk privātuma vairoga izpildi,

— vēstule no Transporta ministrijas, kurā aprakstīts, kā tā panāk privātuma vairoga izpildi,

— Nacionālās izlūkošanas direktora biroja (NIDB) sagatavotas divas vēstules par ASV valsts drošības iestādēm piemērojamiem aizsardzības pasākumiem un ierobežojumiem,

— vēstule no Valsts departamenta un pavadmemorands, kurā aprakstīta Valsts departamenta apņemšanās izveidot jaunu privātuma vairoga ombudu, kam varēs iesniegt jautājumus par ASV īstenoto sakaru izlūkošanas praksi, kā arī

— Tieslietu ministrijas sagatavota vēstule par aizsardzības pasākumiem un ierobežojumiem attiecībā uz ASV valdības piekļuvi datiem tiesībaizsardzības un sabiedrības interešu aizstāvības nolūkā.

Varat būt droša, ka Amerikas Savienotās Valstis uztver savas saistības nopietni.

([1]) Ar nosacījumu, ka Komisijas lēmumu par pienācīgu aizsardzību, kas noteikta ar ES un ASV privātuma vairogu piemēro Islandei, Lihtenšteinai un Norvēģijai, privātuma vairoga pakete attieksies gan uz Eiropas Savienību, gan uz šīm trim valstīm.

30 dienu laikā no brīža, kad tiks galīgi apstiprināts konstatējums par aizsardzības līmeņa pietiekamību, privātuma vairoga paketes pilnīgā versija tiks iesniegta publicēšanai *Federālajā reģistrā*.

Mēs labprāt ar Jums sadarbosimies, strādājot pie privātuma vairoga īstenošanas un kopīgi sākot šā procesa nākamo posmu.

Ar cieņu

Penny Pritzker

1. pielikums

Vēstule no Tirdzniecības ministra starptautiskās tirdzniecības jautājumos vietnieka pienākumu izpildītāja Ken Hyatt

Cien. Verai JOUROVAI,
tieslietu, patērētāju un dzimumu līdztiesības komisārei
Eiropas Komisija
Rue de la Loi/Westraat 200
1049 Brisele
Beļģija

Cienījamā komisāres kundze!

Starptautiskās tirdzniecības pārvaldes vārdā es labprāt aprakstīšu personas datu uzlaboto aizsardzību, ko nodrošina ES un ASV privātuma vairoga regulējums ("privātuma vairogs" vai "regulējums"), kā arī saistības, ko Tirdzniecības ministrija ("ministrija") uzņēmusies, lai nodrošinātu vairoga rezultatīvu darbību. Šīs vēsturiskās vienošanās satura pabeigšana ir būtisks sasniegums privātuma jomā un uzņēmumiem no abām Atlantijas okeāna pusēm. Privātuma vairogs sniedz ES fiziskām personām pārliecību, ka viņu datus aizsargās un ka viņām būs pieejami tiesiskās aizsardzības līdzekļi, ar ko reaģēt uz visām bažām. Šis regulējums rada noteiktību, kas palīdzēs izvērst transatlantisko ekonomiku, nodrošinot, ka tūkstošiem Eiropas un Amerikas uzņēmumu var turpināt ieguldījumus un uzņēmējdarbību otrpus mūsu robežām. Privātuma vairogs ir izstrādāts vairāk nekā divus gadus ilgā nopietnā darbā un sadarbībā ar Jums un kolēģiem no Eiropas Komisijas ("Komisija"). Mēs labprāt arī turpmāk strādāsim kopā ar Komisiju, lai gādātu, ka privātuma vairogs darbojas tā, kā paredzēts.

Kopīgi ar Komisiju esam izstrādājuši tādu privātuma vairogu, kas ļauj Amerikas Savienotajās Valstīs dibinātām organizācijām izpildīt ES tiesību aktos paredzētās prasības par datu aizsardzības līmeņa pietiekamību. Jaunais satvars sniegs vairākus būtiskus ieguvumus gan indivīdiem, gan uzņēmumiem. Pirmkārt, tas nodrošina ES fiziskām personām būtiskus datu privātuma aizsardzības pasākumus. Saskaņā ar regulējumu iesaistītajām ASV organizācijām ir jāizstrādā atbilstīga privātuma politika; publiski jāapņemas ievērot privātuma vairoga principi, lai saistības kļūtu izpildāmas atbilstīgi ASV tiesību aktiem; reizi gadā no jauna jāapliecina šo saistību izpilde ministrijai; jānodrošina ES fiziskām personām neatkarīga un bezmaksas strīdu izšķiršana un jādarbojas ASV federālās tirdzniecības komisijas ("FTK"), Transporta ministrijas ("TM") vai citas tiesībaizsardzības aģentūras pārraudzībā. Otrkārt, privātuma vairogs vairākiem tūkstošiem Amerikas Savienoto Valstu uzņēmumu un Eiropas uzņēmumu filiāļu, kas darbojas ASV, sniegs iespēju saņemt personas datus no Eiropas Savienības, lai atvieglotu transatlantiskajā tirdzniecībā nepieciešamās datu plūsmas. Transatlantiskās ekonomiskās attiecības jau patlaban ir lielākās saimnieciskās attiecības pasaulē un nodrošina pusi no pasaules ekonomikas rezultātiem un gandrīz vienu triljonu dolāru preču un pakalpojumu tirdzniecības izteiksmē, tādējādi uzturot vairākus miljonus darbavietu abpus Atlantijas okeānam. Transatlantiskās datu plūsmas izmanto visu rūpniecības nozaru uzņēmumi, un to vidū ir gan lielākie sarakstā Fortune 500 iekļautie uzņēmumi, gan daudzi mazie un vidējie uzņēmumi (MVU). Transatlantiskās datu plūsmas ļauj ASV organizācijām apstrādāt datus, kas vajadzīgi, lai piedāvātu preces, pakalpojumus un nodarbinātības iespējas Eiropas iedzīvotājiem. Privātuma vairogs atbalsta kopīgā privātuma principus, novēršot mūsu juridisko pieeju atšķirības un vienlaikus sekmējot gan Eiropas, gan Amerikas Savienoto Valstu tirdzniecības un ekonomisko mērķu īstenošanu.

Lai gan lēmumu pašsertificēt jaunā regulējuma īstenošanu uzņēmums varēs pieņemt brīvprātīgi, tiklīdz tas publiski apņemsies ievērot privātuma vairoga principus, tā saistību izpildi saskaņā ar ASV tiesību aktiem drīkstēs panākt vai nu Federālā tirdzniecības komisija, vai arī Transporta ministrija atkarībā no tā, kurai iestādei būs jurisdikcija attiecībā uz privātuma vairoga organizāciju.

Ar privātuma vairoga principiem panāktie uzlabojumi

Izstrādātais privātuma vairogs stiprina privātuma aizsardzību:

— nosakot, ka saskaņā ar informēšanas principu ir jāsniedz indivīdiem papildu informācija, arī paziņojums par organizācijas dalību privātuma vairoga programmā, paziņojums par indivīda tiesībām piekļūt personas datiem, kā arī norāde uz attiecīgo neatkarīgo strīdu izšķiršanas struktūru,

— nostiprinot to personas datu aizsardzību, kurus no privātuma vairoga organizācijas pārsūta datu pārzinim, kas ir trešā persona – pusēm ir jānoslēdz līgums, kurā noteikts, ka šādus datus drīkst apstrādāt vienīgi ierobežotos un precizētos nolūkos, kuri atbilst indivīda sniegtajai piekrišanai, un ka datu saņēmējs nodrošinās tādu pašu aizsardzības līmeni, kādu sniedz privātuma vairoga principi,

— nostiprinot to personas datu aizsardzību, ko no privātuma vairoga organizācijas pārsūta starpniekam, kas ir trešā persona, tostarp prasot privātuma vairoga organizācijai: veikt pamatotas un atbilstošas darbības, lai nodrošinātu, ka starpnieks apstrādā pārsūtīto personisko informāciju, ievērojot no principiem izrietošos organizācijas pienākumus; saņemot attiecīgu paziņojumu, veikt pamatotas un atbilstošas darbības, lai apturētu neatļautu apstrādi un koriģētu tās sekas; kā arī pēc ministrijas pieprasījuma iesniegt tai ar konkrēto starpnieku noslēgtā līguma attiecīgo privātuma noteikumu kopsavilkumu vai reprezentatīvu kopiju,

— nosakot, ka privātuma vairoga organizācija atbild par tās personiskās informācijas apstrādi, ko saņem privātuma vairoga satvarā un pēcāk pārsūta trešajai personai, kas tās vārdā rīkojas kā starpnieks, un ka saskaņā ar privātuma vairoga principiem šī organizācija ir atbildīga arī tad, ja tās starpnieks attiecīgo personisko informāciju apstrādā principiem neatbilstīgā veidā, ja vien organizācija nevar pierādīt, ka nav atbildīga par notikumu, kas izraisīja kaitējumu,

— precizējot, ka privātuma vairoga organizācijām jāaprobežojas vienīgi ar apstrādes nolūkiem nepieciešamo personisko informāciju,

— prasot, lai organizācija katru gadu apliecinātu ministrijai savu apņēmību piemērot principus informācijai, ko tā saņēma, kamēr piedalījās privātuma vairoga īstenošanā, ja tā no vairoga ir izstājusies un nolēmusi attiecīgos datus paturēt,

— prasot, lai indivīdiem bez maksas tiktu nodrošināti neatkarīgi tiesību aizsardzības mehānismi,

— prasot organizācijām un to izvēlētajiem neatkarīgajiem tiesību aizsardzības mehānismiem ātri atbildēt uz ministrijas jautājumiem un informācijas pieprasījumiem par privātuma vairogu,

— prasot organizācijām ātri atbildēt uz sūdzībām par atbilstību principiem, kuras ar ministrijas starpniecību iesniegušas ES dalībvalstu iestādes, kā arī

— prasot privātuma vairoga organizācijai publiskot visas Federālajai tirdzniecības komisijai iesniegtā atbilstības vai novērtējuma ziņojuma sadaļas, kas saistītas ar privātuma vairogu, ja organizācijai neatbilstības dēļ adresē FTK vai tiesas rīkojumu.

Privātuma vairoga programmas pārvaldība un uzraudzība, ko veic Tirdzniecības ministrija

Ministrija atkārtoti apņemas uzturēt un darīt pieejamu sabiedrībai to ASV organizāciju autoritatīvu sarakstu, kuras ir pašsertificējušās ministrijā un paziņojušas par apņemšanos stingri ievērot principus ("privātuma vairoga saraksts"). Ministrija regulāri atjauninās privātuma vairoga sarakstu, svītrojot no tā organizācijas, ja tās brīvprātīgi izstāsies no programmas, nebūs veikušas ikgadējo atkārtoto sertifikāciju atbilstīgi ministrijas procedūrām vai tiks konstatēts, ka tās pastāvīgi neievēro regulējumu. Ministrija arī uzturēs un darīs pieejamu sabiedrībai autoritatīvu reģistru, kurā uzskaitīs tās ASV organizācijas, kas iepriekš pašsertificējušās ministrijā, taču ir svītrotas no privātuma vairoga saraksta, tostarp tās organizācijas, kas svītrotas principu pastāvīgas neievērošanas dēļ. Ministrija norādīs katras organizācijas svītrošanas iemeslu.

Tā arīdzan apņemas stiprināt privātuma vairoga pārvaldību un uzraudzību. Ministrija jo īpaši veiks turpmāk aprakstītās darbības.

Papildu informācijas sniegšana privātuma vairoga tīmekļa vietnē:

— uzturēs privātuma vairoga sarakstu, kā arī to organizāciju reģistru, kas iepriekš pašsertificēja principu stingru ievērošanu, taču vairs nav tiesīgas saņemt no privātuma vairoga izrietošās priekšrocības,

— labi redzamā vietā iekļaus paziņojumu, kurā precizēs, ka visas no privātuma vairoga saraksta svītrotās organizācijas vairs nesaņem ar vairogu saistītās priekšrocības, tomēr tām jāturpina piemērot principus privātuma vairoga īstenošanas laikā saņemtajai personiskajai informācijai tik ilgi, kamēr tās šo informāciju glabā, kā arī

— iekļaus saiti uz FTK tīmekļa vietnē uzturēto sarakstu, kurā uzskaitītas ar privātuma vairogu saistītās FTK lietas.

Pašsertifikācijas prasību izpildes pārbaude:

— pirms organizācijas pašsertifikācijas (vai ikgadējās atkārtotās sertifikācijas) pabeigšanas un tās iekļaušanas privātuma vairoga sarakstā ministrija pārliecināsies, vai organizācija ir:

  — iesniegusi prasīto organizācijas kontaktinformāciju,

  — aprakstījusi organizācijas darbības, kas tiek īstenotas attiecībā uz personisko informāciju, kas saņemta no ES,

  — norādījusi, uz kādu personisko informāciju attiecas tās pašsertifikācija,

  — ja organizācijai ir publiska tīmekļa vietne, norādījusi tīmekļa adresi, kurā ir pieejama tās privātuma politika, un privātuma politikai attiecīgajā tīmekļa adresē var piekļūt, vai, ja organizācijai publiskas tīmekļa vietnes nav, tā ir norādījusi, kur sabiedrība var šo politiku apskatīt,

  — iekļāvusi attiecīgajā privātuma politikā paziņojumu, ka tā stingri ievēro principus un, ja privātuma politika ir pieejama tiešsaistē, ievietojusi hipersaiti uz ministrijas privātuma vairoga tīmekļa vietni,

  — norādījusi konkrētu oficiālo iestādi, kurai ir jurisdikcija uzklausīt visas pret organizāciju izvirzītās prasības par iespējami negodīgu vai maldinošu praksi un iespējamiem privātuma tiesību aktu vai noteikumu pārkāpumiem (un ka tā ir uzskaitīta principos vai to turpmākā pielikumā),

  — ja organizācija nolemj pildīt tiesību aizsardzības, izpildes panākšanas un atbildības principa a) punkta i) un iii) apakšpunktā uzskaitītās prasības, apņemoties sadarboties ar attiecīgajām ES datu aizsardzības iestādēm ("DAI"), ir norādījusi savu nodomu sadarboties ar DAI privātuma vairoga satvarā iesniegto sūdzību izmeklēšanā un risināšanā, jo īpaši atbildēt uz to jautājumiem, ja ES datu subjekti ir iesnieguši sūdzību tieši savas valsts DAI,

  — norādījusi kādu privātuma programmu, kuras dalībniece organizācija ir,

  — norādījusi metodi, ar ko tiek pārbaudīta principu ievērošana (piemēram, iekšēja pārbaude, trešās personas veikta pārbaude),

  — noteikusi – gan iesniegtajā pašsertifikācijas informācijā, gan tās privātuma politikā – neatkarīgo tiesību aizsardzības mehānismu, kas ir pieejams sūdzību izmeklēšanai un risināšanai,

  — attiecīgajā privātuma politikā, ja tā pieejama tiešsaistē, iekļāvusi hipersaiti uz tā neatkarīgā tiesību aizsardzības mehānisma tīmekļa vietni vai sūdzības iesniegšanas veidlapu, kas ir pieejams neatrisināto sūdzību izmeklēšanai, kā arī

  — ja organizācija ir norādījusi, ka tā grasās saņemt cilvēkresursu informāciju, ko no ES pārsūta izmantošanai saistībā ar darba attiecībām, paziņojusi, ka ir apņēmusies sadarboties ar DAI un izpildīt to prasības saistībā ar sūdzību par tās darbībām ar šādiem datiem risināšanu, iesniegusi ministrijai tās cilvēkresursu privātuma politikas kopiju un norādījusi, kur tās skartie darbinieki var privātuma politiku apskatīt,

— sadarbosies ar neatkarīgiem tiesību aizsardzības mehānismiem, lai pārliecinātos, ka organizācijas patiešām ir reģistrējušās iesniegtajā pašsertifikācijas informācijā norādītajā mehānismā, ja šāda reģistrācija ir nepieciešama.

No privātuma vairoga saraksta svītroto organizāciju uzraudzības centienu izvēršana:

— paziņos organizācijām, kas no privātuma vairoga saraksta svītrotas "pastāvīgas neatbilstības" dēļ, ka tās nav tiesīgas glabāt atbilstīgi privātuma vairogam savākto informāciju, kā arī

— nosūtīs anketas organizācijām, kuru pašsertifikācijas termiņš drīz beigsies vai kuras ir brīvprātīgi izstājušās no privātuma vairoga, lai noskaidrotu, vai organizācija atdos atpakaļ vai dzēsīs privātuma vairoga piemērošanas laikā saņemto personisko informāciju vai arī turpinās tai piemērot principus, un, ja personiskā informācija tiks glabāta, noskaidrotu, kas būs organizācijas pastāvīgais kontaktpunkts ar privātuma vairogu saistītajos jautājumos.

Nepatiesu apgalvojumu par dalību programmā meklēšana un reaģēšana uz šādiem apgalvojumiem:

— lai konstatētu visus nepatiesos apgalvojumus par dalību privātuma vairogā, ministrija pārbaudīs to organizāciju privātuma politiku, kuras ir iepriekš piedalījušās privātuma vairoga programmā, taču ir svītrotas no privātuma vairoga saraksta,

— ja organizācija: a) pārtrauc dalību privātuma vairoga programmā, b) atkārtoti neapliecina principu stingru ievērošanu vai c) tiek izslēgta no privātuma vairoga dalībnieku vidus galvenokārt "pastāvīgas neatbilstības" dēļ, pastāvīgi *ex officio* pārbaudīs, vai organizācija no publicētās privātuma politikas ir izdzēsusi visas atsauces uz privātuma vairogu, kuras norāda, ka organizācija tajā joprojām aktīvi piedalās un ir tiesīga saņemt izrietošās priekšrocības. Ministrija, konstatējot, ka šādas atsauces nav dzēstas, brīdinās organizāciju, ka, ja apgalvojumi par privātuma vairoga sertificēšanu tiks turpināti, tā vajadzības gadījumā informēs attiecīgo aģentūru un ierosinās izpildes panākšanas procesu. Ja organizācija nedzēsīs atsauces vai nepašsertificēs savu atbilstību privātuma vairogam, ministrija *ex officio* nodos lietu FTK, TM vai citai atbilstošai tiesībaizsardzības aģentūrai vai attiecīgā gadījumā rīkosies, lai panāktu privātuma vairoga sertifikācijas zīmes noteikumu izpildi,

— citādi centīsies konstatēt nepatiesus apgalvojumus par dalību privātuma vairogā un tā sertifikācijas zīmes neatbilstošu izmantošanu, tostarp veicot meklēšanu internetā, lai noskaidrotu, kur tiek attēloti privātuma vairoga sertifikācijas zīmes attēli un organizāciju privātuma politikā sniegtas atsauces uz privātuma vairogu,

— ātri reaģēs uz visām problēmām, ko konstatēs, ex officio uzraugot nepatiesus apgalvojumus par dalību un sertifikācijas zīmes ļaunprātīgu izmantošanu, tostarp brīdinās organizācijas, kas sagroza informāciju par savu dalību privātuma vairoga programmā, kā aprakstīts iepriekš,

— veiks citu atbilstošu korektīvu darbību, arī izmantos visus ministrijai atļautos tiesību aizsardzības līdzekļus un nodos lietas FTK, TM vai citai atbilstošai tiesībaizsardzības aģentūrai, kā arī

— ātri izskatīs saņemtās sūdzības par nepatiesiem apgalvojumiem par dalību un uz tām ātri reaģēs.

Lai rezultatīvāk konstatētu nepatiesus apgalvojumus par dalību privātuma vairogā un uz tiem reaģētu, ministrija pārskatīs organizāciju privātuma politiku. Konkrētāk, ministrija izskatīs to organizāciju privātuma politiku, kuru pašsertifikācijas termiņš ir beidzies, jo tās nav no jauna sertificējušas principu stingru ievērošanu. Ministrija veiks šāda veida pārbaudi, lai pārliecinātos, ka šīs organizācijas no attiecīgās publicētās privātuma politikas ir dzēsušas visas atsauces, kas ļauj secināt, ka organizācija joprojām aktīvi piedalās privātuma vairogā. Šo pārbaužu rezultātā ministrija apzinās organizācijas, kas šādas atsauces nav dzēsušas, un nosūtīs tām ministrijas galvenā juriskonsulta biroja vēstuli ar brīdinājumu par iespējamu izpildes panākšanas darbību atsauču neizdzēšanas gadījumā. Ministrija veiks turpmākas uzraudzības pasākumus, lai nodrošinātu, ka organizācijas vai nu dzēš neatbilstošās atsauces, vai arī no jauna sertificē principu stingru ievērošanu. Ministrija arīdzan centīsies konstatēt tādu organizāciju nepatiesus apgalvojumus par dalību privātuma vairogā, kuras šajā programmā nekad nav piedalījušās, un attiecībā uz tām veiks līdzīgas korektīvās darbības.

Periodiskas programmas *ex officio* atbilstības pārbaudes un novērtējumi:

— pastāvīgi uzraudzīs atbilstību, tostarp nosūtot dalīborganizācijām sīki izstrādātas anketas, lai konstatētu aspektus, uz kuriem varētu būt jāreaģē ar turpmākiem pasākumiem. Konkrētāk, šādas atbilstības pārbaudes notiks tad, ja: a) ministrija saņems konkrētas un nozīmīgas sūdzības par organizācijas atbilstību principiem; b) organizācija nesniegs apmierinošas atbildes uz ministrijas informācijas pieprasījumiem par privātuma vairogu; vai c) pastāvēs ticami pierādījumi par to, ka organizācija neievēro no privātuma vairoga izrietošās saistības. Attiecīgā gadījumā ministrija par šādām atbilstības pārbaudēm konsultēsies ar kompetentajām datu aizsardzības iestādēm, kā arī

— periodiski novērtēs privātuma vairoga programmas pārvaldību un uzraudzību, lai nodrošinātu, ka ar uzraudzības centieniem var pienācīgi reaģēt uz jaunām problēmām, tiklīdz tās ir radušās.

Ministrija ir paplašinājusi resursus, kas tiks atvēlēti privātuma vairoga programmas pārvaldībai un uzraudzībai, tostarp divkāršojusi par šīm darbībām atbildīgo darbinieku skaitu. Mēs arī turpmāk veltīsim atbilstošus resursus centieniem nodrošināt programmas rezultatīvu uzraudzību un pārvaldību.

Privātuma vairoga tīmekļa vietnes pielāgošana konkrētām mērķauditorijas grupām

Ministrija pielāgos privātuma vairoga tīmekļa vietni trim mērķauditorijas grupām: ES fiziskām personām, ES uzņēmumiem un ASV uzņēmumiem. Iekļaujot vietnē tieši ES fiziskām personām un ES uzņēmumiem paredzētus materiālus, vairākos veidos tiks veicināta pārredzamība. Materiālos ES fiziskām personām tiks konkrēti izskaidrotas: 1) tiesības, ko viņām piešķir privātuma vairogs; 2) tiesību aizsardzības mehānismi, kas pieejami, ja viņas uzskata, ka organizācija ir pārkāpusi savas principu ievērošanas saistības; un 3) kā atrast informāciju par organizācijas privātuma vairoga pašsertifikāciju. Attiecībā uz ES uzņēmumiem tā veicinās šādas informācijas pārbaudi: 1) vai organizācijai pienākas no privātuma vairoga izrietošās priekšrocības; 2) informācijas veids, uz kuru attiecas organizācijas privātuma vairoga pašsertifikācija; 3) attiecīgajai informācijai piemērotā privātuma politika; un 4) metode, ar kuru organizācija pārbauda, vai principi tiek stingri ievēroti.

Sadarbības ar DAI izvēršana

Lai palielinātu iespējas sadarboties ar DAI, ministrija, pirmkārt, izveidos speciālu kontaktpersonu, kas koordinēs sadarbību ar DAI. Ja DAI uzskatīs, ka kāda organizācija neievēro principus, tostarp no ES iedzīvotājiem saņemtu sūdzību gadījumos, tā varēs vērsties pie ministrijas speciālās kontaktpersonas un nodot informāciju par organizāciju turpmākai pārbaudei. Kontaktpersona arī saņems pieprasījumus par organizācijām, kuras nepatiesi apgalvo, ka piedalās privātuma vairoga īstenošanā, lai gan nekad nav pašsertificējušas principu stingru ievērošanu. Kontaktpersona palīdzēs DAI, kas meklē informāciju par kādas organizācijas pašsertifikāciju vai iepriekšēju dalību programmā, un atbildēs uz DAI jautājumiem par konkrētu privātuma vairoga prasību īstenošanu. Otrkārt, lai palielinātu pārredzamību ES fiziskām personām un uzņēmumiem, ministrija piešķirs DAI to tīmekļa vietnēs izvietojamus materiālus par privātuma vairogu. Lielākai informētībai par privātuma vairogu un no tā izrietošajām tiesībām un pienākumiem vajadzētu veicināt problēmu konstatēšanu uzreiz pēc to rašanās un tādējādi to atbilstošu risināšanu.

Par neatbilstību iesniegto sūdzību risināšanas veicināšana

Ministrija ar speciālās kontaktpersonas starpniecību saņems tai nodotās DAI sūdzības par privātuma vairoga organizācijas neatbilstību principiem. Tā, cik vien iespējams, centīsies sekmēt sūdzības risināšanu ar privātuma vairoga organizāciju. Ministrija 90 dienu laikā no sūdzības saņemšanas sniegs DAI jaunāko informāciju. Lai atvieglotu šādu sūdzību iesniegšanu, ministrija izveidos DAI paredzētu standarta veidlapu, kas jāiesniedz ministrijas speciālajai kontaktpersonai. Tā reģistrēs visus ministrijai iesniegtos DAI pieprasījumus, un ministrija turpmāk aprakstītajā gada pārskatā sniegs ziņojumu, kurā apkopojoši analizēs katru gadu saņemtās sūdzības.

Šķīrējtiesas procedūru pieņemšana un šķīrējtiesnešu atlase, konsultējoties ar Komisiju

Ministrija pildīs savas I pielikumā noteiktās saistības un pēc vienošanās panākšanas publicēs informāciju par procedūrām.

Kopīgs privātuma vairoga darbības pārskatīšanas mehānisms

Tirdzniecības ministrija, FTK un, attiecīgā gadījumā, citas aģentūras rīkos ikgadējas sanāksmes ar Komisiju, ieinteresētajām datu aizsardzības iestādēm un attiecīgajiem 29. panta darba grupas pārstāvjiem, kurās ministrija sniegs jaunāko informāciju par privātuma vairoga programmu. Ikgadējās sanāksmēs apspriedīs aktuālos jautājumus saistībā ar privātuma vairoga darbību, īstenošanu, uzraudzību un izpildes panākšanu, tostarp ministrijai iesniegtos DAI pieprasījumus, *ex officio* atbilstības pārbaužu rezultātus un, iespējams, arī attiecīgas tiesību aktu izmaiņas. Pirmo ikgadējo pārskatu un turpmākos pārskatos, ja nepieciešams, tiks ietverts dialogs par citiem jautājumiem, piemēram, par automatizētu lēmumu pieņemšanu, tostarp aspektiem saistībā ar līdzībām un atšķirībām ES un ASV pieejā.

Tiesību aktu atjaunināšana

Ministrija īstenos pamatotus centienus, lai informētu Komisiju par būtiskām izmaiņām ASV tiesību aktos, ciktāl tie attiecas uz privātuma vairogu tādās jomās kā datu privātuma aizsardzību un ierobežojumi un aizsardzības pasākumi attiecībā uz ASV iestāžu piekļuvi personas datiem un to turpmāku izmantošanu.

Valsts drošības izņēmums

Nacionālās izlūkošanas direktora biroja galvenais juriskonsults *Robert Litt* ir nosūtījis Tirdzniecības ministrijas amatpersonām *Justin Antonipillai* un *Ted Dean* vēstules par privātuma vairoga principu ievērošanas ierobežojumiem, kas ir saistīti ar valsts drošību, un tās ir pārsūtītas arī Jums. Šajās vēstulēs cita starpā ir plaši aprakstīta ASV veiktajām sakaru izlūkošanas darbībām piemērotā politika, aizsardzības pasākumi un ierobežojumi, kā arī pārredzamība, ko šajā jomā nodrošina izlūkdienests. Kad Komisija izvērtēs privātuma vairoga regulējumu, tā, pamatojoties uz šajās vēstulēs izklāstīto informāciju, varēs secināt, ka privātuma vairogs darbosies pienācīgi un atbilstīgi attiecīgajiem principiem. Mēs saprotam, ka izlūkdienesta publiskoto, kā arī citu informāciju Jūs turpmāk varat izmantot privātuma vairoga regulējuma gada pārskata izstrādē.

Pamatojoties uz privātuma vairoga principiem, pievienotajām vēstulēm un materiāliem, tostarp ministrijas saistībām privātuma vairoga regulējuma izpildes pārvaldības un uzraudzības jomā, mēs ceram, ka Komisija konstatēs, ka ES un ASV privātuma vairoga regulējuma nodrošinātais aizsardzības līmenis atbilst ES tiesību aktos paredzētajai aizsardzībai, un privātuma vairoga organizācijām arī turpmāk saņems datus no Eiropas Savienības.

Ar cieņu

Ken Hyatt

2. pielikums

Šķīrējtiesas modelis

I PIELIKUMS

Šajā pielikumā ir izklāstīti noteikumi, kas saskaņā ar tiesību aizsardzības, izpildes panākšanas un atbildības principu privātuma vairoga organizācijām jāievēro attiecībā uz prasību izskatīšanu šķīrējtiesā. Turpmāk aprakstītais saistošais šķīrējtiesas process ir piemērojams konkrētām "neatrisinātām" prasībām par datiem, uz kuriem attiecas ES un ASV privātuma vairogs. Šā procesa mērķis ir nodrošināt, lai indivīdiem būtu pieejams ātrs, neatkarīgs un taisnīgs mehānisms, ar ko izskatīt apgalvojumus par principu pārkāpumiem, kurus nav atrisinājis neviens cits privātuma vairoga mehānisms, ja tādi ir.

A. **Darbības joma**

Indivīds var izmantot šķīrējtiesas procesu, lai neatrisinātas prasības gadījumā tiktu noteikts, vai privātuma vairoga organizācija attiecībā uz šo indivīdu ir pārkāpusi no principiem izrietošos pienākumus un vai šāds pārkāpums ir pilnīgi vai daļēji neizlabots. Šī iespēja ir pieejama vienīgi minētajā nolūkā. To nevar izmantot, piemēram, attiecībā uz principu piemērošanas izņēmumiem ([1]) vai apgalvojumiem par privātuma vairoga nodrošinātās aizsardzības pietiekamību.

B. **Pieejamie tiesiskās aizsardzības līdzekļi**

Ja tiek izmantots šķīrējtiesas process, privātuma vairoga komisijai (kuras sastāvā atkarībā no pušu vienošanās ir viens vai trīs šķīrējtiesneši) ir pilnvaras noteikt individuālu, specifisku, nemonetāru un taisnīgu tiesiskās aizsardzības līdzekli (piemēram, piekļuvi, labošanu, dzēšanu vai attiecīgo indivīda datu atdošanu), kas vajadzīgs, lai labotu principu pārkāpumu vienīgi attiecībā uz indivīdu. Tās ir šķīrējtiesas komisijas vienīgās pilnvaras attiecībā uz tiesiskās aizsardzības līdzekļiem. Apsverot piešķiramos līdzekļus, šķīrējtiesas komisijai ir jāņem vērā arī citi tiesiskās aizsardzības līdzekļi, kas jau ir paredzēti citos privātuma vairoga mehānismos. Kaitējuma, izdevumu, maksu kompensācija vai citi tiesiskās aizsardzības līdzekļi nav pieejami. Katra puse sedz sava advokāta maksu.

C. **Prasības, kas jāizpilda pirms šķīrējtiesas procesa**

Indivīdam, kas nolemj izmantot šķīrējtiesas procesu, pirms prasības iesniegšanas jāveic šādas darbības: 1) par iespējamo pārkāpumu tieši jāinformē organizācija un jāsniedz tai iespēja problēmu atrisināt principu III sadaļas 11. daļas d) punkta i) apakšpunktā noteiktajā termiņā; 2) jāizmanto principos paredzētais neatkarīgais tiesību aizsardzības mehānisms, par kuru indivīdam nav jāmaksā; un 3) ar vietējās datu aizsardzības iestādes starpniecību par problēmu jāinformē Tirdzniecības ministrija un jāļauj tai pēc iespējas un bez maksas censties atrisināt problēmu termiņos, kas noteikti vēstulē no Tirdzniecības ministrijas Starptautiskās tirdzniecības pārvaldes.

Šo šķīrējtiesas procesu nevar izmantot, ja indivīda apgalvojums par principu pārkāpumu 1) jau ir izskatīts saistošā šķīrējtiesas procesā; 2) par to ir pieņemts galīgs spriedums tiesas procesā, kura puse bija indivīds; vai 3) puses jau iepriekš ir panākušas mierizlīgumu. Šo procesu nevar izmantot arī tad, ja ES datu aizsardzības iestādei: 1) ir pilnvaras atbilstīgi principu III sadaļas 5. vai 9. daļai; vai 2) ir pilnvaras izskatīt apgalvojumu par pārkāpumu, tieši iesaistot organizāciju. DAI pilnvaras izskatīt tādu pašu prasību pret ES datu pārzini pašas par sevi neliedz ierosināt šķīrējtiesas procesu pret citu juridisko personu, kas nav pakļauta DAI pilnvarām.

D. **Lēmumu saistošums**

Indivīda lēmums ierosināt šo saistošo šķīrējtiesas procesu ir pilnīgi brīvprātīgs. Šķīrējtiesas lēmumi būs saistoši visām procesa pusēm. Ierosinot procesu, indivīds atsakās no iespējas saistībā ar to pašu iespējamo pārkāpumu lūgt tiesību aizsardzību citā iestādē; izņēmums ir gadījumi, kad iespējamo pārkāpumu nav iespējams pilnā apmērā labot ar nemonetāru tiesiskās aizsardzības līdzekli – tad indivīda ierosinātais šķīrējtiesas process neliedz iespēju pieprasīt kaitējuma kompensāciju, kas citkārt ir pieejama tiesās.

([1]) Principu I.5. sadaļa.

E. **Pārskatīšana un izpildes panākšana**

Saskaņā ar Federālo šķīrējtiesas procesa likumu (*Federal Arbitration Act*) ([1]) indivīdi un privātuma vairoga organizācijas varēs lūgt šķīrējtiesnešu lēmumu pārskatīšanu tiesā un izpildes panākšanu atbilstīgi ASV tiesību aktiem. Visas attiecīgās lietas ir jāierosina tajā federālajā apgabaltiesā, kuras teritoriālajā jurisdikcijā ir privātuma vairoga organizācijas galvenā darbības vieta.

Šā šķīrējtiesas procesa uzdevums ir izšķirt individuālus strīdus, un šķīrējtiesas nolēmumiem nav jādarbojas kā pamudinošam vai saistošam precedentam lietās, kas ietver citas puses, tostarp turpmākos šķīrējtiesas procesos ES vai ASV tiesās vai FTK procesos.

F. **Šķīrējtiesas komisija**

Puses izvēlas šķīrējtiesnešus no turpmāk aprakstītā tiesnešu saraksta.

ASV Tirdzniecības ministrija un Eiropas Komisija, ievērojot piemērojamos tiesību aktus, izveidos sarakstu, kurā iekļaus vismaz 20 šķīrējtiesnešu, kas izvēlēti to neatkarības, godprātības un kompetences dēļ. Saistībā ar šo procesu jāievēro turpmāk uzskaitītie nosacījumi.

Šķīrējtiesneši:

1) sarakstā ir trīs gadus un no tā tiek izslēgti ārkārtas apstākļu vai iemeslu dēļ; sarakstā iekļautos speciālistus var atkārtoti iekļaut sarakstā vēl uz trim gadiem;

2) nesaņem norādījumus no kādas procesa puses, privātuma vairoga organizācijas, ASV, ES vai kādas ES dalībvalsts vai kādas citas valdības iestādes, publiskas iestādes vai tiesībaizsardzības iestādes un nav ar tām saistīta; un

3) ir saņēmuši atļauju praktizēt tiesības ASV un ir ASV privātuma tiesību eksperti, kas ir kompetenti ES datu aizsardzības tiesībās.

G. **Šķīrējtiesas procedūras**

Atbilstīgi piemērojamiem tiesību aktiem sešu mēnešu laikā no lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas Tirdzniecības ministrija un Eiropas Komisija vienosies pieņemt jau izveidotu, iedibinātu ASV šķīrējtiesas procedūru (piemēram, AAA vai JAMS) kopumu, lai reglamentētu privātuma vairoga komisijas procedūras atbilstīgi visiem turpmāk uzskaitītajiem apsvērumiem.

1. Indivīds var ierosināt saistošu šķīrējtiesas procesu, ievērojot iepriekš izklāstītās prasības, kas jāizpilda pirms šķīrējtiesas procesa, un iesniedzot organizācijai "paziņojumu". Paziņojumā iekļauj atbilstīgi C punktam veikto prasības risināšanas darbību kopsavilkumu, iespējamā pārkāpuma aprakstu un, ja indivīds vēlas, jebkādus pavaddokumentus un materiālus un/vai ar iespējamo pārkāpumu saistīta tiesību akta aprakstu.

([1]) Atbilstīgi Federālā šķīrējtiesas procesa likuma ("FAA") 2. nodaļai "uz arbitrāžas vienošanos vai šķīrējtiesas nolēmumu, kas izriet no juridiskām – līgumiskām vai ne – attiecībām, ko uzskata par komerciālām attiecībām, tostarp uz darījumu, līgumu vai vienošanos, kas aprakstīta [*FAA* 2. pantā], attiecas [1958. gada 10. jūnija] Konvencija [par ārvalstu šķīrējtiesu nolēmumu atzīšanu un izpildīšanu (*21 U.S.T. 2519, T.I.A.S.* Nr. 6997 ("Ņujorkas Konvencija")]." *9 U.S.C. § 202*. Turklāt saskaņā ar *FAA*"tiek uzskatīts, ka uz vienošanos vai nolēmumu, kas izriet no šādām attiecībām, kuru puses ir vienīgi Amerikas Savienoto Valstu pilsoņi, neattiecas [Ņujorkas] Konvencijas noteikumi, ja vien šīs attiecības neietver īpašumu, kas atrodas ārvalstīs, darbību vai izpildes panākšanu ārvalstīs vai nav citādi un pamatoti saistītas ar vienu vai vairākām ārvalstīm." *Turpat* 2. nodaļā: "ikviena šķīrējtiesas procesa puse var vērsties jebkurā tiesā, kurai ir jurisdikcija saskaņā ar šo nodaļu, un lūgt, lai tā pieņemtu rīkojumu, ar ko apstiprina pret jebkuru šķīrējtiesas procesa pusi pieņemto nolēmumu. Tiesa nolēmumu apstiprina, ja vien tā nekonstatē kādu no [Ņujorkas] Konvencijā noteiktajiem nolēmuma atzīšanas vai izpildes panākšanas atteikuma vai atlikšanas iemesliem." Turpat, § 207. FAA 2. nodaļā arī noteikts, ka "Amerikas Savienoto Valstu apgabaltiesām (…) ir sākotnējā jurisdikcija attiecībā uz (…) prasību vai procesu [saskaņā ar Ņujorkas Konvenciju] neatkarīgi no summas, par kuru ir strīds." Turpat, § 203.
FAA 2. nodaļā ir noteikts arīdzan tas, ka "saskaņā ar šo nodaļu ierosinātajām prasībām un procesiem piemēro 1. nodaļu, ciktāl tā nav pretrunā šai nodaļai vai [Ņujorkas] Konvencijai, ko ir ratificējušas Amerikas Savienotās Valstis." Turpat, § 208. Savukārt 1. nodaļā ir paredzēts, ka (…) "tirdzniecības darījumu apliecinoša līguma [r]akstisks noteikums) par to, ka turpmākas domstarpības par šādu līgumu vai darījumu, vai atteikumu pildīt visu līgumu vai darījumu, vai tā daļu izskata šķīrējtiesā, vai rakstiska vienošanās iesniegt izskatīšanai šķīrējtiesā esošas domstarpības par šādu līgumu, darījumu vai atteikumu ir spēkā, neatsaucama un izpildāma, izņemot tiesību aktos noteiktajos gadījumos vai kāda līguma anulēšanas gadījumā." Turpat, § 2. Turklāt saskaņā ar *FAA* 1. nodaļu "ikviena šķīrējtiesas procesa puse var attiecīgi tiesā lūgt rīkojumu, ar ko apstiprina nolēmumu, un tādā gadījumā tiesai šāds rīkojums ir jāpieņem, ja vien nolēmums nav anulēts, mainīts vai labots, kā paredzēts [*FAA*] 10. un 11. pantā." Turpat, § 9.

2. Tiks izstrādātas procedūras, ar ko nodrošināt, lai uz vienu indivīda prasību par iespējamo pārkāpumu netiktu attiecināti divkārši tiesiskās aizsardzības līdzekļi vai procesi.

3. Vienlaikus šķīrējtiesas procesam var notikt prasības izskatīšana FTK.

4. Šajos šķīrējtiesas procesos nedrīkst piedalīties ASV, ES, ES dalībvalstu vai kādas citas valdības iestādes, publiskās iestādes vai tiesībaizsardzības iestādes pārstāvji, ja pēc ES indivīda pieprasījuma ES DAI var palīdzēt tikai paziņojuma sagatavošanā, taču ES DAI nedrīkst piekļūt konstatējumiem vai citiem ar šo šķīrējtiesas procesu saistītiem materiāliem.

5. Process noris Amerikas Savienotajās Valstīs, un indivīds var izvēlēties dalību ar video vai tālruņa starpniecību, kas tiks nodrošināta bez maksas. Personiska klātbūtne netiek prasīta.

6. Šķīrējtiesas process notiks angļu valodā, ja vien puses nevienosies citādi. Saņemot pamatotu pieprasījumu un ņemot vērā to, vai indivīdu pārstāv advokāts, indivīdam bez maksas nodrošinās šķīrējtiesas sēdes mutisko tulkojumu, kā arī materiālu rakstisko tulkojumu, ja vien komisija nekonstatēs, ka konkrētā procesa apstākļos tas radītu nepamatotas vai nesamērīgas izmaksas.

7. Šķīrējtiesnešiem iesniegtos materiālus uzskatīs par konfidenciāliem un izmantos vienīgi saistībā ar attiecīgo procesu.

8. Ja nepieciešams, var atļaut izmantot ar indivīdu saistītu konstatējumu, un puses šādu konstatējumu uzskatīs par konfidenciālu un izmantos tikai saistībā ar attiecīgo šķīrējtiesas procesu.

9. Process būtu jāizskata 90 dienu laikā no paziņojuma iesniegšanas attiecīgajai organizācijai, ja vien puses nevienojas citādi.

H. **Izmaksas**

Šķīrējtiesnešiem būtu jāveic piemērotas darbības, lai līdz minimumam samazinātu procesa izmaksas vai nodevas.

Saskaņā ar piemērojamiem tiesību aktiem Tirdzniecības ministrija, konsultējoties ar Eiropas Komisiju, veicinās tāda fonda izveidi, kurā privātuma vairoga organizācijām būs jāveic no to lieluma daļēji atkarīgas gada iemaksas, ar kurām tiks segtas šķīrējtiesas procesa izmaksas, ieskaitot šķīrējtiesnešu honorārus, kuri nepārsniedz maksimālo apmēru ("robežvērtību"). Fondu pārvaldīs trešā persona, kas regulāri ziņos par tā darbību. Gada pārskatā Tirdzniecības ministrija un Eiropas Komisija pārskatīs fonda darbību, tostarp nepieciešamību pielāgot iemaksu vai robežvērtību apmēru, un cita starpā izskatīs šķīrējtiesas procesu skaitu, izmaksas un ilgumu, saprotot, ka nevajadzētu radīt privātuma vairoga organizācijām pārmērīgu finansiālo slogu. Šā noteikuma un neviena saskaņā ar to izveidota fonda darbības joma neattiecas uz advokātu honorāriem.

II PIELIKUMS

ES UN ASV PRIVĀTUMA VAIROGA REGULĒJUMA PRINCIPI, KO IZDEVUSI ASV TIRDZNIECĪBAS MINISTRIJA

I. PĀRSKATS

1. Gan Amerikas Savienoto Valstu, gan Eiropas Savienības mērķis ir uzlabot privātuma aizsardzību, taču Amerikas Savienotajās Valstīs īsteno citādu pieeju privātuma aizsardzībai nekā Eiropas Savienībā. Amerikas Savienotās Valstis izmanto nozaru pieeju, kuras pamatā ir gan ārēji, gan iekšēji normatīvie akti. Ņemot vērā šīs atšķirības un nolūkā nodrošināt Amerikas Savienoto Valstu organizācijām uzticamu mehānismu, ar ko personas datus pārsūtīt no Eiropas Savienības uz Amerikas Savienotajām Valstīm, vienlaikus arī turpmāk garantējot ES datu subjektiem Eiropas tiesību aktos prasītos rezultatīvos aizsardzības pasākumus un aizsardzību viņu personas datu apstrādei, kad tie ir pārsūtīti uz valstīm ārpus ES, Tirdzniecības ministrija, lai veicinātu, sekmētu un izvērstu starptautisko tirdzniecību, saskaņā ar savām likumiskajām pilnvarām ir pieņēmusi šos privātuma vairoga principus un papildu principus (kopā "principi") (*15 U.S.C. § 1512*). Principi tika izstrādāti, apspriežoties ar Eiropas Komisiju, nozares uzņēmumiem un citām ieinteresētajām personām, lai veicinātu tirdzniecību starp Amerikas Savienotajām Valstīm un Eiropas Savienību. Ir paredzēts, ka tos izmantos tikai tās Amerikas Savienoto Valstu organizācijas, kas saņem personas datus no Eiropas Savienības un izpilda privātuma vairoga nosacījumus un uz kurām līdz ar to attiecas Eiropas Komisijas lēmums par aizsardzības līmeņa pietiekamību ([1]). Principi neietekmē to valsts noteikumu piemērošanu, ar kuriem īsteno Direktīvu 95/46/EK ("direktīva") un kuri attiecas uz personas datu apstrādi dalībvalstīs. Principi arī neierobežo privātuma saistības, kas ir citādi paredzētas ASV tiesību aktos.

2. Lai varētu pārsūtīt personas datus no ES, pamatojoties uz privātuma vairogu, organizācijai ir pašai jāapliecina Tirdzniecības ministrijai (vai tās pārstāvim) ("ministrija"), ka tā stingri ievēro principus. Lai gan organizāciju lēmumi šādi iesaistīties privātuma vairoga īstenošanā ir pilnīgi brīvprātīgi, attiecīgo noteikumu ievērošana ir obligāta – organizācijām, kuras ir pašas apliecinājušas ministrijai un publiski paziņojušas par apņemšanos stingri ievērot principus, tie ir pilnīgi jāizpilda. Lai iesaistītos privātuma vairoga īstenošanā, organizācijai a) jāpakļaujas Federālās tirdzniecības komisijas ("FTK"), Transporta ministrijas vai citas tādas oficiālas iestādes izmeklēšanas un tiesībaizsardzības pilnvarām, kas rezultatīvi nodrošinās atbilstību principiem (*citas ES atzītas ASV oficiālās iestādes turpmāk varētu tikt uzskaitītas atsevišķā pielikumā*); b) publiski jāpaziņo par savu apņemšanos principus ievērot; c) jāpublisko sava privātuma politika atbilstīgi šiem principiem; un d) tie pilnā apmērā jāīsteno. Ja organizācija principus neievēro, tās atbilstība ir panākama saskaņā ar Federālās tirdzniecības komisijas likuma (*Federal Trade Commission Act*) 5. pantu, ar ko aizliedz negodīgas un maldinošas darbības, kuras veic tirdzniecībā vai kuras to ietekmē (*15 U.S.C. § 45(a)*), vai citiem tiesību aktiem vai noteikumiem, kuros šādas darbības ir aizliegtas.

3. Tirdzniecības ministrija uzturēs un darīs sabiedrībai zināmu to ASV organizāciju autoritatīvu sarakstu, kuras pašas ir apliecinājušas ministrijai un paziņojušas par apņemšanos stingri ievērot principus ("privātuma vairoga saraksts"). Ar privātuma vairogu saistītās priekšrocības tiek saņemtas no dienas, kad ministrija iekļauj organizāciju privātuma vairoga sarakstā. Ministrija svītros organizāciju no privātuma vairoga saraksta, ja tā brīvprātīgi izstāsies no privātuma vairoga vai nebūs veikusi ikgadējo atkārtoto sertifikāciju ministrijā. Ja organizācija no privātuma vairoga saraksta ir svītrota, uz to vairs neattiecas Eiropas Komisijas lēmums par aizsardzības līmeņa pietiekamību, kas ļauj saņemt personisko informāciju no ES. Organizācijai ir jāturpina piemērot principus personiskajai informācijai, ko tā saņēma, kad piedalījās privātuma vairogā, un ik gadu jāapstiprina ministrijai sava apņemšanās to darīt, kamēr tā šo informāciju glabās; citādi organizācijai informācija ir jāatdod atpakaļ vai jādzēš, vai arī jānodrošina tās "pienācīga" aizsardzība ar citiem atļautiem līdzekļiem. Ministrija no privātuma vairoga saraksta svītros arī tās organizācijas, kas pastāvīgi nav ievērojušas principus; šīs organizācijas nav tiesīgas saņemt privātuma vairoga radītās priekšrocības, un tām ir jāatdod atpakaļ vai jādzēš privātuma vairoga satvarā saņemtā personiskā informācija.

4. Ministrija arī uzturēs un darīs sabiedrībai pieejamu to ASV organizāciju autoritatīvu reģistru, kuras iepriekš ir apliecinājušas ministrijai apņemšanos ievērot privātuma vairogu, taču ir svītrotas no tā saraksta. Ministrija skaidri brīdinās, ka šīs organizācijas nav privātuma vairoga dalībnieces; ka pēc svītrošanas no privātuma vairoga saraksta šādas organizācijas nevar apgalvot, ka atbilst privātuma vairoga nosacījumiem un tām nevajadzētu izplatīt paziņojumus vai īstenot maldinošu praksi, kas norādītu uz to dalību privātuma vairogā; un ka uz šādām organizācijām vairs nevar attiecināt Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību, kas tām ļautu saņemt personisko informāciju no ES. Attiecībā uz organizāciju, kas pēc tās svītrošanas no privātuma vairoga

([1]) Ar nosacījumu, ka Komisijas lēmumu par pienācīgu aizsardzību, kas noteikta ar ES un ASV privātuma vairogu piemēro Islandei, Lihtenšteinai un Norvēģijai, privātuma vairoga pakete attieksies gan uz Eiropas Savienību, gan uz šīm trim valstīm. Attiecīgi atsauces uz ES un tās dalībvalstīm būs lasāmas, ietverot arī Islandi, Lihtenšteinu un Norvēģiju.

saraksta turpina apgalvot, ka piedalās privātuma vairoga īstenošanā, vai izsaka citus ar to saistītus sagrozītus apgalvojumus, FTK, Transporta ministrija vai citas tiesībaizsardzības iestādes var īstenot izpildes panākšanas darbību.

5. Šo principu ievērošanu var ierobežot: a) ciktāl tas ir vajadzīgs, lai ievērotu valsts drošību, sabiedrības intereses vai izpildītu tiesībaizsardzības prasības; b) ar likumu, valdības noteikumiem vai judikatūru, kas rada pretrunīgus pienākumus vai paredz skaidras atļaujas, ja, izmantojot šādu atļauju, organizācija var pierādīt, ka neīsteno principus vienīgi tiktāl, ciktāl ir vajadzīgs, lai ievērotu sevišķi svarīgas likumīgās intereses, kuras izriet no šādas atļaujas; vai c) ja direktīva vai dalībvalsts tiesību akti pieļauj izņēmumus vai atkāpes, ar nosacījumu, ka šādus izņēmumus vai atkāpes piemēro līdzvērtīgās situācijās. Saskaņā ar mērķi uzlabot privātās dzīves aizsardzību organizācijām jācenšas šos principus īstenot pilnībā un pārredzamā veidā, tostarp savā slepenības politikā norādot to, vai ar b) punktu atļautos izņēmumus attiecībā uz principiem piemēros regulāri. Tā paša iemesla dēļ organizācijām, ja iespējams, jāizvēlas labāka aizsardzība, ja izvēli atļauj principi un/vai ASV tiesību akti.

6. Organizācijām jāpiemēro principi visiem personas datiem, kas pārsūtīti, pamatojoties uz privātuma vairogu, tiklīdz tie nonāk privātuma vairogā. Organizācijai, kas vēlas privātuma vairoga priekšrocības attiecināt arī uz cilvēkresursu personisko informāciju, kas no ES pārsūtīta izmantošanai saistībā ar darba attiecībām, tas jānorāda ministrijai, kad tā veic pašsertifikāciju, un tai jāievēro papildu principā par pašsertifikāciju izvirzītās prasības.

7. Jautājumus par to, kā privātuma vairoga organizācijas interpretē un ievēro principus un attiecīgo privātuma politiku, risina saskaņā ar ASV tiesību aktiem, izņemot gadījumus, kad šādas organizācijas ir apņēmušās sadarboties ar Eiropas datu aizsardzības iestādēm ("DAI"). Ja vien nav norādīts citādi, visus principu noteikumus piemēro attiecīgā gadījumā.

8. Definīcijas:

   a. "personas dati" un "personiskā informācija" ir tādi dati par identificētu vai identificējamu indivīdu, uz kuriem attiecas direktīva un kurus Amerikas Savienoto Valstu organizācija ir saņēmusi no Eiropas Savienības un jebkādā veidā reģistrējusi;

   b. personas datu "apstrāde" ir jebkura ar personas datiem veikta darbība vai darbību kopums ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrēšana, sakārtošana, glabāšana, pielāgošana vai pārveidošana, izgūšana, skatīšana, izmantošana, izpaušana vai izplatīšana un dzēšana vai iznīcināšana;

   c. "pārzinis" ir persona vai organizācija, kas viena pati vai kopā ar citiem nosaka personas datu apstrādes nolūkus un līdzekļus.

9. Principi stājas spēkā dienā, kad Eiropas Komisija galīgi apstiprina aizsardzības līmeņa pietiekamību.

II. PRINCIPI

1. **Informēšana**

   a. Organizācijai jāinformē indivīdi par:

      i. tās dalību privātuma vairogā un jānorāda saite uz privātuma vairoga sarakstu vai tā tīmekļa adrese;

      ii. vākto personas datu veidiem un, attiecīgā gadījumā, organizācijas struktūrām vai filiālēm, kas arī ievēro principus;

iii. tās apņemšanos piemērot principus visiem personas datiem, kas no ES saņemti, pamatojoties uz privātuma vairogu;

iv. mērķiem, kādiem tā vāc un izmanto to personas datus;

v. to, kā pie organizācijas var vērsties ar jautājumiem vai sūdzībām, tostarp norādot visas attiecīgās ES iestādes, kas var atbildēt uz šādiem jautājumiem vai sūdzībām;

vi. to trešo personu veidu vai identitāti, kam tā izpauž personisko informāciju, un šādas rīcības iemesliem;

vii. indivīdu tiesībām piekļūt saviem personas datiem;

viii. izvēles iespējām un līdzekļiem, ko organizācija indivīdiem piedāvā, lai ierobežotu to personas datu izmantošanu un izpaušanu;

ix. neatkarīgo strīdu izšķiršanas struktūru, kurai jāizskata sūdzības un jānodrošina indivīdam attiecīgie tiesību aizsardzības līdzekļi bez maksas, un to, vai šī struktūra ir: 1) DAI izveidota komisija; 2) alternatīvs strīdu izšķiršanas pakalpojumu sniedzējs, kas darbojas ES; vai 3) alternatīvs strīdu izšķiršanas pakalpojumu sniedzējs, kas darbojas Amerikas Savienotajās Valstīs;

x. to, ka tā ir pakļauta FTK, Transporta ministrijas vai kādas citas ASV pilnvarotas oficiālas iestādes izmeklēšanas un tiesībaizsardzības pilnvarām;

xi. viņu iespēju konkrētos apstākļos ierosināt saistošu šķīrējtiesas procesu;

xii. prasību izpaust personisko informāciju, atbildot uz likumīgiem publisko iestāžu pieprasījumiem, tostarp ievērot ar valsts drošību vai tiesībaizsardzību saistītas prasības, un

xiii. tās atbildību, ja informāciju tālāk pārsūta trešajām personām.

b. Šis paziņojums jāsniedz skaidrā un viegli saprotamā veidā; to nosūta indivīdiem, pirmo reizi lūdzot tos sniegt personisko informāciju organizācijai, vai cik drīz vien iespējams pēc tam, bet jebkurā gadījumā pirms organizācija šādu informāciju izmanto citiem mērķiem, izņemot tos, kuriem nosūtītāja organizācija to sākotnēji ievākusi vai apstrādājusi, vai to pirmo reizi izpaudusi trešai personai.

2. **Izvēle**

a. Organizācijai jāpiedāvā indivīdiem iespēja izvēlēties (atteikt), vai viņu personisko informāciju i) izpaudīs trešajai personai vai ii) izmantos mērķim, kas būtiski atšķiras no mērķa(-iem), kuram(-iem) to sākotnēji vāca vai indivīds pēc tam atļāva izmantot. Lai indivīdi varētu izdarīt izvēli, ir jānodrošina viņiem skaidri, viegli saprotami, gatavi un pieejami mehānismi.

b. Atkāpjoties no iepriekšējā punkta, izvēles principi nav obligāti jāpiemēro, ja datus izpauž trešajai personai, kura darbojas kā pārstāvis, lai pildītu uzdevumu(-us) organizācijas vārdā un saskaņā ar tās norādījumiem. Tomēr organizācijai ar pārstāvi vienmēr jānoslēdz līgums.

c. Attiecībā uz sensitīvu informāciju (t. i., personisko informāciju, kas ietver medicīniskos datus vai datus par veselības stāvokli, norāda personas rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībā, vai ietver datus par indivīda seksuālo dzīvi), ja šādu informāciju i) izpaudīs trešajai personai vai ii) izmantos citam mērķim, kas nav tas, kuram tā sākotnēji vākta vai kuram indivīdi, izdarot attiecīgu izvēli, pēc tam atļāvuši to izmantot. Turklāt organizācijai jebkāda informācija, kas ir saņemta no trešās personas, būtu jāapstrādā kā sensitīva informācija, ja trešā persona to identificē un apstrādā kā sensitīvu.

3. **Atbildība par tālākpārsūtīšanu**

a. Pārsūtot personisko informāciju trešajai personai, kura darbojas kā pārzinis, organizācijām jāievēro informēšanas un izvēles principi. Tām arī jānoslēdz līgums ar pārzini, kas ir trešā persona, kurā noteikts, ka šādus datus drīkst apstrādāt vienīgi ierobežotos un precizētos nolūkos, kas atbilst indivīda sniegtajai piekrišanai, un ka saņēmējs nodrošinās tādu pašu aizsardzības līmeni, kādu sniedz privātuma vairoga principi un informēs organizāciju, ja tiek konstatēts, ka pārzinis vairs nevar izpildīt šo pienākumu. Līgumā paredz, ka šāda konstatējuma gadījumā pārzinis trešā persona pārtrauc personas datu apstrādi vai veic citus pamatotus un atbilstošus pasākumus, lai labotu situāciju.

b. Pārsūtot personas datus trešajai personai, kura rīkojas kā pārstāvis, organizācijām: i) šādi dati jāpārsūta vienīgi ierobežotos un precizētos nolūkos; ii) jāpārliecinās, ka pārstāvim ir pienākums nodrošināt vismaz tādu pašu privātuma aizsardzības līmeni, kāds ir prasīts principos; iii) jāveic pamatotas un atbilstošas darbības, lai nodrošinātu, ka pārstāvis apstrādā pārsūtīto personisko informāciju, ievērojot no principiem izrietošos organizācijas pienākumus; iv) jāprasa pārstāvim informēt organizāciju, ja tiek konstatēts, ka pārzinis vairs nevar izpildīt pienākumu nodrošināt tādu pašu aizsardzības līmeni, kādu pieprasa principi; v) saņemot attiecīgu paziņojumu, tostarp atbilstoši iv) punktam, jāveic pamatotas un atbilstošas darbības, lai apturētu neatļautu apstrādi un koriģētu tās sekas; un vi) pēc ministrijas pieprasījuma iesniedz tai ar pārstāvi noslēgtā līguma attiecīgo privātuma noteikumu kopsavilkumu vai reprezentatīvu kopiju.

4. **DROŠĪBA**

a. Organizācijām, kas izveido, uztur, izmanto vai izplata personisko informāciju, jāveic saprātīgi un atbilstoši pasākumi, lai to aizsargātu no pazaudēšanas, ļaunprātīgas izmantošanas, neatļautas piekļuves, izpaušanas, mainīšanas un iznīcināšanas, pienācīgi ņemot vērā ar personas datu apstrādi un veidu saistītos riskus.

5. **Datu integritāte un mērķa ierobežošana**

a. Saskaņā ar principiem personiskā informācija ir jāierobežo līdz tādai informācijai, kas ir saistīta ar apstrādes mērķiem ([1]). Organizācija nedrīkst personisko informāciju apstrādāt tādā veidā, kas ir nesavienojams ar tiem mērķiem, kuriem tā sākotnēji vākta, vai kuriem indivīds pēc tam atļāvis to izmantot. Ciktāl tas ir vajadzīgs šiem mērķiem, organizācijai jāveic samērīgi pasākumi, lai nodrošinātu, ka dati saistībā ar paredzētajiem mērķiem ir ticami, precīzi, pilnīgi un aktuāli. Organizācijai stingri jāievēro principi tik ilgi, kamēr tā šādu informāciju glabā.

b. Informāciju var saglabāt tādā veidā, kas ļauj identificēt vai padarīt identificējamu ([2]) indivīdu tikai tik ilgi, cik tas nepieciešams apstrādes mērķim 5.a punkta nozīmē. Šis pienākums neliedz organizācijām apstrādāt personisku informāciju ilgāk un tādā apmērā, kādā šāda apstrāde pamatoti nepieciešama arhivēšanas mērķim sabiedrības interesēs, žurnālistikas, literatūras un mākslas, zinātniskās un vēstures pētniecības un statistiskā analīzes nolūkos. Šādos gadījumos šādai apstrādei piemēro shēmas principus un noteikumus. Organizācijām būtu jāveic samērīgi un piemēroti pasākumi šo noteikumu ievērošanai.

6. **Piekļuve**

a. Indivīdiem jābūt piekļuvei personiskajai informācijai par viņiem, kas ir organizācijas rīcībā, un iespējai šo informāciju labot, mainīt vai dzēst, ja tā ir neprecīza vai arī tikusi apstrādāta, pārkāpjot principus, izņemot, ja apgrūtinājums vai izmaksas saistībā ar piekļuves nodrošināšanu būtu neatbilstīgas indivīda privātās dzīves apdraudējumam attiecīgajā gadījumā vai ja tas pārkāptu citu personu tiesības.

([1]) Atkarībā no apstākļiem, saderīgu pārstrādes mērķu piemēri var būt tādi, kas pamatoti izmantojami klientu attiecības, atbilstības un juridisku apsvērumu nolūkos, revīzijām, drošībai un krāpšanas novēršanai, organizācijas likumīgo tiesību saglabāšanai vai aizstāvēšanai, vai citi mērķi, kas atbilst saprātīgas personas cerībām, ņemot vērā datu vākšanas kontekstu.

([2]) Šajā sakarā, ja identifikācijas līdzekļus, kurus pamatoti varētu izmantot (cita starpā ņemot vērā izmaksas un laiku, kas vajadzīgs identifikācijas veikšanai, un pieejamo tehnoloģiju apstrādes laikā), un veidu, kādā tiek saglabāti dati, organizācija vai trešā persona, ja tai būtu piekļuve datiem, varētu pamatoti identificēt indivīdu, tad attiecīgais indivīds ir "identificējams".

7. **Tiesību aizsardzība, izpildes panākšana un atbildība**

a. Efektīvai provātuma aizsardzībai jāietver stingri mehānismi, ar ko nodrošināt principu ievērošanu, to indivīdu tiesību aizsardzību, kurus ietekmē principu neievērošana, un radīt sekas organizācijai, ja principi nav ievēroti. Šādiem mehānismiem jāietver vismaz:

i. gatavi, pieejami un neatkarīgi tiesību aizsardzības mehānismi, ar ko izmeklēt un ātri risināt katra indivīda sūdzības un domstarpības, neprasot no indivīda maksu un ievērojot principus, kā arī atlīdzināt kaitējumu, ja to paredz piemērojamie tiesību akti vai privātā sektora iniciatīvas;

ii. paveiktā darba kontroles procedūras, ar ko pārbaudīt, vai organizāciju apliecinājumi un apgalvojumi par to privātuma nodrošināšanas praksi ir patiesi un vai šo praksi īsteno, kā tiek apgalvots, jo īpaši saistībā ar neatbilstības gadījumiem; kā arī

iii. pienākums risināt problēmas, kas rodas saistībā ar to, ka organizācijas, kuras ir pasludinājušas, ka stingri ievēro principus, to nedara, un sekas attiecībā uz šādām organizācijām. Sankcijām jābūt pietiekami stingrām, lai nodrošinātu, ka organizācijas principus ievēro.

b. Organizācijām un to izvēlētajiem neatkarīgajiem tiesību aizsardzības mehānismiem ātri jāatbild uz ministrijas jautājumiem un informācijas pieprasījumiem par privātuma vairogu. Visām organizācijām ir ātri jāreaģē uz sūdzībām par atbilstību principiem, ko ar ministrijas starpniecību iesniegušas ES dalībvalstu iestādes. Organizācijām, kas ir izvēlējušās sadarboties ar DAI, arī organizācijām, kuras apstrādā cilvēkresursu datus, saistībā ar sūdzību izmeklēšanu un risināšanu ir jāatbild šīm iestādēm nepastarpināti.

c. Ja indivīds ir ierosinājis saistošu šķīrējtiesas procesu, iesniedzot attiecīgajai organizācijai paziņojumu un ievērojot I pielikumā izklāstītās procedūras un nosacījumus, tai ir pienākums piedalīties šķīrējtiesas procesā un izpildīt I pielikumā paredzētos noteikumus.

d. Saistībā ar tālākpārsūtīšanu privātuma vairoga organizācija ir atbildīga par personiskās informācijas apstrādi, ko tā saņem privātuma vairoga satvarā un pēcāk pārsūta trešajai personai, kura tās vārdā darbojas kā pārstāvis. Privātuma vairoga organizācija saskaņā ar principiem ir atbildīga, ja tās pārstāvis apstrādā šādu personisko informāciju principiem neatbilstīgā veidā, izņemot, ja organizācija var pierādīt, ka nav atbildīga par notikumu, kas izraisīja kaitējumu.

e. Ja par organizāciju tās neatbilstības dēļ pieņem FTK vai tiesas rīkojumu, tā publisko visas Federālajai tirdzniecības komisijai iesniegta atbilstības vai novērtējuma ziņojuma sadaļas, kas ir saistītas ar privātuma vairogu, ciktāl tas nav pretrunā konfidencialitātes prasībām. Ministrija ir izveidojusi speciālu kontaktpersonu, ar ko DAI var sazināties par jebkādām ar privātuma vairoga organizāciju atbilstību saistītām problēmām. FTK prioritāri izskatīs ministrijas un ES dalībvalstu iestāžu pieprasījumus par neatbilstību principiem un ar pieprasījumu iesniedzējām iestādēm savlaicīgi un atbilstīgi piemērojamiem konfidencialitātes ierobežojumiem apmainīsies ar informāciju par pieprasījumiem.

III. PAPILDU PRINCIPI

1. **Sensitīvi dati**

a. Organizācijai nav jāsaņem apstiprinoša un skaidra (atļaujoša) piekrišana attiecībā uz sensitīviem datiem, ja apstrāde ir:

i. datu subjekta vai citas personas sevišķi svarīgās interesēs;

ii. vajadzīga, lai celtu likumīgas prasības vai aizstāvētu tās;

iii. vajadzīga, lai sniegtu medicīnisko aprūpi vai noteiktu diagnozi;

iv. veikta kāda fonda, asociācijas vai jebkuras citas bezpeļņas organizācijas likumīgu darbību laikā ar politisku, filozofisku, reliģisku vai ar arodbiedrībām saistītu mērķi, un ar nosacījumu, ka apstrāde attiecas tikai uz šīs organizācijas locekļiem vai personām, kas ar šo organizāciju uztur regulārus sakarus saistībā ar tās mērķiem, un ka datus neizpauž trešām personām bez datu subjektu piekrišanas;

v. vajadzīga, lai izpildītu organizācijas pienākumus darba tiesību jomā; vai vai

vi. saistīta ar datiem, ko indivīds acīmredzami ir publiskojis.

2. **Izņēmumi attiecībā uz žurnālistiku**

a. Ņemot vērā ASV nodrošināto preses brīvības konstitucionālo aizsardzību un direktīvā paredzēto atbrīvojumu attiecībā uz žurnālistikas materiālu, ja ASV Konstitūcijas Pirmajā grozījumā noteiktās brīvas preses tiesības saduras ar privātās dzīves aizsardzības interesēm, Pirmajam grozījumam jāreglamentē šo interešu līdzsvarošana attiecībā uz ASV personu vai organizāciju darbībām.

b. Privātuma vairoga principu prasības neattiecas uz personisko informāciju, kas ir savākta publicēšanai, apraidei vai citiem žurnālistikas materiālu publiskas paziņošanas veidiem, neatkarīgi no tā, vai šī informācija ir vai nav izmantota, kā arī uz informāciju, kura ir atrodama iepriekš publicētos materiālos, kas ir izplatīti no mediju arhīviem.

3. **Sekundārā atbildība**

a. Interneta pakalpojumu sniedzēji ("IPS"), telekomunikāciju uzņēmumi un citas organizācijas nav atbildīgas saskaņā ar privātuma vairoga principiem, ja tās citas organizācijas vārdā tikai pārsūta, maršrutē, maina vai uzglabā informāciju. Privātuma vairogs, tāpat kā direktīva, nerada sekundāro atbildību. Ciktāl organizācija darbojas tikai kā nodošanas kanāls trešās personas nosūtītajiem datiem un nenosaka šo personas datu apstrādes mērķus un līdzekļus, tai nav jāuzņemas atbildība.

4. **Pienācīga pārbaude un revīziju veikšana**

a. Revidentu un investīciju baņķieru darījumi var būt saistīti ar personas datu apstrādi bez indivīda piekrišanas vai ziņas. Informēšanas, izvēles un piekļuves principi to pieļauj, ja vien apstrāde notiek turpmāk aprakstītajos apstākļos.

b. Regulāri tiek veikta valsts akciju sabiedrību un šauram lokam piederošu uzņēmumu, tostarp privātuma vairoga organizāciju, revīzija. Priekšlaicīgi izpaužot informāciju par šādām revīzijām, jo īpaši tām, kurās izskata iespējamus pārkāpumus, var tās nelabvēlīgi ietekmēt. Arī privātuma vairoga organizācijai, kas ir iesaistīta iespējamā apvienošanas vai pārņemšanas darījumā, būs jāveic "pienācīga pārbaude" vai jākļūst par tās subjektu. Saistībā ar šādu pārbaudi nereti tiek vākti un apstrādāti personas dati, piemēram, informācija par augstākā līmeņa vadītājiem un citiem galvenajiem darbiniekiem. Priekšlaicīga informācijas izpaušana varētu izraisīt darījuma kavēšanos vai pat būt pretrunā piemērojamiem drošības noteikumiem. Pienācīgas rūpības pārbaudē iesaistītie investīciju baņķieri un advokāti vai revidenti, kas veic revīziju, var informāciju apstrādāt bez indivīda ziņas vienīgi tiktāl un tikai tādu laikposmu, kas ir vajadzīgs, lai izpildītu likumā noteiktās vai ar sabiedrības interesēm saistītās prasības, un citos apstākļos, kad šo principu piemērošana kaitētu organizācijas likumīgajām interesēm. Šīs likumīgās intereses ir, piemēram, uzraudzīt, vai organizācijas ievēro savas juridiskās saistības, un likumīgas grāmatvedības darbības, kā arī tādas konfidencialitātes nepieciešamība, kas ir saistīta ar iespējamu iegādi, apvienošanos, kopuzņēmumiem vai citiem līdzīgiem darījumiem, ko veic investīciju baņķieri vai revidenti.

5. **Datu aizsardzības iestāžu loma**

a. Organizācijas īstenos savu apņemšanos sadarboties ar Eiropas Savienības datu aizsardzības iestādēm ("DAI"), kā aprakstīts turpmāk. Atbilstīgi privātuma vairogam tām ASV organizācijām, kuras saņem personas datus no ES, jāapņemas izmantot rezultatīvus mehānismus, ar ko nodrošināt privātuma vairoga principu ievērošanu. Konkrētāk, kā izklāstīts tiesību aizsardzības, izpildes panākšanas un atbildības principā, dalīborganizācijām jānodrošina: a) i) to indivīdu tiesību aizsardzība, uz kuriem dati attiecas, a) ii) paveiktā darba kontroles procedūras, ar ko pārbaudīt, vai apliecinājumi un apgalvojumi, ko tās ir izteikušas par savu privātuma nodrošināšanas praksi, ir patiesi, un a) iii) pienākums risināt problēmas, kas rodas saistībā ar principu neievērošanu, un sekas attiecībā uz šādām organizācijām. Ja organizācija stingri ievēro šeit izklāstītās prasības par sadarbību ar DAI, tā var izpildīt tiesību aizsardzības, izpildes panākšanas un atbildības principa a) i) un a) iii) punktu.

b. Organizācija apņemas sadarboties ar DAI, savā privātuma vairoga pašsertifikācijas iesniegumā Tirdzniecības ministrijai (sk. papildu principu par pašsertifikāciju) paziņojot, ka tā:

i. ir nolēmusi izpildīt privātuma vairoga tiesību aizsardzības, izpildes panākšanas un atbildības principa a) i) un a) iii) punkta prasības, apņemoties sadarboties ar DAI;

ii. sadarbosies ar DAI saistībā ar atbilstīgi privātuma vairogam iesniegto sūdzību izmeklēšanu un risināšanu; un

iii. ievēros visus DAI ieteikumus, ja tās ņem vērā, ka organizācijai jāveic īpaši pasākumi, lai ievērotu privātuma vairoga principus, tostarp pasākumi stāvokļa izlabošanai vai kompensācijas pasākumi to indivīdu labā, ko principu neievērošana ir ietekmējusi, un sniegs DAI rakstisku apstiprinājumu, ka šādi pasākumi ir veikti.

c. DAI komisiju darbība

i. DAI sadarbosies, sniedzot informāciju un ieteikumus šādā veidā:

1. DAI ieteikumus nodos ar DAI neformālas komisijas starpniecību, kas izveidota Eiropas Savienības līmenī un kas cita starpā palīdzēs nodrošināt saskaņotu un viendabīgu pieeju.

2. Komisija attiecīgajām ASV organizācijām sniegs ieteikumus par neatrisinātām indivīdu sūdzībām par tādas personiskās informācijas apstrādi, kas privātuma vairoga satvarā ir pārsūtīta no ES. Šie ieteikumi būs izstrādāti, lai nodrošinātu, ka privātuma vairoga principus piemēro pareizi, un tajos būs iekļauti tādi tiesiskās aizsardzības līdzekļi attiecīgajam(-iem) indivīdam(-iem), ko DAI uzskata par piemērotiem.

3. Komisija šādus ieteikumus sniegs, atbildot uz attiecīgo organizāciju pieprasījumiem un/vai nepastarpinātām indivīdu sūdzībām par organizācijām, kas ir apņēmušās sadarboties ar DAI privātuma vairoga īstenošanas nolūkā, vienlaikus iedrošinot un, ja vajadzīgs, palīdzot šādiem indivīdiem vispirms izmantot iekšējos sūdzību izskatīšanas mehānismus, ko organizācija var piedāvāt.

4. Ieteikumus sniegs tikai pēc tam, kad abām strīdā iesaistītajām pusēm būs bijusi pienācīga iespēja sniegt atsauksmes un visus pierādījumus, ko tās vēlas. Komisija centīsies ieteikumus sniegt, cik vien drīz to atļauj šī prasība par pienācīgu izskatīšanu. Parasti komisija centīsies sniegt ieteikumus 60 dienās pēc sūdzības vai pieprasījuma saņemšanas un, ja iespējams, ātrāk.

5. Ja tā sūdzības uzskatīs par pamatotām, komisija publicēs tai iesniegto sūdzību izskatīšanas rezultātus.

6. Ar komisijas starpniecību sniegtie ieteikumi neuzliek komisijai vai atsevišķām datu aizsardzības iestādēm nekādu atbildību.

ii. Kā iepriekš minēts, organizācijām, kas izvēlas šo strīdu izšķiršanas veidu, jāapņemas ievērot datu aizsardzības iestāžu ieteikumus. Ja 25 dienās no ieteikumu sniegšanas organizācija tos nav izpildījusi un nav pietiekami pamatojusi kavēšanos, komisija paziņos par savu nodomu vai nu nodot lietu Federālajai tirdzniecības komisijai, Transporta ministrijai vai citai ASV federālajai vai pavalsts iestādei, kam ir likumiskas pilnvaras veikt izpildes panākšanas darbības krāpšanas vai informācijas sagrozīšanas lietās, vai arī secināt, ka vienošanās par sadarbību ir būtiski pārkāpta un tāpēc uzskatāma par spēkā neesošu. Pēdējā gadījumā komisija informēs Tirdzniecības ministriju, lai tā varētu atbilstoši grozīt privātuma vairoga sarakstu. Ja organizācija neievēro apņemšanos sadarboties ar DAI, kā arī privātuma vairoga principus, saskaņā ar FTK likuma 5. pantu vai citu attiecīgu likumu var vērsties tiesā ar prasību par maldinošu praksi.

d. Ja organizācija vēlas, lai tās privātuma vairoga priekšrocības attiektos arī uz cilvēkresursu datiem, ko no ES pārsūta izmantošanai saistībā ar darba attiecībām, tai attiecībā uz šādiem datiem jāapņemas sadarboties ar DAI (sk. papildu principu par cilvēkresursu datiem).

e. Organizācijām, kas izvēlas šo variantu, būs jāmaksā gada maksa, kas ir noteikta, lai segtu komisijas darbības izmaksas, un tām var papildus prasīt segt visas vajadzīgās tulkošanas izmaksas, kuras rodas saistībā ar tādu pieprasījumu vai sūdzību izskatīšanu komisijā, kuri vērsti pret šīm organizācijām. Ikgadējais maksājums nepārsniedz USD 500 un ir zemāks mazākiem uzņēmumiem.

6. **Pašsertifikācija**

a. Organizācija saņem ar privātuma vairogu saistītās priekšrocības no dienas, kad ministrija – pēc tam, kad ir pārliecinājusies par organizācijas pašsertifikācijas iesnieguma pilnīgumu, – to ir iekļāvusi privātuma vairoga sarakstā.

b. Lai organizācija pašsertificētu privātuma vairoga ievērošanu, tai jāiesniedz ministrijai pašsertifikācijas iesniegums, ko topošās privātuma vairoga dalīborganizācijas vārdā ir parakstījusi tās amatpersona, un kurā ir iekļauta vismaz šāda informācija:

i. organizācijas nosaukums, pasta adrese, e-pasta adrese, telefona un faksa numuri;

ii. organizācijas darbību apraksts attiecībā uz personisko informāciju, kas saņemta no ES; kā arī

iii. organizācijas privātuma politikas apraksts attiecībā uz šādu personisko informāciju, tostarp norādot:

1. ja organizācijai ir publiska vietne, attiecīgo tīmekļa adresi, kurā ir pieejama privātuma politika, vai, ja organizācijai publiskas vietnes nav, norādot, kur sabiedrība privātuma politiku var apskatīt;

2. tās īstenošanas sākuma datumu;

3. kontaktinformāciju, ko izmantot saistībā ar sūdzību izskatīšanu, piekļuves pieprasījumiem un jebkādiem citiem ar privātuma vairogu saistītiem jautājumiem;

4. konkrētu oficiālo iestādi, kurai ir jurisdikcija uzklausīt visas pret organizāciju izvirzītās prasības par iespējami negodīgu vai maldinošu praksi un iespējamiem privātuma tiesību aktu vai noteikumu pārkāpumiem (un ka tā ir uzskaitīta principos vai to turpmākā pielikumā);

5. visu to privātuma programmu nosaukumus, kuru dalībniece organizācija ir;

6. pārbaudes metodi (piemēram, iekšēja, trešās personas veikta) (sk. papildu principu par pārbaudi); kā arī

7. neatrisināto sūdzību izmeklēšanas nolūkiem pieejamo neatkarīgo tiesību aizsardzības mehānismu.

c. Ja organizācija vēlas, lai tās privātuma vairoga priekšrocības attiektos arī uz cilvēkresursu informāciju, ko no ES pārsūta izmantošanai saistībā ar darba attiecībām, tā var šādi rīkoties tad, ja principos vai turpmākā principu pielikumā uzskaitītai oficiālajai iestādei ir jurisdikcija uzklausīt pret organizāciju ierosinātas prasības, kas izriet no cilvēkresursu informācijas apstrādes. Turklāt organizācijai tas jānorāda pašsertifikācijas iesniegumā un jāizsaka apņemšanās sadarboties ar attiecīgo ES iestādi vai iestādēm atbilstīgi piemērojamiem papildu principiem par cilvēkresursu datiem un datu aizsardzības iestāžu lomu, kā arī ievērot šo iestāžu sniegtos ieteikumus. Organizācijai arī jāiesniedz ministrijai tās cilvēkresursu privātuma politikas kopija un jānorāda, kur privātuma politiku var apskatīt darbinieki, uz kuriem tā attiecas.

d. Ministrija uzturēs privātuma vairoga sarakstu ar organizācijām, kas ir iesniegušas pilnīgus pašsertifikācijas iesniegumus, tādējādi nodrošinot privātuma vairoga priekšrocību pieejamību, un atjauninās šo sarakstu, pamatojoties uz ikgadējiem pašsertifikācijas iesniegumiem un paziņojumiem, kas saņemti saskaņā ar papildu principu par strīdu izšķiršanu un par izpildes panākšanu. Šie pašsertifikācijas iesniegumi jāiesniedz ne retāk kā reizi gadā, Pretējā gadījumā organizāciju svītros no privātuma vairoga saraksta un tā vairs nesaņems no privātuma vairoga izrietošās priekšrocības. Gan privātuma vairoga sarakstu, gan organizāciju pašsertifikācijas iesniegumus darīs publiski pieejamus. Visām organizācijām, ko ministrija ir iekļāvusi privātuma vairoga sarakstā, attiecīgajos publicētajos privātuma politikas paziņojumos jānorāda, ka tās stingri ievēro privātuma vairoga

principus. Ja organizācijas privātuma politika ir pieejama tiešsaistē, tajā jāiekļauj hipersaite uz ministrijas privātuma vairoga tīmekļa vietni un hipersaite uz neatrisināto sūdzību izmeklēšanai pieejamā neatkarīgā tiesību aizsardzības mehānisma tīmekļa vietni vai sūdzības iesniegšanas veidlapu.

e. Privātuma principus piemēro no sertifikācijas brīža. Tā kā tie ietekmēs komercattiecības ar trešajām personām, organizācijas, kas sertificē privātuma vairoga regulējuma ievērošanu pirmajos divos mēnešos pēc regulējuma piemērošanas sākuma datuma, nodrošina pašreizējo komercattiecību ar trešajām personām atbilstību atbildības par tālākpārsūtīšanu principam iespējami drīz un noteikti ne vēlāk kā deviņu mēnešu laikā no datuma, kurā tās sertificēja privātuma vairoga ievērošanu. Šajā pagaidu periodā, organizācijas, pārsūtot datus trešajai personai, pirmkārt, piemēro informēšanas un izvēles principus un, otrkārt, ja personas datus pārsūta trešajai personai, kura darbojas kā pārstāvis, pārliecinās, ka tai ir pienākums nodrošināt vismaz tādu pašu aizsardzības līmeni, kāds ir prasīts principos.

f. Organizācijai jāpiemēro privātuma vairoga principi visiem personas datiem, kas no ES saņemti, pamatojoties uz privātuma vairogu. Apņemšanās stingri ievērot privātuma vairoga principus laika ziņā nav ierobežota attiecībā uz personas datiem, kas saņemti periodā, kad organizācija izmanto privātuma vairoga priekšrocības. Organizācijas apņemšanās nozīmē, ka tā turpinās šādiem datiem piemērot principus tik ilgi, kamēr organizācija tos glabās, izmantos vai izpaudīs, pat ja pēcāk tā kāda iemesla dēļ no privātuma vairoga izstāsies. Organizācijai, kas izstājas no privātuma vairoga, taču vēlas attiecīgos datus glabāt arī turpmāk, katru gadu jāapstiprina ministrijai apņemšanās turpināt principu piemērošanu vai nodrošināt "pienācīgu" informācijas aizsardzību ar citiem atļautiem līdzekļiem (piemēram, izmantojot līgumu, kurā ir pilnīgi atspoguļotas attiecīgo Eiropas Komisijas pieņemto standarta līguma klauzulu prasības); citādi organizācijai informācija jāatdod atpakaļ vai jādzēš. Organizācijai, kas izstājas no privātuma vairoga, jādzēš no attiecīgās privātuma politikas visas atsauces uz privātuma vairogu, kuras norāda, ka organizācija aktīvi turpina piedalīties privātuma vairogā un ir tiesīga saņemt ar to saistītās priekšrocības.

g. Organizācijai, kas apvienošanās vai pārņemšanas rezultātā pārstās pastāvēt kā atsevišķa juridiska persona, par to iepriekš jāpaziņo ministrijai. Paziņojumā arī būtu jānorāda, vai iegūstošajai juridiskajai personai vai juridiskajai personai, kas radīsies apvienošanās rezultātā, i) privātuma vairoga principi arī turpmāk būs saistoši saskaņā ar tiesību aktu, kas reglamentē pārņemšanu vai apvienošanos, vai ii) tā izvēlas pati apliecināt, ka tā stingri ievēro privātuma vairoga principus, vai ieviest citus aizsardzības pasākumus, piemēram rakstisku vienošanos, kas nodrošinās privātuma vairoga principu stingru ievērošanu. Ja nepiemēro ne i), nedz ii) punktu, visi personas dati, kas iegūti saistībā ar privātuma vairogu, nekavējoties jāizdzēš.

h. Ja organizācija kāda iemesla dēļ pārtrauc dalību privātuma vairogā, tai jādzēš visi paziņojumi, kas norāda, ka tā turpina piedalīties vairogā vai ir tiesīga saņemt no tā izrietošās priekšrocības. Ja tiek izmantota ES un ASV privātuma vairoga sertifikācijas zīme, arī tā ir jānoņem. FTK vai cita attiecīga valdības iestāde var tiesiski apstrīdēt jebkuru plašai sabiedrībai sniegtu sagrozītu paziņojumu par to, ka organizācija stingri ievēro privātuma vairoga principus. Ja ministrijai tiek sniegta sagrozīta informācija, var piemērot sankcijas saskaņā ar Likumu par nepatiesu ziņu sniegšanu (*False Statements Act*) (*18 U.S.C. § 1001*).

7. **Verifikācija**

a. Organizācijām ir jānodrošina paveiktā darba kontroles procedūras, ar ko pārbaudīt, vai apliecinājumi un apgalvojumi, ko tās ir izteikušas par savu privātuma vairoga praksi, ir patiesi un vai šo praksi īsteno, kā aprakstīts, un atbilstīgi privātuma vairoga principiem.

b. Lai izpildītu tiesību aizsardzības, izpildes panākšanas un atbildības principa prasības par pārbaudi, organizācijai šādi apliecinājumi un apgalvojumi jāapstiprina vai nu ar pašnovērtēšanu, vai arī ārējām atbilstības pārbaudēm.

c. Ja tiek īstenota pašnovērtēšanas pieeja, šādā pārbaudē jānorāda, vai organizācijas publicētā privātuma politika attiecībā uz personisko informāciju, kas saņemta no ES, ir precīza, visaptveroša, izvietota redzamā vietā, pilnīgi īstenota un pieejama. Pārbaudē arī jānorāda, vai organizācijas privātuma politika atbilst privātuma vairoga principiem; ka indivīdi ir informēti par iekšējo sūdzību izskatīšanas kārtību un par neatkarīgiem mehānismiem, ar kuriem viņi var iesniegt sūdzību; ka tai ir izstrādātas darbinieku apmācības procedūras, lai politiku īstenotu, un procedūras darbinieku sodīšanai par tās neievērošanu; un ka tai ir izstrādātas iekšējās procedūras, kā veikt

periodisku, objektīvu pārskatīšanu attiecībā uz iepriekš minēto. Paziņojums, kas apliecina pašnovērtēšanu, vismaz reizi gadā jāparaksta organizācijas amatpersonai vai citam organizācijas pilnvarotam pārstāvim un jāuzrāda pēc indivīdu pieprasījuma vai saistībā ar izmeklēšanu vai sūdzību par neatbilstību.

d. Ja organizācija ir izvēlējusies ārēju atbilstības pārbaudi, šādai pārbaudei ir jāparāda, ka privātuma politika attiecībā uz personisko informāciju, kas saņemta no ES, atbilst privātuma vairoga principiem, ka to ievēro un ka indivīdi ir informēti par mehānismiem, ar kuriem viņi var iesniegt sūdzības. Pārbaudes metodes var neierobežoti un atbilstoši vajadzībai ietvert revīziju, izlases veida pārskatīšanu, "mānekļu" vai tehnoloģisku rīku izmantošanu. Paziņojums, kas apliecina ārējas atbilstības pārbaudes veiksmīgu īstenošanu, vismaz reizi gadā jāparaksta vai nu pārbaudes veicējam, vai arī organizācijas amatpersonai vai citam organizācijas pilnvarotam pārstāvim un jāuzrāda pēc indivīdu pieprasījuma vai saistībā ar izmeklēšanu vai sūdzību par neatbilstību.

e. Organizācijām jāglabā savas atskaites par privātuma vairoga prakses īstenošanu un pēc pieprasījuma saistībā ar izmeklēšanu vai sūdzību par neatbilstību jāuzrāda tās neatkarīgai iestādei, kas ir atbildīga par sūdzību izmeklēšanu, vai iestādei, kuras jurisdikcijā ir negodīgas un maldinošas prakses lietas. Organizācijām ir arī ātri jāatbild uz ministrijas jautājumiem un citiem informācijas pieprasījumiem par principu stingru ievērošanu organizācijā.

8. **Piekļuve**

a. Piekļuves principa īstenošana praksē

i. Saskaņā ar privātuma vairoga principiem būtisks privātuma aizsardzības priekšnosacījums ir piekļuves tiesības. Jo īpaši, tās ļauj indivīdiem pārliecināties par tās informācijas precizitāti, ko par viņiem glabā. Piekļuves princips nozīmē, ka indivīdiem ir tiesības:

1. iegūt no organizācijas apstiprinājumu par to, vai tā apstrādā vai neapstrādā ar viņiem saistītus personas datus ([1]);

2. uz datu paziņošanu, lai viņi varētu pārbaudīt to precizitāti un apstrādes likumību; kā arī

3. uz datu labošanu, grozīšanu vai dzēšanu, ja tie ir neprecīzi vai apstrādāti, pārkāpjot principus.

ii. Indivīdiem nav jāpamato pieprasījumi piekļūt saviem personas datiem. Atbildot uz indivīdu piekļuves pieprasījumiem, organizācijām visupirms būtu jāņem vērā pieprasījuma iemesls(-i). Piemēram, ja piekļuves pieprasījums ir neskaidrs vai attiecas uz plašu jomu, organizācija var sākt ar indivīdu dialogu, lai labāk saprastu pieprasījuma cēloni un atrastu attiecīgo informāciju. Organizācija varētu jautāt, ar kuru organizācijas daļu(-ām) indivīds ir sazinājies, vai par tās informācijas veidu vai izmantojumu, kurai prasa piekļuvi.

iii. Ņemot vērā piekļuves pamatbūtību, organizācijām vienmēr būtu godprātīgi jācenšas piekļuvi nodrošināt. Piemēram, ja konkrēta informācija jāaizsargā un to var viegli nošķirt no pārējās personiskās informācijas, kurai prasa piekļuvi, tad organizācijai būtu jānošķir aizsargājamā informācija un jādara pieejama pārējā informācija. Ja organizācija nosaka, ka piekļuve kādā konkrētā gadījumā būtu jāierobežo, tai indivīdam, kas prasa piekļuvi, būtu jāpaskaidro, kāpēc ir pieņemts šāds lēmums, un jānorāda, kur var saņemt papildu informāciju.

b. Ar piekļuves nodrošināšanu saistītais apgrūtinājums vai izmaksas

i. Tiesības piekļūt personas datiem var ierobežot izņēmuma apstākļos, ja ar šādu piekļuvi tiktu pārkāptas citu personu likumīgās tiesības vai ar piekļuves nodrošināšanu saistītais apgrūtinājums vai izmaksas būtu nesamērīgas attiecīgajā gadījumā radītajiem indivīda privātuma apdraudējumiem. Izmaksas un apgrūtinājums ir svarīgi faktori, un tie būtu jāņem vērā, taču tie nav galvenie aspekti, nosakot, vai piekļuves nodrošināšana ir pamatota.

([1]) Organizācijai būtu jāatbild uz indivīda pieprasījumiem par apstrādes mērķiem, attiecīgo personas datu kategorijām un saņēmējiem vai saņēmēju kategorijām, kam izpauž personas datus.

ii. Piemēram, ja personisko informāciju izmanto, lai pieņemtu lēmumus, kas indivīdu būtiski ietekmēs (piemēram, par tādu svarīgu priekšrocību kā apdrošināšana, hipotēka vai darbs piešķiršanu vai atteikšanu), atbilstīgi šo papildu principu pārējiem noteikumiem organizācijai informācija būtu jāizpauž arī tad, ja tās sniegšana būtu diezgan sarežģīta vai dārga. Ja pieprasītā personiskā informācija nav sensitīva vai to neizmanto, pieņemot lēmumus, kas būtiski ietekmēs indivīdu, un tā ir gatava, pieejama un nerada lielas sniegšanas izmaksas, organizācijai būtu jānodrošina piekļuve šādai informācijai.

c. Konfidenciāla komercinformācija

i. Konfidenciāla komercinformācija ir informācija, attiecībā uz kuru organizācija ir veikusi pasākumus, lai nepieļautu tās izpaušanu, ja izpaušana palīdzētu kādam konkurentam tirgū. Organizācijas var liegt vai ierobežot piekļuvi, ja pilnīgas piekļuves nodrošināšana atklātu viņu pašu konfidenciālu komercinformāciju, piemēram, secinājumus par tirgvedību vai organizācijas izveidoto klasifikāciju, vai citu konfidenciālu komercinformāciju, uz ko attiecas konfidencialitātes līgumsaistības.

ii. Ja konfidenciālu komercinformāciju var viegli nošķirt no pārējās personiskās informācijas, kurai prasa piekļuvi, organizācijai būtu jānošķir konfidenciālā komercinformācija un jādara pieejama nekonfidenciālā informācija.

d. Datubāzu sakārtošana

i. Organizācija var sniegt piekļuvi, izpaužot indivīdam attiecīgo personisko informāciju; tai nav jānodrošina indivīdam piekļuve organizācijas datubāzei.

ii. Piekļuve jāsniedz tikai tad, ja organizācija glabā personisko informāciju. Piekļuves princips nerada pienākumu saglabāt, uzturēt, pārkārtot vai pārstrukturēt datnes ar personisko informāciju.

e. Kad var ierobežot piekļuvi

i. Tā kā organizācijām vienmēr godprātīgi jācenšas nodrošināt indivīdiem piekļuvi viņu personas datiem, tās var šādu piekļuvi ierobežot tikai noteiktos apstākļos un visiem piekļuves ierobežošanas iemesliem jābūt konkrētiem. Saskaņā ar direktīvu organizācija var ierobežot piekļuvi informācijai, ja tās izpaušana var būt pretrunā svarīgu sabiedrības interešu aizsardzībai, piemēram, valsts drošībai, aizsardzībai vai sabiedrības drošībai. Turklāt piekļuvi var liegt, ja personisko informāciju apstrādā tikai pētnieciskiem vai statistiskiem mērķiem. Citi iemesli, lai piekļuvi liegtu vai ierobežotu, ir šādi:

1. tiesību akta izpildes vai izpildes panākšanas vai privātas darbības kavēšana, tostarp pārkāpumu novēršana, izmeklēšana vai atklāšana, kā arī tiesības uz taisnīgu tiesu;

2. informācijas izpaušana, ja tā būtu pretrunā citu personu likumīgām tiesībām vai būtiskām interesēm;

3. juridiskas vai citas profesionālas priekšrocības neievērošana vai pienākuma neizpilde;

4. kaitējums darbinieku drošības izmeklēšanai vai šķīrējtiesas procesiem vai saistībā ar plāniem par jaunu darbinieku pieņemšanu un uzņēmuma reorganizāciju; vai

5. apdraudējums konfidencialitātei, kas jāievēro saistībā ar pareizas pārvaldības uzraudzības, pārbaudes vai regulatīvajām funkcijām, vai turpmākās vai jau notiekošās sarunās, kurās ir iesaistīta organizācija.

ii. Organizācijai, kas apgalvo, ka jāpiemēro izņēmums, ir pienākums pierādīt tā nepieciešamību, un tai būtu jānorāda indivīdiem piekļuves ierobežošanas iemesli, kā arī, kur tie var saņemt papildu informāciju.

f. Tiesības saņemt apstiprinājumu un iekasēt samaksu, lai segtu piekļuves nodrošināšanas izmaksas

i. Indivīdam ir tiesības saņemt apstiprinājumu par to, vai konkrētās organizācijas rīcībā ir ar viņu saistīti personas dati. Indivīdam arī ir tiesības pieprasīt, lai viņam paziņo ar viņu saistītos personas datus. Organizācija drīkst iekasēt samērīgu samaksu.

ii. Maksas iekasēšana ir pamatota, piemēram, tad, ja piekļuves pieprasījumi ir acīmredzami pārmērīgi, jo īpaši, ja tie ir atkārtoti.

iii. Piekļuvi nedrīkst atteikt, pamatojoties uz izmaksām, ja indivīds piedāvā tās segt.

g. Atkārtoti vai apgrūtinoši piekļuves pieprasījumi

Organizācija var saprātīgi ierobežot to, cik reižu noteiktā laikposmā tiks izpildīti viena indivīda iesniegtie piekļuves pieprasījumi. Nosakot šādus ierobežojumus, organizācijai būtu jāņem vērā tādi faktori kā informācijas atjaunināšanas biežums, datu izmantošanas mērķis un informācijas raksturs.

h. Krāpnieciski piekļuves pieprasījumi

Organizācijai jānodrošina piekļuve tikai tad, ja tai ir iesniegta pietiekama informācija, kas apstiprina pieprasījuma iesniedzēja identitāti.

i. Atbildēšanas termiņš

Organizācijām būtu jāatbild uz piekļuves pieprasījumiem saprātīgā laikposmā, ar pieņemamām metodēm un indivīdam saprotamā veidā. Organizācija, kas regulāri sniedz datu subjektiem informāciju, individuālu piekļuves pieprasījumu var izpildīt informācijas kārtējās izpaušanas satvarā, ja vien šādi netiktu izraisīta pārmērīga kavēšanās.

9. **Dati par cilvēkresursiem**

a. Privātuma vairoga tvērums

i. Ja ES organizācija pārsūta pakalpojumu sniedzējam no Amerikas Savienotajām Valstīm, kas ir tās mātesuzņēmums, filiāle vai ar to nesaistīta struktūra un kas piedalās privātuma vairogā, tādu personisko informāciju par saviem (pašreizējiem vai bijušajiem) darbiniekiem, kura ir savākta saistībā ar darba attiecībām, uz pārsūtīšanu attiecas ar privātuma vairogu saistītās priekšrocības. Tādos gadījumos uz informācijas vākšanu un tās apstrādi pirms nosūtīšanas attiecas tās ES valsts tiesību akti, kurā informācija savākta, un jāievēro visi nosacījumi vai ierobežojumi attiecībā uz tās nosūtīšanu atbilstīgi šiem tiesību aktiem.

ii. Privātuma vairoga principus piemēro, tikai pārsūtot atsevišķi identificētus datus vai tiem piekļūstot. Statistikas ziņojumi, kuros izmantoti apkopoti nodarbinātības dati un kuros nav personas datu, un anonimizētu datu izmantošana nerada bažas par privātumu.

b. Informēšanas un izvēles principu piemērošana

i. ASV organizācija, kas saskaņā ar privātuma vairogu ir no ES saņēmusi informāciju par darbiniekiem, drīkst to izpaust trešajām personām vai izmantot atšķirīgiem mērķiem vienīgi atbilstīgi informēšanas un izvēles principiem. Piemēram, ja organizācija ir paredzējusi darba attiecību laikā savāktu personisko informāciju izmantot ar nodarbinātību nesaistītiem mērķiem, piemēram, tirdzniecības paziņojumu izstrādei, ASV organizācijai pirms tam jādod attiecīgajiem indivīdiem nepieciešamā izvēle, ja vien tie jau nav atļāvuši informāciju izmantot šādiem mērķiem. Šāda izmantošana nedrīkst būt pretrunā mērķiem, kuriem personas dati ir vākti vai kuriem indivīds pēc tam atļāvis to izmantot. Turklāt šādu izvēli nedrīkst izmantot, lai ierobežotu darba iespējas vai šādus darbiniekus jebkādā veidā sodītu.

ii. Jāpiebilst, ka atsevišķi vispārēji piemērojami nosacījumi attiecībā uz pārsūtīšanu no dažām ES dalībvalstīm var liegt šādu informāciju izmantot citādi pat pēc pārsūtīšanas ārpus ES, un šādi nosacījumi ir jāievēro.

iii. Turklāt darba devējiem jādara viss iespējamais, lai ievērotu darbinieku vēlmes attiecībā uz slepenību. Viņi varētu, piemēram, ierobežot piekļuvi personas datiem, anonimizēt konkrētus datus vai piešķirt kodus vai pseidonīmus, ja attiecīgā pārvaldības mērķa īstenošanai īstie vārdi nav vajadzīgi.

iv. Organizācijai nav jāpiemēro informēšanas un izvēles principi, ciktāl un tādu laikposmu, kas ir vajadzīgs, lai nemazinātu tās spēju paaugstināt amatā vai nolīgt darbiniekus un pieņemt citus līdzīgus lēmumus par nodarbinātību.

c. Piekļuves principa piemērošana

Papildu principā par piekļuvi ir sniegti norādījumi par iemesliem, kas var pamatot ar cilvēkresursiem saistīta piekļuves pieteikuma noraidīšanu vai ierobežošanu. Protams, Eiropas Savienības darba devējiem jāievēro vietējie noteikumi un jānodrošina, ka Eiropas Savienības darbiniekiem ir piekļuve šādai informācijai, kā to prasa viņu mītnes valsts tiesību akti, neatkarīgi no datu apstrādes un uzglabāšanas vietas. Privātuma vairogs paredz, ka organizācijai, kas šādus datus apstrādā Amerikas Savienotajās Valstīs, ir jāsadarbojas, sniedzot šādu piekļuvi tieši vai ar ES darba devēja starpniecību.

d. Izpildes panākšana

i. Ciktāl personisko informāciju izmanto tikai saistībā ar darba attiecībām, par darbinieku datiem atbildīga pirmkārt ir ES organizācija. Tātad, ja Eiropas darbinieki sūdzas par viņu datu aizsardzības tiesību pārkāpumiem un nav apmierināti ar iekšējās pārbaudes, sūdzības un pārsūdzības procedūru rezultātiem (vai piemērojamām šķīrējtiesas procedūrām, ko veic atbilstīgi līgumam ar arodbiedrību), viņi būtu jānosūta uz pavalsts vai valsts datu aizsardzības iestādi vai uz iestādi, kas ir atbildīga par darba jautājumiem, tajā jurisdikcijā, kur darbinieki strādā. Tas attiecas arī uz gadījumiem, kad par viņu personiskās informācijas iespējami pretlikumīgu apstrādi ir atbildīga tā ASV organizācija, kas ir saņēmusi informāciju no darba devēja, un tādējādi tas nozīmē, ka, iespējams, ir pārkāpti privātuma vairoga principi. Tas ir visefektīvākais veids, kā atrisināt bieži sastopamos gadījumus, kad tiesības un pienākumi, kas ir noteikti vietējā darba likumā, darba līgumos un datu aizsardzības likumā, daļēji sakrīt.

ii. Tāpēc ASV organizācijai, kas piedalās privātuma vairoga programmā, izmanto ES datus par cilvēkresursiem, kuri no Eiropas Savienības pārsūtīti saistībā ar darba attiecībām, un vēlas, lai uz šādu pārsūtīšanu attiektos privātuma vairogs, jāapņemas šādos gadījumos sadarboties ar kompetentajām ES iestādēm izmeklēšanā un ievērot to ieteikumus.

e. Atbildības par tālākpārsūtīšanu principa piemērošana

Ja privātuma vairoga organizācijai rodas neregulāras ar nodarbinātību saistītas operatīvās vajadzības attiecībā uz personas datiem, ko pārsūta privātuma vairoga satvarā, piemēram, lidojuma, viesnīcas numura rezervāciju vai apdrošināšanas segumu, neliela darbinieku skaita personas datus var pārsūtīt pārziņiem, nepiemērojot piekļuves principu un neslēdzot līgumu ar pārzini, kas ir trešā persona, kā tiek prasīts citkārt saskaņā ar atbildību par tālākpārsūtīšanu, ja vien privātuma vairoga organizācija ir izpildījusi informēšanas un izvēles principus.

10. **Obligāti līgumi par tālākpārsūtīšanu**

a. Datu apstrādes līgumi

i. Ja personas datus no ES uz Amerikas Savienotajām Valstīm pārsūta tikai apstrādei, neatkarīgi no tā, vai apstrādātājs piedalās privātuma vairogā, ir vajadzīgs līgums.

ii. Eiropas Savienības datu pārziņiem vienmēr jānoslēdz līgums, ja notiek pārsūtīšana tikai apstrādei, neatkarīgi no tā, vai apstrādes darbību veic ES vai ārpus tās, un tā, vai apstrādātājs ir vai nav privātuma vairoga dalībnieks. Līguma mērķis ir nodrošināt, ka datu apstrādātājs:

1. rīkojas tikai saskaņā ar pārziņa norādījumiem;

2. īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai aizsargātu personas datus no nejaušas vai nelikumīgas iznīcināšanas vai nejaušas pazaudēšanas, pārveidošanas, nesankcionētas izpaušanas vai piekļuves, un saprot, vai tālākpārsūtīšana ir atļauta; kā arī

3. ņemot vērā apstrādes veidu, palīdz pārzinim atbildēt indivīdiem, kas izmanto savas no principiem izrietošās tiesības.

iii. Tā kā privātuma vairoga dalībnieki nodrošina pienācīgu aizsardzību, lai noslēgtu ar viņiem līgumus tikai par apstrādi, nav vajadzīga iepriekšēja atļauja (vai arī šādu atļauju automātiski piešķir ES dalībvalstis), kas būtu nepieciešama līgumiem ar saņēmējiem, kuri nepiedalās privātuma vairogā un nenodrošina pienācīgu aizsardzību citā veidā.

b. Pārsūtīšana kontrolētā uzņēmumu vai struktūru grupā

Ja personisko informāciju pārsūta starp diviem pārziņiem kontrolētā uzņēmumu vai struktūru grupā, saskaņā ar atbildības par tālākpārsūtīšanu principu līgums ne vienmēr ir nepieciešams. Datu pārziņi, kas darbojas kontrolētā uzņēmumu vai struktūru grupā, var datus šādi pārsūtīt, pamatojoties uz citiem instrumentiem, piemēram, ES saistošiem uzņēmumu noteikumiem vai citiem grupas līmeņa instrumentiem (piemēram, atbilstības un kontroles programmām), kas nodrošina privātuma vairoga satvarā sniegtās personiskās informācijas aizsardzības turpināmību. Šādas datu pārsūtīšanas gadījumā privātuma vairoga organizācijai joprojām ir jānodrošina atbilstība principiem.

c. Pārsūtīšana starp pārziņiem

Datus var pārsūtīt starp pārziņiem arī tad, ja saņēmējs pārzinis nav privātuma vairoga organizācija un nav nodrošinājis neatkarīgu tiesību aizsardzības mehānismu. Privātuma vairoga organizācijai ar saņēmēju-pārzini, kas ir trešā persona, jānoslēdz līgums, kas nodrošina tādu pašu aizsardzības līmeni, kāds ir pieejams saskaņā ar privātuma vairogu, nenosakot, ka pārzinim, kas ir trešā persona, jābūt privātuma vairoga organizācijai vai nodrošinājušam neatkarīgu tiesību aizsardzības mehānismu, ja vien tas dara pieejamu līdzvērtīgu mehānismu.

11. **Strīdu izšķiršana un izpildes panākšana**

a. Tiesību aizsardzības, izpildes panākšanas un atbildības princips nosaka prasības attiecībā uz privātuma vairoga izpildes panākšanu. Tas, kā izpildīt šā principa a) punkta ii) apakšpunkta prasības, ir izklāstīts papildu principā par pārbaudi. Šis papildu princips attiecas uz a) punkta i) un iii) apakšpunktu, kuros ir prasīts nodrošināt neatkarīgus tiesību aizsardzības mehānismus. Šie mehānismi var būt dažādi, taču tiem jāatbilst tiesību aizsardzības, izpildes panākšanas un atbildības principa prasībām. Organizācijas šīs prasības izpilda šādi: i) ievērojot privātajā sektorā izstrādātas privātuma programmas, kuru noteikumos iekļauti privātuma vairoga principi un kas ietver rezultatīvus tāda veida izpildes panākšanas mehānismus, kas aprakstīti tiesību aizsardzības, izpildes panākšanas un atbildības principā; ii) pakļaujoties juridiskām vai reglamentējošām uzraudzības iestādēm, kas nosaka indivīdu sūdzību izskatīšanu un strīdu izšķiršanu; vai iii) apņemoties sadarboties ar datu aizsardzības iestādēm, kas atrodas Eiropas Savienībā, vai to pilnvarotajiem pārstāvjiem.

b. Šis saraksts ir aptuvens un nerada ierobežojumus. Privātais sektors var izstrādāt papildu mehānismus, ar ko nodrošināt izpildi, ja vien tie atbilst tiesību aizsardzības, izpildes panākšanas un atbildības principa, kā arī papildu principu prasībām. Jāpiebilst, ka tiesību aizsardzības, izpildes panākšanas un atbildības principa prasības

papildina prasību, ka pašregulatīvajiem centieniem jābūt izpildāmiem saskaņā ar Federālās tirdzniecības komisijas likuma 5. pantu, kurā ir aizliegtas negodīgas vai maldinošas darbības, vai arī saskaņā ar citiem tiesību aktiem vai noteikumiem, kuros aizliegta šāda rīcība.

c. Lai palīdzētu nodrošināt savu no privātuma vairoga izrietošo saistību izpildi un veicinātu programmas pārvaldību, organizācijām un to neatkarīgajiem tiesību aizsardzības mehānismiem jāsniedz ar privātuma vairogu saistīta informācija, kad ministrija to pieprasa. Organizācijām arī ātri jāatbild uz sūdzībām par to atbilstību principiem, kuras ar ministrijas starpniecību iesniegušas DAI. Atbildē būtu jānorāda, vai sūdzība ir pamatota un, ja tā ir pamatota, kā organizācija problēmu labos. Ministrija nodrošinās tās saņemtās informācijas konfidencialitāti saskaņā ar ASV tiesību aktiem.

d. Tiesību aizsardzības mehānismi

i. Pirms izmanto neatkarīgus tiesību aizsardzības mehānismus, patērētāji jārosina iesniegt sūdzības, kas viņiem var rasties par attiecīgo organizāciju. Organizācijām jāatbild patērētājam 45 dienu laikā no sūdzības saņemšanas. To, vai tiesību aizsardzības mehānisms ir neatkarīgs, var pierādīt ar faktiem, piemēram, objektivitāti, pārredzamu sastāvu un finansējumu, kā arī pierādītiem sasniegumiem. Kā prasīts tiesību aizsardzības, izpildes panākšanas un atbildības principā, indivīdiem pieejamai tiesību aizsardzībai jābūt gatavai, viegli pieejamai un bez maksas. Strīdu izšķiršanas iestādēm jāizskata visas sūdzības, kas saņemtas no indivīdiem, ja vien tās nav acīmredzami nepamatotas vai nenozīmīgas. Tas neliedz organizācijai, kas strādā ar tiesību aizsardzības mehānismu, noteikt atbilstības prasības, taču tām vajadzētu būt pārredzamām un pamatotām (piemēram, lai varētu izslēgt sūdzības, kas uz programmu neattiecas vai ir izskatāmas citā iestādē) un tās nedrīkstētu mazināt apņemšanos izskatīt pamatotas sūdzības. Turklāt ar tiesību aizsardzības mehānismiem indivīdiem jāsniedz pilnīga un viegli pieejama informācija par to, kā darbojas strīdu izšķiršanas procedūra, kad viņi iesniedz sūdzību. Šādā informācijā atbilstīgi privātuma vairoga principiem vajadzētu būt iekļautam paziņojumam par mehānisma privātuma aizsardzības praksi. Tiem arī būtu jāsadarbojas tādu līdzekļu izstrādē kā standarta sūdzību veidlapas, lai veicinātu sūdzību atrisināšanas procesu.

ii. Neatkarīgajiem tiesību aizsardzības mehānismiem savā publiskajā tīmekļa vietnē jāiekļauj informācija par privātuma vairoga principiem un pakalpojumiem, ko tie sniedz privātuma vairoga satvarā. Tajā jānorāda: 1) informācija par vai saite uz privātuma vairoga principu prasībām attiecībā uz neatkarīgiem tiesību aizsardzības mehānismiem; 2) saite uz ministrijas izstrādāto privātuma vairoga tīmekļa vietni; 3) paskaidrojums, ka privātuma vairoga satvarā sniegtos strīdu izšķiršanas pakalpojumus indivīdi var saņemt bez maksas; 4) apraksts par to, kā var iesniegt ar privātuma vairogu saistītu sūdzību; 5) ar privātuma vairogu saistītu sūdzību apstrādes laikposms; un 6) iespējamo tiesiskās aizsardzības līdzekļu apraksts.

iii. Neatkarīgajiem tiesību aizsardzības mehānismiem jāpublicē gada pārskats, kurā izklāstīta apkopota statistika par to strīdu izšķiršanas pakalpojumiem. Gada pārskatā jāiekļauj: 1) kopējais pārskata gada laikā saņemto ar privātuma vairogu saistīto sūdzību skaits; 2) saņemto sūdzību veidi; 3) strīdu izšķiršanas pasākumu kvalitātes rādītāji, piemēram, sūdzību apstrādei veltītais laiks; un 4) saņemto sūdzību iznākumi, jo īpaši noteikto tiesiskās aizsardzības līdzekļu vai sankciju skaits un veids.

iv. Kā norādīts I pielikumā, indivīds var izmantot šķīrējtiesas procesu, lai neatrisinātas sūdzības gadījumā tiktu noteikts, vai privātuma vairoga organizācija attiecībā uz šo indivīdu ir pārkāpusi no principiem izrietošos pienākumus un vai šāds pārkāpums ir pilnīgi vai daļēji neizlabots. Šī iespēja ir pieejama vienīgi minētajā nolūkā. To nevar izmantot, piemēram, attiecībā uz principu piemērošanas izņēmumiem ([1]) vai apgalvojumiem par privātuma vairoga nodrošinātās aizsardzības pietiekamību. Ja tiek izmantots šķīrējtiesas process, privātuma vairoga komisijai (kuras sastāvā atkarībā no pušu vienošanās ir viens vai trīs šķīrējtiesneši) ir pilnvaras noteikt individuālu, specifisku, nemonetāru un taisnīgu tiesiskās aizsardzības līdzekli (piemēram, piekļuvi, labošanu, dzēšanu vai attiecīgo indivīda datu atdošanu), kas vajadzīgs, lai labotu principu pārkāpumu vienīgi attiecībā uz indivīdu. Saskaņā ar Federālo šķīrējtiesas procesa likumu (*Federal Arbitration Act*) indivīdi un privātuma vairoga organizācijas varēs lūgt šķīrējtiesnešu lēmumu pārskatīšanu tiesā un izpildes panākšanu atbilstīgi ASV tiesību aktiem.

([1]) Principu I daļas 5. punkts.

e. Tiesiskās aizsardzības līdzekļi un sankcijas

Visu strīda izšķiršanas struktūras piešķirto tiesiskās aizsardzības līdzekļu rezultātā neatbilstība organizācijā būtu jānovērš vai jālabo, ciktāl tas ir praktiski iespējams, un jānodrošina, ka turpmāk organizācijas veiktā apstrāde atbildīs principiem un ka attiecīgā gadījumā to indivīdu personas datu apstrādi, kas ir iesnieguši sūdzību, pārtrauks. Sankcijām jābūt pietiekami stingrām, lai nodrošinātu, ka organizācija principus ievēro. Vairākas dažādas stingrības pakāpes sankcijas ļaus strīdu izšķiršanas iestādēm pienācīgi reaģēt uz dažādas pakāpes neatbilstību. Sankcijām būtu jāietver gan neatbilstības konstatējumu publicēšana, gan prasība konkrētos apstākļos datus dzēst ([1]). Citas sankcijas varētu ietvert darbības atļaujas apturēšanu un atņemšanu, atlīdzību indivīdiem par zaudējumiem, kas radušies neatbilstības rezultātā, un aizlieguma noteikšanu. Privātā sektora strīdu izšķiršanas struktūrām un pašregulatīvajām iestādēm par to, ka privātuma vairoga organizācijas neievēro to nolēmumus, jāziņo attiecīgi kompetentajai valdības iestādei vai tiesām un jāinformē par to ministrija.

f. FTK darbība

FTK ir apņēmusies prioritāri izskatīt pieprasījumus ar apgalvojumiem par principu neievērošanu, kurus iesniegušas: i) privātuma pašregulatīvās organizācijas un citas neatkarīgas strīdu izšķiršanas struktūras; ii) ES dalībvalstis; un iii) ministrija, lai noteiktu, vai ir pārkāpts FTK likuma 5. pants, kurā ir aizliegtas negodīgas vai maldinošas darbības vai šāda komercprakse. Ja FTK secina, ka tai ir pamats uzskatīt, ka 5. pants ir pārkāpts, tā var jautājumu risināt, pieprasot administratīvu rīkojumu par pretlikumīgas darbības pārtraukšanu, kurā apstrīdēto praksi aizliegtu, vai iesniedzot sūdzību federālajā apgabaltiesā; ja sūdzību apmierinās, federālā tiesa varētu pieņemt rīkojumu ar tādu pašu spēku. Tas attiecas arī uz nepatiesiem apgalvojumiem par privātuma vairoga principu stingru ievērošanu vai tādu organizāciju dalību privātuma vairogā, kuras vai nu vairs nav iekļautas privātuma vairoga sarakstā, vai arī nekad nav ministrijai pašsertificējušas tā ievērošanu. FTC var piemērot civiltiesiskas sankcijas par pretlikumīgas darbības pārtraukšanas rīkojuma neievērošanu un var ierosināt civillietas vai krimināllietas par federālās tiesas nolēmuma neievērošanu. FTK par visām tās veiktām šādām darbībām paziņo ministrijai. Ministrija aicina citas valdības iestādes tai ziņot par šādu lietu iznākumiem un citiem nolēmumiem, kas nosaka atbilstību privātuma vairoga principiem.

g. Pastāvīga neievērošana

i. Ja organizācija pastāvīgi neievēro principus, tā vairs nav tiesīga saņemt ar privātuma vairogu saistītās priekšrocības. Organizācijas, kas pastāvīgi neievēro principus, ministrija svītros no privātuma vairoga saraksta, un tām ir jāatdod atpakaļ vai jāizdzēš privātuma vairoga satvarā saņemtā personiskā informācija.

ii. Pastāvīga neievērošana ir tad, ja organizācija, kas ir pašsertificējusi ministrijai principu piemērošanu, atsakās ievērot kādas privātuma pašregulatīvās iestādes, neatkarīgas strīdu izšķiršanas struktūras vai valdības iestādes galīgo lēmumu vai ja šāda struktūra konstatē, ka organizācija bieži neievēro principus, ciktāl tās apgalvojums par atbilstību vairs nav ticams. Šādos gadījumos organizācijai par šādiem faktiem nekavējoties jāinformē ministrija. Pretējā gadījumā tai piemēro sankcijas saskaņā ar Likumu parnepatiesu ziņu sniegšanu (*18 U. S. C. § 1001*). Organizācijas atteikšanās no privātā sektora privātuma pašregulatīvās programmas vai neatkarīga strīdu izšķiršanas mehānisma to neatbrīvo no pienākuma izpildīt principus un būtu uzskatāma par pastāvīgu neievērošanu.

iii. Ministrija svītros organizāciju no privātuma vairoga saraksta, ja no pašas organizācijas, privātuma pašregulatīvās struktūras vai citas neatkarīgas strīdu izšķiršanas struktūras vai valdības iestādes saņems paziņojumu par pastāvīgu neievērošanu, par to brīdinot organizāciju, kas principus neievēro, 30 dienas iepriekš un dodot

([1]) Strīdu izšķiršanas iestādēm ir rīcības brīvība attiecībā uz apstākļiem, kuros tās šīs sankcijas izmanto. Viens no faktoriem, kas jāņem vērā, lemjot, vai būtu jāpieprasa datu dzēšana, ir to sensitivitāte; būtiski ir arī tas, vai organizācija informāciju ir ievākusi, izmantojusi vai izpaudusi klajā pretrunā privātuma vairoga principiem.

tai iespēju atbildēt. Tādējādi ministrijas uzturētais privātuma vairoga saraksts skaidri parādīs, kuras organizācijas saņem ar privātuma vairogu saistītās priekšrocības un kurām tādu vairs nav.

iv. Organizācijai, kas piesakās līdzdarboties pašregulatīvā struktūrā, lai atkal varētu pretendēt uz privātuma vairogu, jāsniedz šai struktūrai pilnīga informācija par tās iepriekšējo līdzdalību privātuma vairogā.

12. **Izvēle – atteikuma laiks**

a. Parasti izvēles principa mērķis ir nodrošināt, ka personisko informāciju izmanto un izpauž indivīda vēlmēm un izvēlei atbilstošos veidos. Tāpēc indivīdam būtu jāvar jebkurā laikā izvēlēties liegt personisko informāciju izmantot tiešai tirgvedībai, ievērojot samērīgus ierobežojumus, ko nosaka organizācija, piemēram, dodot organizācijai laiku atteikumu īstenot. Organizācija var arī prasīt pietiekamu informāciju, lai apstiprinātu tā indivīda identitāti, kas vēlas izmantošanu liegt. Amerikas Savienotās Valstīs indivīdi šo izvēli var realizēt, izmantojot centrālu atteikuma programmu, piemēram, Tiešas tirgvedības asociācijas pasta izvēles dienests. Organizācijām, kas līdzdarbojas Tiešas tirgvedības asociācijas pasta izvēles dienestā, būtu jāveicina tā pieejamība patērētājiem, kuri nevēlas saņemt komercinformāciju. Jebkurā gadījumā indivīdam šīs izvēles izdarīšanai piedāvā gatavus un viegli pieejamus mehānismus.

b. Līdzīgi organizācija var izmantot informāciju atsevišķiem tiešas tirgvedības mērķiem, kad nav iespējams pirms informācijas izmantošanas dot indivīdam iespēju izmantošanu liegt, ja tikām organizācija nekavējoties (un pēc pieprasījuma vienmēr) dod indivīdam iespēju (bez maksas) atteikties no turpmākas tirgvedības paziņojumu saņemšanas un organizācija ievēro indivīda vēlmes.

13. **Ceļojuma informācija**

a. Organizācijām, kas atrodas ārpus ES, vairākos gadījumos var pārsūtīt informāciju par aviosabiedrības pasažieru rezervāciju un citu ceļojuma informāciju, piemēram, informāciju par biežiem lidojumiem vai viesnīcas rezervāciju, kā arī informāciju par īpašām vajadzībām, piemēram, par reliģiskām prasībām atbilstošām maltītēm vai fizisku palīdzību. Saskaņā ar direktīvas 26. pantu personas datus var pārsūtīt "uz trešo valsti, kas nenodrošina pienācīgu aizsardzības līmeni 25. panta 2. punkta nozīmē", ja i) ir jāsniedz patērētāja prasītie pakalpojumi vai jāpilda vienošanās noteikumi, piemēram vienošanās par "biežiem lidojumiem"; vai ii) patērētājs tam ir skaidri piekritis. ASV organizācijas, kas ievēro privātuma vairoga principus, nodrošina personas datu pienācīgu aizsardzību un tāpēc var no ES saņemt pārsūtītos datus, neievērojot šos nosacījumus vai citus direktīvas 26. panta nosacījumus. Tā kā privātuma vairogs paredz īpašus noteikumus attiecībā uz sensitīvu informāciju, šādu informāciju (kas, iespējams, jāvāc, piemēram saistībā ar patērētāju vajadzību saņemt fizisku palīdzību) var iekļaut sūtījumos privātuma vairoga dalībniekiem. Tomēr visos gadījumos organizācijai, kas informāciju nosūta, jāievēro tās ES dalībvalsts tiesību akti, kurā tā darbojas, un tie, cita starpā, var paredzēt īpašus nosacījumus sensitīvu datu apstrādei.

14. **Farmaceitiski preparāti un medicīnas produkti**

a. <u>ES dalībvalstu tiesību aktu vai privātuma vairoga principu piemērošana</u>

Uz personas datu vākšanu un jebkādu apstrādi, kas notiek pirms pārsūtīšanas uz Amerikas Savienotajām Valstīm, attiecas ES dalībvalstu tiesību akti. Privātuma vairoga principus datiem piemēro, tiklīdz tie ir pārsūtīti uz Amerikas Savienotajām Valstīm. Dati, ko izmanto farmaceitiskos pētījumos un citiem mērķiem, vajadzības gadījumā jāpadara anonīmi.

b. Turpmāka zinātniskā pētniecība

i. Personas dati, kas ir izstrādāti īpašos medicīnas vai farmaceitiskos pētījumos, bieži ir ļoti noderīgi turpmākajā zinātniskajā pētniecībā. Ja personas datus, kas ir iegūti vienam zinātniskam pētījumam, pārsūta privātuma vairoga organizācijai no ASV, tā var datus izmantot jaunai zinātniskās pētniecības darbībai, ja pirms tam ir izpildīti informēšanas un izvēles principi. Informējot jāsniedz ziņas par visiem turpmākiem īpašiem datu izmantošanas mērķiem, piemēram, periodiskas paveiktā darba kontroles, saistītu pētījumu vai tirgvedības vajadzībām.

ii. Saprotams, ka nevar norādīt visus turpmākos datu izmantošanas mērķus, jo jauns pētījuma mērķis var rasties saistībā ar jaunu izpratni par sākotnējiem datiem, jauniem medicīnas atklājumiem un attīstību, kā arī izmaiņām sabiedrības veselības aizsardzībā un reglamentācijā. Tādēļ attiecīgajā gadījumā, informējot, jāsniedz paskaidrojums, ka personas datus var izmantot turpmākos medicīnas un farmaceitiskos pētījumos, kas nav paredzami. Ja izmantošanas veids neatbilst vispārīgajam pētījuma mērķim(-iem), kuram(-iem) dati sākotnēji savākti vai kuram(-iem) indivīds pēc tam piekritis, ir jāsaņem jauna piekrišana.

c. Dalības klīniskajā izpētē pārtraukšana

Dalībnieki var nolemt vai viņus var lūgt pārtraukt piedalīties klīniskajā izpētē jebkurā laikā. Visus personas datus, kas ir iegūti pirms dalības pārtraukšanas, drīkst turpināt apstrādāt kopā ar citiem datiem, kuri iegūti klīniskās izpētes gaitā, ja vien tas dalībniekam tika skaidri norādīts brīdī, kad viņš/viņa piekrita piedalīties.

d. Datu pārsūtīšana reglamentējošos un uzraudzības nolūkos

Farmācijas un medicīnas ierīču uzņēmumiem ir atļauts personiskos datus no ES veiktajiem klīniskajiem pētījumiem sniegt regulatoriem Amerikas Savienotajās Valstīs reglamentējošiem un uzraudzības mērķiem. Ar nosacījumu, ka tiek ievēroti informēšanas un izvēles principi, līdzīga pārsūtīšana ir atļauta pusēm, kas nav regulatīvas struktūras, piemēram, uzņēmumiem un citiem pētniekiem.

e. "Slēptie" pētījumi

i. Lai nodrošinātu objektivitāti daudzos klīniskajos pētījumos, dalībniekiem un bieži vien arī izmeklētājiem nevar piešķirt piekļuvi informācijai par to, kā katru dalībnieku ārstē. Tas apdraudētu zinātnisko pētījumu un rezultātu pamatotību. Šādas klīniskās izpētes (dēvēta par "slēptajiem" pētījumiem) dalībniekiem izpētes laikā nav jāsaņem piekļuve datiem par viņu ārstēšanu, ja šis ierobežojums tika izskaidrots, kad dalībnieks iesaistījās izpētē, un ja šādas informācijas izpaušana apdraudētu veikto pētījumu integritāti.

ii. Vienošanās par dalību izpētē saskaņā ar šiem nosacījumiem ir pamatota atteikšanās no tiesībām uz piekļuvi. Pēc izpētes slēdziena saņemšanas un rezultātu analīzes dalībniekiem jābūt piekļuvei saviem datiem, ja viņi to prasa. Piekļuve visupirms būtu jālūdz ārstam vai citam veselības aprūpes sniedzējam, kas viņus klīniskās izpētes laikā ārstēja, un pēc tam – sponsorējošajai organizācijai.

f. Produktu drošuma un iedarbīguma uzraudzība

Farmācijas vai medicīnas ierīču uzņēmumam nav jāpiemēro privātuma vairoga principi – informēšanas, izvēles, atbildības par tālākpārsūtīšanu un piekļuves principi –, veicot savu produktu drošuma un iedarbīguma uzraudzību, tostarp ziņojot par blakusefektiem un sekojot līdzi tādiem pacientiem/subjektiem, kas izmanto konkrētas zāles vai medicīnas ierīces, ciktāl principu stingra ievērošana traucē reglamentējošu prasību izpildi. Tas

attiecas gan, piemēram, uz veselības aprūpes sniedzēju ziņojumiem farmācijas un medicīnas ierīču uzņēmumiem, gan uz farmācijas un medicīnas ierīču uzņēmumu ziņojumiem tādām valdības aģentūrām kā Pārtikas un zāļu pārvalde.

g. Ar šifru kodēti dati

Galvenais izmeklētājs sākotnējos pētījumu datus vienmēr ir īpaši kodējis ar šifru tā, lai neatklātu atsevišķu datu subjektu identitāti. Farmācijas uzņēmumi, kas šādu pētījumu sponsorē, šifru nesaņem. Īpaši šifrētais kods ir pieejams tikai pētniekam, lai īpašos apstākļos viņš varētu pētījuma subjektu identificēt (piemēram, ja tam pēcāk ir vajadzīga medicīniska uzraudzība). Šādi kodētu datu pārsūtīšana no ES uz Amerikas Savienotajām Valstīm nav uzskatāma par personas datu pārsūtīšanu, uz kuru attiecas privātuma vairoga principi.

15. **Publiskie reģistri un publiski pieejama informācija**

a. Organizācijai jāpiemēro no privātuma vairoga izrietošie drošības, datu integritātes un mērķa ierobežošanas, kā arī tiesību aizsardzības, izpildes panākšanas un atbildības principi personas datiem no publiski pieejamiem avotiem. Šos principus piemēro arī personas datiem, kas savākti no publiskiem reģistriem, t. i., reģistriem, ko glabā valdības aģentūras vai struktūrvienības jebkurā līmenī un kas parasti ir sabiedrībai pieejami.

b. Informēšanas, izvēles vai atbildības par tālākpārsūtīšanu principi nav jāpiemēro publisko reģistru informācijai, ja tā nav kopā ar nepublisku reģistru informāciju un ir ievēroti visi attiecīgajā jurisdikcijā paredzētie izmantošanas nosacījumi. Parasti informēšanas, izvēles vai atbildības par tālākpārsūtīšanu principi nav jāpiemēro arī publiski pieejamai informācijai, ja vien Eiropas pārsūtītājs nenorāda, ka uz šādu informāciju attiecas ierobežojumi, kas prasa organizācijai piemērot principus paredzētajiem izmantošanas veidiem. Organizācijas nebūs atbildīgas par to, kā šādu informāciju izmanto tie, kuri to ir ieguvuši no publicētiem materiāliem.

c. Ja tiek konstatēts, ka organizācija pretrunā principiem ar nodomu ir publiskojusi personisku informāciju, lai tā vai citi varētu izmantot šos izņēmumus, tā vairāk nevarēs pretendēt uz privātuma vairoga radītajām priekšrocībām.

d. Uz publisko reģistru informāciju nav jāattiecina piekļuves princips, kamēr tā nav apvienota ar citu personisko informāciju (izņemot gadījumus, kad personiskas informācijas neliela daļa ir izmantota publiskā reģistra rādītāja sastādīšanai vai organizācijai); tomēr jāievēro visi izmantošanas nosacījumi, ko noteikusi attiecīgā kompetentā iestāde. Savukārt, ja publiskā reģistra informācija ir kopā ar citu informāciju no reģistra, kas nav publisks (kas nav īpaši noteikta iepriekš), organizācijai jānodrošina piekļuve visai šādai informācijai, pieņemot, ka uz to neattiecas citi atļauti izņēmumi.

e. Tāpat kā ar publisko reģistru informāciju, nav jānodrošina piekļuve informācijai, kas jau ir publiski pieejama plašai sabiedrībai, ja vien tā nav kopā ar informāciju, kura nav publiski pieejama. Organizācijas, kas nodarbojas ar publiski pieejamas informācijas pārdošanu, var iekasēt organizācijas parasto samaksu, atbildot uz piekļuves pieprasījumiem. Vai arī indivīdi var prasīt piekļuvi savai informācijai organizācijai, kas datus apkopoja sākotnēji.

16. **Publisko iestāžu piekļuves pieprasījumi**

a. Lai nodrošinātu pārredzamību attiecībā uz publisko iestāžu likumīgiem pieprasījumiem piekļūt personiskajai informācijai, privātuma vairoga organizācijas var brīvprātīgi sagatavot periodiskus pārredzamības ziņojumus par to, cik personiskās informācijas pieprasījumu tās no publiskajām iestādēm saņēmušas saistībā ar tiesībaizsardzības vai valsts drošības apsvērumiem, ciktāl šādu ziņu izpaušana ir atļauta piemērojamos tiesību aktos.

b. Šajos privātuma vairoga organizāciju ziņojumos sniegto informāciju, kā arī izlūkdienesta publiskoto un citu informāciju, ievērojot principus, var izmantot gada kopīgajā pārskatā par privātuma vairoga darbību.

c. Informēšanas principa a) punkta xii) apakšpunktā noteiktās informācijas nesniegšana neliedz un neierobežo organizācijas spēju atbildēt uz visiem likumīgajiem pieprasījumiem.

I pielikums

Šķīrējtiesas modelis

Šajā pielikumā ir izklāstīti noteikumi, kas saskaņā ar tiesību aizsardzības, izpildes panākšanas un atbildības principu privātuma vairoga organizācijām jāievēro attiecībā uz prasību izskatīšanu šķīrējtiesā. Turpmāk aprakstītais saistošais šķīrējtiesas process ir piemērojams konkrētām "neatrisinātām" prasībām par datiem, uz kuriem attiecas ES un ASV privātuma vairogs. Šā procesa mērķis ir nodrošināt, lai indivīdiem būtu pieejams ātrs, neatkarīgs un taisnīgs mehānisms, ar ko izskatīt apgalvojumus par principu pārkāpumiem, kurus nav atrisinājis neviens cits privātuma vairoga mehānisms, ja tādi ir.

A. **Darbības joma**

Indivīds var izmantot šķīrējtiesas procesu, lai neatrisinātas prasības gadījumā tiktu noteikts, vai privātuma vairoga organizācija attiecībā uz šo indivīdu ir pārkāpusi no principiem izrietošos pienākumus un vai šāds pārkāpums ir pilnīgi vai daļēji neizlabots. Šī iespēja ir pieejama vienīgi minētajā nolūkā. To nevar izmantot, piemēram, attiecībā uz principu piemērošanas izņēmumiem ([1]) vai apgalvojumiem par privātuma vairoga nodrošinātās aizsardzības pietiekamību.

B. **Pieejamie tiesiskās aizsardzības līdzekļi**

Ja tiek izmantots šķīrējtiesas process, privātuma vairoga komisijai (kuras sastāvā atkarībā no pušu vienošanās ir viens vai trīs šķīrējtiesneši) ir pilnvaras noteikt individuālu, specifisku, nemonetāru un taisnīgu tiesiskās aizsardzības līdzekli (piemēram, piekļuvi, labošanu, dzēšanu vai attiecīgo indivīda datu atdošanu), kas vajadzīgs, lai labotu principu pārkāpumu vienīgi attiecībā uz indivīdu. Tās ir šķīrējtiesas komisijas vienīgās pilnvaras attiecībā uz tiesiskās aizsardzības līdzekļiem. Apsverot piešķiramos līdzekļus, šķīrējtiesas komisijai ir jāņem vērā arī citi tiesiskās aizsardzības līdzekļi, kas jau ir paredzēti citos privātuma vairoga mehānismos. Kaitējuma, izdevumu, maksu kompensācija vai citi tiesiskās aizsardzības līdzekļi nav pieejami. Katra puse sedz sava advokāta maksu.

C. **Prasības, kas jāizpilda pirms šķīrējtiesas procesa**

Indivīdam, kas nolemj izmantot šķīrējtiesas procesu, pirms prasības iesniegšanas jāveic šādas darbības: 1) par iespējamo pārkāpumu tieši jāinformē organizācija un jāsniedz tai iespēja problēmu atrisināt principu III sadaļas 11. daļas d) punkta i) apakšpunktā noteiktajā termiņā; 2) jāizmanto principos paredzētais neatkarīgais tiesību aizsardzības mehānisms, par kuru indivīdam nav jāmaksā; un 3) ar vietējās datu aizsardzības iestādes starpniecību par problēmu jāinformē Tirdzniecības ministrija un jāļauj tai pēc iespējas un bez maksas censties atrisināt problēmu termiņos, kas noteikti vēstulē no Tirdzniecības ministrijas Starptautiskās tirdzniecības pārvaldes.

Šo šķīrējtiesas procesu nevar izmantot, ja indivīda apgalvojums par principu pārkāpumu 1) jau ir izskatīts saistošā šķīrējtiesas procesā; 2) par to ir pieņemts galīgs spriedums tiesas procesā, kura puse bija indivīds; vai 3) puses jau iepriekš ir panākušas mierizlīgumu. Šo procesu nevar izmantot arī tad, ja ES datu aizsardzības iestādei: ir pilnvaras atbilstīgi principu III sadaļas 5. vai 9. daļai; vai 2) ir pilnvaras izskatīt apgalvojumu par pārkāpumu, tieši iesaistot organizāciju. DAI pilnvaras izskatīt tādu pašu prasību pret ES datu pārzini pašas par sevi neliedz ierosināt šķīrējtiesas procesu pret citu juridisko personu, kas nav pakļauta DAI pilnvarām.

D. **Lēmumu saistošums**

Indivīda lēmums ierosināt šo saistošo šķīrējtiesas procesu ir pilnīgi brīvprātīgs. Šķīrējtiesas lēmumi būs saistoši visām procesa pusēm. Ierosinot procesu, indivīds atsakās no iespējas saistībā ar to pašu iespējamo pārkāpumu lūgt tiesību aizsardzību citā iestādē; izņēmums ir gadījumi, kad iespējamo pārkāpumu nav iespējams pilnā apmērā labot ar nemonetāru tiesiskās aizsardzības līdzekli – tad indivīda ierosinātais šķīrējtiesas process neliedz iespēju pieprasīt kaitējuma kompensāciju, kas citkārt ir pieejama tiesās.

([1]) Principu I.5. sadaļa.

E. **Pārskatīšana un izpildes panākšana**

Saskaņā ar Federālo šķīrējtiesas procesa likumu (*Federal Arbitration Act*) ([1]) indivīdi un privātuma vairoga organizācijas varēs lūgt šķīrējtiesnešu lēmumu pārskatīšanu tiesā un izpildes panākšanu atbilstīgi ASV tiesību aktiem. Visas attiecīgās lietas ir jāierosina tajā federālajā apgabaltiesā, kuras teritoriālajā jurisdikcijā ir privātuma vairoga organizācijas galvenā darbības vieta.

Šā šķīrējtiesas procesa uzdevums ir izšķirt individuālus strīdus, un šķīrējtiesas nolēmumiem nav jādarbojas kā pamudinošam vai saistošam precedentam lietās, kas ietver citas puses, tostarp turpmākos šķīrējtiesas procesos ES vai ASV tiesās vai FTK procesos.

F. **Šķīrējtiesas komisija**

Puses izvēlas šķīrējtiesnešus no turpmāk aprakstītā tiesnešu saraksta.

ASV Tirdzniecības ministrija un Eiropas Komisija, ievērojot piemērojamos tiesību aktus, izveidos sarakstu, kurā iekļaus vismaz 20 šķīrējtiesnešu, kas izvēlēti to neatkarības, godprātības un kompetences dēļ. Saistībā ar šo procesu jāievēro turpmāk uzskaitītie nosacījumi.

Šķīrējtiesneši:

1) sarakstā ir trīs gadus un no tā tiek izslēgti ārkārtas apstākļu vai iemeslu dēļ; sarakstā iekļautos speciālistus var atkārtoti iekļaut sarakstā vēl uz trim gadiem;

2) nesaņem norādījumus no kādas procesa puses, privātuma vairoga organizācijas, ASV, ES vai kādas ES dalībvalsts vai kādas citas valdības iestādes, publiskas iestādes vai tiesībaizsardzības iestādes un nav ar tām saistīta; un

3) ir saņēmuši atļauju praktizēt tiesības ASV un ir ASV privātuma tiesību eksperti, kas ir kompetenti ES datu aizsardzības tiesībās.

G. **Šķīrējtiesas procedūras**

Atbilstīgi piemērojamiem tiesību aktiem sešu mēnešu laikā no lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas Tirdzniecības ministrija un Eiropas Komisija vienosies pieņemt jau izveidotu, iedibinātu ASV šķīrējtiesas procedūru (piemēram, AAA vai JAMS) kopumu, lai reglamentētu privātuma vairoga komisijas procedūras atbilstīgi visiem turpmāk uzskaitītajiem apsvērumiem.

1. Indivīds var ierosināt saistošu šķīrējtiesas procesu, ievērojot iepriekš izklāstītās prasības, kas jāizpilda pirms šķīrējtiesas procesa, un iesniedzot organizācijai "paziņojumu". Paziņojumā iekļauj atbilstīgi C punktam veikto prasības risināšanas darbību kopsavilkumu, iespējamā pārkāpuma aprakstu un, ja indivīds vēlas, jebkādus pavaddokumentus un materiālus un/vai ar iespējamo pārkāpumu saistīta tiesību akta aprakstu.

([1]) Atbilstīgi Federālā šķīrējtiesas procesa likuma ("FAA") 2. nodaļai "uz arbitrāžas vienošanos vai šķīrējtiesas nolēmumu, kas izriet no juridiskām – līgumiskām vai ne – attiecībām, ko uzskata par komerciālām attiecībām, tostarp uz darījumu, līgumu vai vienošanos, kas aprakstīta [*FAA* 2. pantā], attiecas [1958. gada 10. jūnija] Konvencija [par ārvalstu šķīrējtiesu nolēmumu atzīšanu un izpildīšanu (*21 U.S.T. 2519, T.I.A.S.* Nr. 6997 ("Ņujorkas Konvencija")]." *9 U.S.C. § 202*. Turklāt saskaņā ar *FAA*"tiek uzskatīts, ka uz vienošanos vai nolēmumu, kas izriet no šādām attiecībām, kuru puses ir vienīgi Amerikas Savienoto Valstu pilsoņi, neattiecas [Ņujorkas] Konvencijas noteikumi, ja vien šīs attiecības neietver īpašumu, kas atrodas ārvalstīs, darbību vai izpildes panākšanu ārvalstīs vai nav citādi un pamatoti saistītas ar vienu vai vairākām ārvalstīm." *Turpat* 2. nodaļā: "ikviena šķīrējtiesas procesa puse var vērsties jebkurā tiesā, kurai ir jurisdikcija saskaņā ar šo nodaļu, un lūgt, lai tā pieņemtu rīkojumu, ar ko apstiprina pret jebkuru šķīrējtiesas procesa pusi pieņemto nolēmumu. Tiesa nolēmumu apstiprina, ja vien tā nekonstatē kādu no [Ņujorkas] Konvencijā noteiktajiem nolēmuma atzīšanas vai izpildes panākšanas atteikuma vai atlikšanas iemesliem." Turpat, § 207. FAA 2. nodaļā arī noteikts, ka "Amerikas Savienoto Valstu apgabaltiesām (…) ir sākotnējā jurisdikcija attiecībā uz (…) prasību vai procesu [saskaņā ar Ņujorkas Konvenciju] neatkarīgi no summas, par kuru ir strīds." Turpat, § 203.
FAA 2. nodaļā ir noteikts arīdzan tas, ka "saskaņā ar šo nodaļu ierosinātajām prasībām un procesiem piemēro 1. nodaļu, ciktāl tā nav pretrunā šai nodaļai vai [Ņujorkas] Konvencijai, ko ir ratificējušas Amerikas Savienotās Valstis." Turpat, § 208. Savukārt 1. nodaļā ir paredzēts, ka (…) "tirdzniecības darījumu apliecinoša līguma [r]akstisks noteikums) par to, ka turpmākas domstarpības par šādu līgumu vai darījumu, vai atteikumu pildīt visu līgumu vai darījumu, vai tā daļu izskata šķīrējtiesā, vai rakstiska vienošanās iesniegt izskatīšanai šķīrējtiesā esošas domstarpības par šādu līgumu, darījumu vai atteikumu ir spēkā, neatsaucama un izpildāma, izņemot tiesību aktos noteiktajos gadījumos vai kāda līguma anulēšanas gadījumā." Turpat, § 2. Turklāt saskaņā ar *FAA* 1. nodaļu "ikviena šķīrējtiesas procesa puse var attiecīgi tiesā lūgt rīkojumu, ar ko apstiprina nolēmumu, un tādā gadījumā tiesai šāds rīkojums ir jāpieņem, ja vien nolēmums nav anulēts, mainīts vai labots, kā paredzēts [*FAA*] 10. un 11. pantā." Turpat § 9.

2. Tiks izstrādātas procedūras, ar ko nodrošināt, lai uz vienu indivīda prasību par iespējamo pārkāpumu netiktu attiecināti divkārši tiesiskās aizsardzības līdzekļi vai procesi.

3. Vienlaikus šķīrējtiesas procesam var notikt prasības izskatīšana FTK.

4. Šajos šķīrējtiesas procesos nedrīkst piedalīties ASV, ES, ES dalībvalstu vai kādas citas valdības iestādes, publiskās iestādes vai tiesībaizsardzības iestādes pārstāvji, ja pēc ES indivīda pieprasījuma ES DAI var palīdzēt tikai paziņojuma sagatavošanā, taču ES DAI nedrīkst piekļūt konstatējumiem vai citiem ar šo šķīrējtiesas procesu saistītiem materiāliem.

5. Process noris Amerikas Savienotajās Valstīs, un indivīds var izvēlēties dalību ar video vai tālruņa starpniecību, kas tiks nodrošināta bez maksas. Personiska klātbūtne netiek prasīta.

6. Šķīrējtiesas process notiks angļu valodā, ja vien puses nevienosies citādi. Saņemot pamatotu pieprasījumu un ņemot vērā to, vai indivīdu pārstāv advokāts, indivīdam bez maksas nodrošinās šķīrējtiesas sēdes mutisko tulkojumu, kā arī materiālu rakstisko tulkojumu, ja vien komisija nekonstatēs, ka konkrētā procesa apstākļos tas radītu nepamatotas vai nesamērīgas izmaksas.

7. Šķīrējtiesnešiem iesniegtos materiālus uzskatīs par konfidenciāliem un izmantos vienīgi saistībā ar attiecīgo procesu.

8. Ja nepieciešams, var atļaut izmantot ar indivīdu saistītu konstatējumu, un puses šādu konstatējumu uzskatīs par konfidenciālu un izmantos tikai saistībā ar attiecīgo šķīrējtiesas procesu.

9. Process būtu jāizskata 90 dienu laikā no paziņojuma iesniegšanas attiecīgajai organizācijai, ja vien puses nevienojas citādi.

H. **Izmaksas**

Šķīrējtiesnešiem būtu jāveic piemērotas darbības, lai līdz minimumam samazinātu procesa izmaksas vai nodevas.

Saskaņā ar piemērojamiem tiesību aktiem Tirdzniecības ministrija, konsultējoties ar Eiropas Komisiju, veicinās tāda fonda izveidi, kurā privātuma vairoga organizācijām būs jāveic no to lieluma daļēji atkarīgas gada iemaksas, ar kurām tiks segtas šķīrējtiesas procesa izmaksas, ieskaitot šķīrējtiesnešu honorārus, kuri nepārsniedz maksimālo apmēru ("robežvērtību"). Fondu pārvaldīs trešā persona, kas regulāri ziņos par tā darbību. Gada pārskatā Tirdzniecības ministrija un Eiropas Komisija pārskatīs fonda darbību, tostarp nepieciešamību pielāgot iemaksu vai robežvērtību apmēru, un cita starpā izskatīs šķīrējtiesas procesu skaitu, izmaksas un ilgumu, saprotot, ka nevajadzētu radīt privātuma vairoga organizācijām pārmērīgu finansiālo slogu. Šā noteikuma un neviena saskaņā ar to izveidota fonda darbības joma neattiecas uz advokātu honorāriem.

III PIELIKUMS

Vēstule no ASV valsts sekretāra *John Kerry*

2016. gada 7. jūlijs

Cienījamā komisāres kundze!

Priecājos, ka esam panākuši sapratni par Eiropas Savienības un Amerikas Savienoto Valstu privātuma vairogu, kas ietvers ombuda mehānismu, ar kura starpniecību ES iestādes varēs ES iedzīvotāju vārdā iesniegt pieprasījumus par ASV īstenoto sakaru izlūkošanas praksi.

ASV prezidents Baraks Obama 2014. gada 17. janvārī paziņoja par svarīgām izlūkošanas reformām, kas ir paredzētas Prezidenta politikas direktīvā Nr. 28 (PPD-28). Īstenojot PPD-28, es iecēlu valsts sekretāra vietnieci *Catherine A. Novelli*, kura darbojas arī kā vecākā koordinatore starptautiskās informāciju tehnoloģijas diplomātijas jautājumos, par ASV kontaktpersonu ārvalstu valdībām, kuras vēlas paust bažas par ASV sakaru izlūkošanas darbībām. Papildinot šīs funkcijas, esmu izveidojis privātuma vairoga ombuda mehānismu saskaņā ar A pielikumā izklāstītajiem noteikumiem, kuri ir aktualizēti kopš manas 2016. gada 22. februāra vēstules. Šīs funkcijas izpildi es uzticēju valsts sekretāra vietniecei *Novelli* kundzei. Valsts sekretāra vietniece *Novelli* ir neatkarīga no ASV izlūkdienesta un tieši pakļauta man.

Esmu licis saviem darbiniekiem jaunā ombuda mehānisma īstenošanai veltīt visus vajadzīgos resursus, un esmu pārliecināts, ka tas būs rezultatīvs līdzeklis, ar ko reaģēt uz ES iedzīvotāju bažām.

Ar cieņu

John F. Kerry

A pielikums

ES un ASV privātuma vairoga ombuda mehānisms Sakaru izlūkošanas jomā

Atzīstot ES un ASV privātuma vairoga regulējuma nozīmi, šajā memorandā ir izklāstīts process, kas jāievēro, lai īstenotu jauno mehānismu – atbilstīgi Prezidenta politikas direktīvai Nr. 28 (PPD-28) – sakaru izlūkošanas jomā ([1]).

ASV prezidents Baraks Obama 2014. gada 17. janvārī teica runu, kurā paziņoja par būtiskām izlūkošanas nozares reformām. Šajā runā viņš norādīja, ka "[m]ūsu centieni palīdz aizsargāt ne tikai mūsu nāciju, bet arī mūsu draugus un sabiedrotos. Mūsu centieni būs rezultatīvi tikai tad, ja citu valstu parastie pilsoņi ticēs, ka Amerikas Savienotās Valstis ievēro arī viņu privātumu." Prezidents B. Obama paziņoja, ka, lai "skaidri noteiktu, kādas darbības mēs veicam un kādas neveicam saistībā ar mūsu īstenoto aizjūras izlūkošanu", tiks pieņemta jauna prezidenta direktīva – PPD-28.

Tās 4. panta d) punktā ir noteikts, ka valsts sekretārs ieceļ "vecāko koordinatoru starptautiskās informācijas tehnoloģijas diplomātijas jautājumos" ("vecākais koordinators"), "kas (…) darbosies kā kontaktpersona ārvalstu valdībām, kuras vēlas paust bažas par Amerikas Savienoto Valstu īstenotajām sakaru izlūkošanas darbībām." No 2015. gada janvāra vecākās koordinatores funkcijas pilda valsts sekretāra vietniece *C. Novelli*.

Šajā memorandā ir aprakstīts jauns mehānisms, ko vecākā koordinatore ievēros, lai veicinātu tādu ar valsts drošību saistītu piekļuves pieprasījumu apstrādi, kuri attiecas uz datiem, ko ar iedibinātiem piemērojamos Amerikas Savienoto Valstu tiesību aktos un politikā paredzētiem līdzekļiem no ES pārsūta Amerikas Savienotajām Valstīm saskaņā ar privātuma vairogu, standarta līgumu klauzulām (SLK), saistošiem uzņēmumu noteikumiem (SUN), "atkāpēm" ([2]) vai "iespējamām turpmākām atkāpēm" ([3]), kā arī atbildēšanu uz tiem.

1. **Privātuma vairoga ombuds.** Vecākais koordinators darbosies kā privātuma vairoga ombuds un iecels papildu valsts departamenta darbiniekus, kas nepieciešami, lai palīdzētu šajā memorandā sīki izklāstīto pienākumu pildīšanā. (turpmāk koordinators un visi darbinieki, kas pilda šādus pienākumus, dēvēti par "privātuma vairoga ombudu") Privātuma vairoga ombuds cieši sadarbosies ar attiecīgajiem darbiniekiem no citām ministrijām un aģentūrām, kas atbild par pieprasījumu apstrādi atbilstīgi piemērojamiem Amerikas Savienoto Valstu tiesību aktiem un politikai. Ombuds ir neatkarīgs no izlūkdienestiem. Ombuds ir tieši pakļauts valsts sekretāram, kas nodrošina, ka ombuds savus uzdevumus veic objektīvi un neatkarīgi no neatbilstīgas ietekmes, kas var ietekmēt sniedzamo atbildi.

2. **Efektīva koordinācija.** Privātuma vairoga ombuds varēs rezultatīvi izmantot un koordinēt turpmāk aprakstītās pārraudzības iestades, lai nodrošinātu, ka ombuda atbilžu uz pieprasījumiem, ko iesnieguši ES individuālo sūdzību

([1]) Ar nosacījumu, ka Komisijas lēmumu par pienācīgu aizsardzību, kas noteikta ar ES un ASV privātuma vairogu piemēro Islandei, Lihtenšteinai un Norvēģijai, privātuma vairoga pakete attieksies gan uz Eiropas Savienību, gan uz šīm trim valstīm. Attiecīgi atsauces uz ES un tās dalībvalstīm būs lasāmas, ietverot arī Islandi, Lihtenšteinu un Norvēģiju.

([2]) "Atkāpes" šajā kontekstā ir komerciāla pārsūtīšana vai pārsūtīšanas, ko veic ar nosacījumu, ka: a) datu subjekts ir skaidri piekritis ierosinātajai datu pārsūtīšanai; vai b) pārsūtīšana ir vajadzīga, lai izpildītu līgumu starp datu subjektu un pārzini vai īstenotu pasākumus pirms līguma noslēgšanas, kas pieņemti, reaģējot uz datu subjekta pieprasījumu; vai c) pārsūtīšana ir nepieciešama, lai noslēgtu vai izpildītu līgumu, kas datu subjekta interesēs noslēgts starp pārzini un trešo personu; vai d) pārsūtīšana ir vajadzīga vai likumīgi prasīta, pamatojoties uz svarīgām sabiedrības interesēm, vai prasījumu pamatošanai, īstenošanai vai aizstāvībai; vai e) pārsūtīšana ir nepieciešama, lai aizsargātu datu subjekta īpaši svarīgas intereses; vai f) pārsūtīšanu izdara no reģistra, kas saskaņā ar tiesību aktiem vai noteikumiem ir paredzēts, lai sniegtu informāciju sabiedrībai, un ko var izmantot vai nu plaša sabiedrība, vai jebkura persona, kura var pierādīt likumīgu interesi, ciktāl konkrētajā gadījumā ir izpildīti tiesību aktos paredzētie izmantošanas nosacījumi.

([3]) "Iespējamas turpmākas atkāpes" šajā kontekstā ir komerciāla pārsūtīšana vai pārsūtīšanas, kas notiek kādos no turpmāk uzskaitītajiem apstākļiem, ciktāl tie ir uzskatāmi par likumīgu pamatu personas datu pārsūtīšanai no ES uz ASV: a) datu subjekts ir skaidri piekritis ierosinātajai pārsūtīšanai pēc tam, kad ir ticis informēts par iespējamiem riskiem, ko šāda pārsūtīšana var radīt datu subjektam lēmuma par aizsardzības līmeņa pietiekamību un atbilstošu aizsardzības pasākumu trūkuma dēļ; vai b) pārsūtīšana ir vajadzīga, lai aizsargātu datu subjekta vai citu personu īpaši svarīgas intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu; vai c) ja veic pārsūtīšanu uz trešo valsti vai starptautisku organizāciju un nav piemērojama neviena cita atkāpe vai iespējama turpmāka atkāpe, un tikai tad, ja pārsūtīšana nav atkārtota, attiecas vienīgi uz ierobežotu datu subjektu skaitu, ir jāveic pārliecinošās un likumīgās pārziņa īstenotās interesēs, pār kurām nedominē datu subjekta intereses vai tiesības un brīvības, un pārzinis ir novērtējis visus ar datu pārsūtīšanu saistītos apstākļus un, pamatojoties uz minēto novērtējumu, nodrošinājis piemērotus personas datu aizsardzības pasākumus.

izskatīšanas struktūras, pamatā ir nepieciešamā informācija. Ja pieprasījums attiecas uz novērošanas atbilstību ASV tiesību aktiem, privātuma vairoga ombuds varēs sadarboties ar vienu no neatkarīgajām pārraudzības struktūrām, kam ir izmeklēšanas pilnvaras.

a. Privātuma vairoga ombuds cieši sadarbosies ar citām Amerikas Savienoto Valstu valstības amatpersonām, tostarp atbilstošām neatkarīgām pārraudzības struktūrām, lai nodrošinātu aizpildīto pieprasījumu apstrādi un izskatīšanu atbilstīgi piemērojamiem tiesību aktiem un politikai. Konkrētāk, privātuma vairoga ombuds varēs cieši koordinēt darbību ar Nacionālās izlūkošanas direktora biroju, Tieslietu ministriju un citām ministrijām un aģentūrām, kas ir attiecīgi iesaistītas Amerikas Savienoto Valstu nacionālās drošības garantēšanā, kā arī ģenerālinspektoriem, Likuma par informācijas brīvību (*Freedom of Information Act*) īstenošanas amatpersonām un pilsonisko brīvību un privātuma aizsardzības amatpersonām.

b. Amerikas Savienoto Valstu valdība izmantos mehānismus valsts drošības jautājumu koordinēšanai un pārraudzībai starp ministrijām un aģentūrām, lai palīdzētu nodrošināt privātuma vairoga ombuda spēju 4. punkta e) apakšpunkta nozīmē reaģēt uz pieprasījumiem, kas iesniegti saskaņā ar 3. punkta b) apakšpunktu).

c. Privātuma vairoga ombuds ar pieprasījumiem saistītos jautājumus var nodot izskatīšanai Privātuma un pilsonisko brīvību pārraudzības padomē.

3. **Pieprasījumu iesniegšana**

a. Pieprasījumu sākotnēji iesniedz dalībvalstu uzraudzības iestādēm, kas ir kompetentas pārraudzīt valsts drošības dienestus un/vai to, kā valsts iestādes apstradā personas datus. Pieprasījumu ombudam iesniegs ES centralizēta struktūra (turpmāk kopā "ES individuālo sūdzību izskatīšanas struktūra").

b. ES individuālo sūdzību izskatīšanas struktūra, veicot turpmāk aprakstītās darbības, nodrošinās, ka pieprasījums ir pilnīgs:

i) pārbaudīs indivīda identitāti un to, vai viņš/viņa rīkojas savā vārdā, nevis kā valdības vai starpvaldību organizācijas pārstāvis;

ii) nodrošinās, ka pieprasījums ir sagatavots rakstiski un tajā ir iekļauta šāda pamatinformācija:

— visa pieprasījuma pamatinformācija,

— prasītās informācijas vai tiesiskās aizsardzības līdzekļa veids,

— iespējami iesaistītās Amerikas Savienoto Valstu struktūras, ja tādas ir, un

— citi pasākumi, kas veikti, lai iegūtu prasīto informāciju vai tiesiskās aizsardzības līdzekli, un ar šiem pasākumiem saistītā reakcija;

iii) pārbaudīs, vai pieprasījums attiecas uz datiem, par kuriem ir pamatoti uzskatīt, ka tie ir pārsūtīti no ES un Amerikas Savienotajām Valstīm saskaņā ar privātuma vairogu, SLK, SUN, atkāpēm vai iespējamām turpmākām atkāpēm;

iv) sākotnēji konstatēs, vai pieprasījums nav maznozīmīgs, apgrūtinošs vai iesniegts ļaunticīgi.

c. Lai pieprasījums būtu pilnīgs un privātuma vairoga ombuds to varētu apstrādāt atbilstīgi šim memorandam, tajā nav jāpierāda, ka Amerikas Savienoto Valstu valdība ir faktiski piekļuvusi pieprasījuma iesniedzēja datiem, veicot sakaru izlūkošanas darbības.

4. **Pienākums komunicēt ar ES individuālo sūdzību izskatīšanas struktūru, kas iesniedz dokumentus**

a. Privātuma vairoga ombuds apstiprinās pieprasījuma saņemšanu ES individuālo sūdzību izskatīšanas struktūrai, kas to iesniedza.

b. Ombuds veiks sākotnēju pārbaudi, lai apstiprinātu, ka pieprasījums ir izpildīts saskaņā ar 3. sadaļas b) punktu. Ja privātuma vairoga ombuds ievēros kādas nepilnības vai viņam radīsies jautājumi par pieprasījuma aizpildīšanu, viņš centīsies kopā ar attiecīgo ES individuālo sūdzību izskatīšanas struktūru šīs šaubas izskatīt un novērst.

c. Ja, lai atvieglotu pieprasījuma atbilstošu apstrādi, privātuma vairoga ombudam vajadzēs vairāk informācijas par pieprasījumu vai indivīdam, kas sākotnēji iesniedza pieprasījumu, būs jāveic konkrētas darbības, ombuds par to informēs ES individuālo sūdzību izskatīšanas struktūru, kas pieprasījumu iesniedza.

d. Privātuma vairoga ombuds sekos līdzi pieprasījumu statusam un paziņos iesniedzējai ES individuālo sūdzību izskatīšanas struktūrai attiecīgo jaunāko informāciju.

e. Kad pieprasījums būs aizpildīts, kā aprakstīts šā memoranda 3. punktā, privātuma vairoga ombuds savlaicīgi sniegs iesniedzējai ES individuālo sūdzību izskatīšanas struktūrai atbilstošu atbildi, ievērojot pastāvīgo pienākumu aizsargāt informāciju saskaņā ar piemērojamiem tiesību aktiem un politiku. Privātuma vairoga ombuds atbildēs iesniedzējai ES individuālo sūdzību izskatīšanas struktūrai, apstiprinot: i) ka sūdzība ir pienācīgi izmeklēta un ii) ka ir ievēroti ASV tiesību akti, statūti, izpildrīkojumi, prezidenta direktīvas un aģentūras politikas virzieni, kas paredz NIDB vēstulē aprakstītos ierobežojumus un aizsardzības pasākumus, vai – neatbilstības gadījumā –, ka šāda neatbilstība ir novērsta. Privātuma vairoga ombuds neapstiprinās un nenoliegs, vai indivīds ir ticis novērots; ombuds arī neapstiprinās konkrēto piemēroto tiesiskās aizsardzības līdzekli. Kā paskaidrots 5. sadaļā, atbilstīgi LIB iesniegtie pieprasījumi tiks apstrādāti, kā noteikts minētajā likumā un piemērojamos noteikumos.

f. Privātuma vairoga ombuds nepastarpināti komunicēs ar ES individuālo sūdzību izskatīšanas struktūru, savukārt tā būs atbildīga par saziņu ar indivīdu, kas iesniedza pieprasījumu. Ja tieša saziņa ir daļa no viena no turpmāk aprakstītajiem pamata procesiem, tā notiks atbilstoši pastāvošajām procedūrām.

g. Šajā memorandā paredzētās saistības neattieksies uz vispārīgiem apgalvojumiem par to, ka ES un ASV privātuma vairogs neatbilst Eiropas Savienības datu aizsardzības prasībām. Memorandā izklāstītās saistības ir noteiktas, pamatojoties uz Eiropas Komisijas un ASV valdības kopīgu izpratni par to, ka, ņemot vērā no šā mehānisma izrietošo saistību darbības jomu, var rasties resursu ierobežojumi, tostarp attiecībā uz pieprasījumiem, kas iesniegti saskaņā ar Likumu par informācijas brīvību. Ja, pildot privātuma vairoga ombuda funkcijas, tiks pārsniegti saprātīgi resursu ierobežojumi un kavēta šo saistību izpilde, ASV valdība ar Eiropas Komisiju apspriedīs visas korekcijas, kas varētu būt piemērotas situācijas risināšanai.

5. **Informācijas pieprasījumi.** Pieprasījumus par piekļuvi Amerikas Savienoto Valstu valdības reģistriem var iesniegt un apstrādāt saskaņā ar Likumu par informācijas brīvību (LIB).

a. LIB ikvienai personai nodrošina iespēju lūgt piekļuvi pastāvošiem federālās aģentūras reģistriem neatkarīgi no pieprasītāja valstspiederības. Šis likums ir kodificēts Amerikas Savienoto Valstu Kodeksā (5 U.S.C. § 552). Likuma teksts un papildu informācija par LIB ir atrodama šādās vietnēs www.FOIA.gov un http://www.justice.gov/oip/foia-resources. Katrai aģentūrai ir galvenā amatpersona ar LIB saistītos jautājumos, un aģentūras savā publiskajā tīmekļa vietnē ir norādījušas, kā tām var iesniegt LIB pieprasījumu. Aģentūras ir izveidojušas procesus, lai savstarpēji sazinātos par LIB pieprasījumiem, kuri attiecas uz citas aģentūras reģistriem.

b. Piemēram:

i) Nacionālās izlūkošanas direktora birojs (NIDB) ir izveidojis NIDB LIB portālu, kas attiecas uz NIDB: http://www.dni.gov/index.php/about-this-site/foia. Portālā ir informācija par pieprasījuma iesniegšanu, iesniegta pieprasījuma statusa noskaidrošanu un piekļuvi informācijai, ko NIDB izpaudis un publiskojis saskaņā ar LIB. NIDB LIB portālā ir norādītas saites uz citām NIDB tīmekļa vietnēm par izlūkdienesta struktūrvienībām: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites

ii) Vispusīga informācija par LIB ir sniegta Tieslietu ministrijas Informācijas politikas biroja vietnē: http://www.justice.gov/oip. Tajā ir ne tikai informācija par LIB pieprasījuma iesniegšanu Tieslietu ministrijai, bet arī sniegtas norādes Amerikas Savienoto Valstu valdībai par LIB prasību interpretēšanu un piemērošanu.

c. LIB ir paredzēti konkrēti izņēmumi attiecībā uz piekļuvi valdības reģistriem. Šie ierobežojumi attiecībā uz piekļuvi klasificētai valsts drošības informācijai, trešo personu personiskajai informācijai un informācijai par tiesībaizsardzības izmeklēšanām, un tie ir pielīdzināmi ierobežojumiem, kas ir paredzēti katras ES dalībvalsts tiesību aktos par piekļuvi informācijai Šie ierobežojumi vienādi attiecas gan uz amerikāņiem, gan indivīdiem ar citu valstspiederību.

d. Strīdus par atbilstīgi LIB pieprasītas informācijas izpaušanu var pārsūdzēt administratīvi un pēc tam – federālajā tiesā. Tiesai ir jāpieņem *de novo* nolēmums par to, vai informācijas neizpaušana ir pamatota (*5 U.S.C. § 552(a)(4)(B)*), un tā var likt valdībai nodrošināt piekļuvi reģistriem. Atsevišķos gadījumos tiesas ir noraidījušas valdības apgalvojumus par to, ka informācija nebūtu jāizpauž, jo ir klasificēta. Lai gan finansiāla zaudējumu kompensācija nav paredzēta, tiesa var nolemt, ka ir jākompensē advokāta honorārs.

6. **Turpmākas rīcības pieprasījumi.** Pieprasījums, kurā apgalvots, ka ir pārkāpti tiesību akti vai notikusi cita ļaunprātīga rīcība, tiks nodots attiecīgajai Amerikas Savienoto Valstu valdības struktūrai, tostarp neatkarīgām pārraudzības struktūrām, kurām ir pilnvaras izmeklēt attiecīgo pieprasījumu un reaģēt uz neatbilstību, kā aprakstīts turpmāk.

a. Ģenerālinspektori ir likumiski neatkarīgi, tiem ir plašas pilnvaras izmeklēt, revidēt un pārbaudīt programmas, tostarp attiecībā uz krāpšanu un tiesību aktu ļaunprātīgu izmantošanu vai pārkāpšanu, un viņi var ieteikt korektīvas darbības.

i) Ar 1978. gada Ģenerālinspektora likumu (*Inspector General Act*) (grozītajā versijā) tika likumiski izveidots federālā ģenerālinspektora (ĢI) amats – neatkarīgas un objektīvas struktūrvienības, kas darbojas vairumā aģentūru un kuru pienākums ir apkarot izšķērdēšanu, krāpšanu un ļaunprātīgu izmantošanu attiecīgo aģentūru programmu īstenošanā un darbībās. Šajā nolūkā katram ĢI ir jāveic ar tā aģentūras programmām un darbībām saistītas revīzijas un izmeklēšanas. ĢI arī sniedz norādes, koordinē un iesaka politiku attiecībā uz darbībām, kas izstrādātas, lai veicinātu taupīgumu, rezultativitāti un efektivitāti un novērstu un konstatētu krāpšanu un ļaunprātīgu izmantošanu aģentūras programmu un darbību īstenošanā.

ii) Katrai izlūkdienesta struktūrvienībai ir savs ģenerālinspektora birojs, kura pienākums *inter alia* ir ārējās izlūkošanas darbību pārraudzība. Ir publiskoti vairāki ģenerālinspektoru ziņojumi par izlūkošanas programmām.

iii) Piemēram:

— Izlūkdienesta ģenerālinspektora (ID ĢI) birojs tika izveidots atbilstoši 405. pantam 2010. fiskālā gada Izlūkošanas atļaujas likumā *Intelligence Authorization Act of Fiscal Year 2010*. ID ĢI pārziņā ir ID līmeņa revīzijas, izmeklēšanas, pārbaudes un pārskatīšanas, kurās nosaka un novērš ID aģentūras misijās pastāvošos sistēmiskos riskus, neaizsargātību un nepilnības, lai izlūkdienestā palielinātu ietaupījumus un rezultativitāti. ID ĢI ir pilnvarots izmeklēt sūdzības vai informāciju par iespējamiem tiesību aktu, noteikumu pārkāpumiem, izšķērdēšanu, krāpšanu, pilnvaru ļaunprātīgu izmantošanu vai būtiskiem vai specifiskiem sabiedrības veselības un drošības apdraudējumiem saistībā ar NIDB un/vai ID izlūkošanas programmām un darbībām. ID ĢI sniedz informāciju par to, kā ar to tieši sazināties, lai iesniegtu ziņojumu: http://www.dni.gov/index.php/about-this-site/contact-the-ig

— ASV Tieslietu ministrijas (TM) Ģenerālinspektora birojs (ĢIB) ir likumiski izveidota neatkarīga struktūra, kuras uzdevums ir konstatēt un nepieļaut ar TM programmām un darbiniekiem saistītu izšķērdēšanu, krāpšanu, ļaunprātīgu izmantošanu un neatbilstošu rīcību, kā arī veicināt šo programmu taupīgu un efektīvu īstenošanu. ĢIB izmeklē iespējamus TM darbinieku izdarītus krimināltiesību un civiltiesību aktu pārkāpumus, kā arī veic TM programmu revīzijas un pārbaudes. ĢIB ir jurisdikcija attiecībā uz visām sūdzībām par Tieslietu ministrijas, tostarp Federālā izmeklēšanas biroja, Narkotiku apkarošanas pārvaldes, Federālā cietumu biroja, ASV Maršalu dienesta, Alkohola, tabakas, ieroču un sprāgstvielu aprites biroja, Amerikas Savienoto Valstu prokuratūru un citu Tieslietu ministrijas struktūrvienību vai biroju darbinieku ļaunprātīgu rīcību. (Vienīgais izņēmums ir tas, ka apgalvojumus par ministrijas advokāta vai tiesībaizsardzības darbinieka ļaunprātīgu rīcību, kas ir saistīta ar ministrijas advokāta izmeklēšanas, tiesāšanās vai

juridiskās konsultēšanas pilnvarām, izskata Tieslietu ministrijas Profesionālās atbildības birojs.) Turklāt 2001. gada 26. gada oktobrī parakstītā ASV Patriotisma likuma (*USA Patriot Act*) 1001. pantā ir noteikts, ka ģenerālinspektoram jāpārbauda informācija un jāsaņem sūdzības par iespējamiem Tieslietu ministrijas darbinieku izdarītiem civiltiesību un pilsonisko brīvību pārkāpumiem. ĢIB uztur publisku tīmekļa vietni https://www.oig.justice.gov, kurā ir iekļauta "karstā līnija" sūdzību iesniegšanai: https://www.oig.justice.gov/hotline/index.htm

b. Attiecīgi pienākumi ir arī Amerikas Savienoto Valstu valdības privātuma un pilsonisko brīvību aizsardzības birojiem un struktūrvienībām. Piemēram:

i) ar 2007. gada Likuma par 11. septembra komisiju (*9/11 Commission Act*) 803. pantu (likums kodificēts Amerikas Savienoto Valstu Kodeksā: *42 U.S.C. § 2000-ee1*) ir izveidotas atsevišķu ministriju un aģentūru, tostarp Valsts departamenta, Tieslietu ministrijas un NIDB, amatpersonas privātuma un pilsonisko brīvību aizsardzības jautājumos. Likuma 803. pantā ir noteikts, ka šīs privātuma un pilsonisko brīvību aizsardzības amatpersonas darbosies kā galvenie padomdevēji, lai cita starpā nodrošinātu, ka attiecīgā ministrija, aģentūra vai struktūrvienība ir ieviesusi pienācīgas procedūras, ar ko reaģēt uz sūdzībām no indivīdiem, kuri apgalvo, ka tā ir pārkāpusi viņu privātumu vai pilsoniskās brīvības.

ii) NIDB Pilsonisko brīvību un privātuma aizsardzības biroju (NIDB PBPAB) vada NIDB pilsonisko brīvību aizsardzības amatpersona, kuras amats ir izveidots ar 1948. gada Valsts drošības likumu (*National Security Act*) (grozītā versija). NIDB PBPAB pienākums ir, piemēram, nodrošināt pienācīgas privātuma un pilsonisko brīvību aizsardzības iekļaušanu izlūkdienesta struktūrvienību politikā un procedūrās, kā arī izskatīt un izmeklēt sūdzības par pilsonisko brīvību un privātuma pārkāpumiem NIDB programmās un darbībās. NIDB PBPAB sniedz sabiedrībai informāciju, arī norādes par sūdzības iesniegšanu, savā tīmekļa vietnē: www.dni.gov/clpo. Saņemot sūdzību par privātuma vai pilsonisko brīvību pārkāpumu saistībā ar ID programmām un darbībām, NIDB PBPAB ar citām ID struktūrvienībām saskaņos, kā šī sūdzība būtu jāapstrādā ID līmenī. Jāatzīmē, ka Pilsonisko brīvību un privātuma aizsardzības birojs ir arī Nacionālās drošības aģentūrai (NDA), un informācija par tā pienākumiem ir pieejama aģentūras tīmekļa vietnē: https://www.nsa.gov/civil_liberties/. Ja informācijā ir norādīts, ka aģentūra neievēro privātuma aizsardzības prasības (piemēram, PPD-28 4. panta prasību), aģentūrām ir pieejami atbilstības panākšanas mehānismi incidenta izskatīšanai un labošanai. Aģentūrām ir jāziņo NIDB par PPD-28 neievērošanas gadījumiem.

iii) Tieslietu ministrijas Privātuma un pilsonisko brīvību aizsardzības birojs (PPBAB) palīdz Tieslietu ministrijas galvenās privātuma un pilsonisko brīvību aizsardzības amatpersonas (GPPBAA) pienākumu izpildē. Galvenais PPBAB uzdevums ir aizsargāt Amerikas iedzīvotāju privātumu un pilsoniskās brīvības, pārbaudot, pārraugot un koordinējot ar privātumu saistītās ministrijas darbības. PPBAB sniedz juridiskās konsultācijas un norādes ministrijas struktūrvienībām; nodrošina privātuma ievērošanu ministrijā, tostarp atbilstību 1974. gada Privātuma likumam (*Privacy Act*), 2002. gada E-pārvaldības likuma (*E-Government Act*) un Federālā informācijas drošības pārvaldības likuma (*Federal Information Security Management Act*) noteikumiem par privātumu, kā arī šo likumu izpildes veicināšanas nolūkā pieņemtajām pārvaldības politikas direktīvām; izstrādā un pasniedz ministrijā mācības par privātumu; palīdz PPBAA izstrādāt ministrijas privātuma politiku; sagatavo ar privātumu saistītus ziņojumus prezidentam un Kongresam; pārskata ministrijā īstenoto informācijas apstrādes praksi, lai nodrošinātu tās atbilstību privātuma un pilsonisko brīvību aizsardzības noteikumiem. PPBAB informē sabiedrību par saviem pienākumiem vietnē: http://www.justice.gov/opcl

iv) Atbilstīgi *42 U.S.C. § 2000ee* un turpm. sadaļām Privātuma un pilsonisko brīvību pārraudzības padome pastāvīgi pārbauda: i) kā un kādu politiku un procedūras īsteno ministrijas, aģentūras un izpildvaras struktūrvienības saistībā ar centieniem aizsargāt valsti pret terorismu, un tas tiek darīts nolūkā nodrošināt privātuma un pilsonisko brīvību aizsardzību; ii) citas ar šādiem centieniem saistītas izpildvaras darbības, lai noteiktu, vai tās pienācīgi aizsargā privātumu un pilsoniskās brīvības un atbilst reglamentējošiem tiesību aktiem, noteikumiem un politikai attiecībā uz privātumu un pilsoniskajām brīvībām. Tās saņem un izskata ziņojumus un citu informāciju no privātuma aizsardzības amatpersonām un pilsonisko brīvību aizsardzības amatpersonām un, attiecīgā gadījumā, izsaka ar to darbībām saistītus ieteikumus. Saskaņā ar 2007. gada Likuma par 11. septembra komisiju (kodificēts: *42 U.S.C. § 2000ee-1*) Īstenošanas noteikumu 803. pantu astoņu federālo aģentūru (tostarp Aizsardzības ministrijas, Iekšzemes drošības ministrijas, Nacionālās izlūkošanas direktora biroja un Centrālās izlūkošanas aģentūras direktora biroja) un visu pārējo Padomes

iecelto papildu aģentūru privātuma un pilsonisko brīvību aizsardzības amatpersonām ir jāiesniedz PPBPP periodiski pārskati, tostarp jānorāda attiecīgās aģentūras saņemto sūdzību par iespējamiem pārkāpumiem skaits, veids un ievirze. Likumā, ar ko pilnvaro PPBPP, šai padomei ir likts saņemt šos pārskatus un, attiecīgā gadījumā, izteikt privātuma un pilsonisko brīvību aizsardzības amatpersonām ieteikumus par to darbībām.

IV PIELIKUMS

Vēstule no Federālās tirdzniecības komisijas priekšsēdētājas *Edith Ramirez*

2016. gada 7. jūlijs

PA E-PASTU

Verai Jourovai,
tieslietu, patērētāju un dzimumu līdztiesības komisārei
Eiropas Komisija
Rue de la Loi/Wetstraat 200
1049 Brisele
Beļģija

Cienījamā komisāres kundze!

Amerikas Savienoto Valstu Federālās tirdzniecības komisija ("FTK") novērtē iespēju aprakstīt, kā tā panāk jaunā ES un ASV privātuma vairoga regulējuma ("privātuma vairoga regulējums" vai "regulējums") izpildi. Mēs uzskatām, ka regulējums ievērojami palīdzēs veicināt privātumu aizsargājošus komercdarījumus pasaulē, kas kļūst arvien vairāk savienota. Tas ļaus uzņēmumiem īstenot svarīgas darbības pasaules ekonomikā, vienlaikus nodrošinot, ka ES patērētāji nezaudē būtiskas privātuma aizsardzības garantijas. FTK ir izsenis apņēmusies aizsargāt privātumu otrpus robežām un uzskatīs jaunā regulējuma izpildes panākšanu par svarīgu prioritāti. Turpmāk esam snieguši vispārīgu izklāstu par to, kā FTK līdz šim ir stingri panākusi privātuma aizsardzību, tostarp sākotnējās "drošības zonas" programmas izpildi, un esam aprakstījuši FTK pieeju jaunā regulējuma izpildei.

FTK pirmoreiz publiski pauda apņemšanos īstenot "drošības zonas" programmu 2000. gadā. FTK tālaika priekšsēdētājs Robert Pitofsky toreiz nosūtīja Eiropas Komisijai vēstuli, kurā izklāstīja FTK solījumu aktīvi strādāt pie "drošības zonas" privātuma principu izpildes panākšanas. FTK ir turpinājusi pildīt šo apņemšanos, ierosinot gandrīz 40 izpildes panākšanas prasību, īstenojot daudz papildu izmeklēšanu, kā arī sadarbojoties ar individuālām Eiropas datu aizsardzības iestādēm ("ES DAI") abām pusēm aktuālos jautājumos.

Pēc tam, kad Eiropas Komisija 2013. gada novembrī pauda bažas par "drošības zonas" programmas pārvaldību un izpildi, mēs un ASV Tirdzniecības ministrija sākām konsultēties ar Eiropas Komisijas amatpersonām, lai apzinātu programmas stiprināšanas veidus. Šo konsultāciju norises gaitā Tiesa 2015. gada 6. oktobrī pieņēma nolēmumu lietā *Schrems*, kurā *inter alia* atzina par spēkā neesošu Eiropas Komisijas lēmumu par "drošības zonas" programmas nodrošinātā aizsardzības līmeņa pietiekamību. Pēc šā nolēmuma pieņemšanas mēs turpinājām ciešu sadarbību ar Tirdzniecības ministriju un Eiropas Komisiju, cenšoties nostiprināt ES iedzīvotājiem nodrošināto privātuma aizsardzību. Privātuma vairoga regulējums ir šo pastāvīgo apspriešanos rezultāts. FTK, tāpat kā tika darīts attiecībā uz "drošības zonas" programmu, ar šo apņemas aktīvi īstenot jauno regulējumu. Šī vēstule ir šīs apņemšanās apliecinājums.

Konkrētāk, mēs apstiprinām, ka uzņemamies saistības četrās galvenajās jomās: 1) pieprasījumu prioritāra izskatīšana un izmeklēšana; 2) reaģēšana uz nepatiesiem vai maldinošiem apgalvojumiem par dalību privātuma vairoga programmā; 3) pastāvīga rīkojumu izpildes uzraudzība un 4) lielāka mijiedarbība un sadarbība ar izpildes panākšanu saistītos jautājumos ar ES DAI. Turpmāk ir sniegta sīki izstrādāta informācija par katru apņemšanos, attiecīgā pamatinformācija par FTK lomu patērētāju privātuma aizsardzībā un "drošības zonas" izpildes panākšanā, kā arī plašāk ieskicēts Amerikas Savienoto Valstu privātuma regulējums ([1]).

I. PAMATINFORMĀCIJA

A. **FTK darbs izpildes panākšanas jomā un politiskais darbs**

FTK ir plašas civiltiesiskās izpildes pilnvaras, lai veicinātu patērētāju aizsardzību un konkurenci komerciālajā jomā. Īstenojot savas patērētāju aizsardzības pilnvaras, FTK panāk plaša tiesību aktu klāsta izpildi, lai aizsargātu patērētāju datu

([1]) A papildinājumā esam snieguši papildu informāciju par ASV federālajiem un štatu privātuma tiesību aktiem. Savukārt mūsu jaunāko darbību privātuma un drošības izpildes panākšanas jomā kopsavilkums ir pieejams arī FTK tīmekļa vietnē https://www.ftc.gov/reports/privacy-data-security-update-2015

privātumu un drošību. FTK piemērotajā primārajā tiesību aktā, proti, FTK likumā (*FTC Act*), ir aizliegtas "negodīgas" un "maldinošas" darbības vai prakse, ko veic tirdzniecībā vai kuras to ietekmē ([1]). Atspoguļojums, bezdarbība vai darbība ir maldinoša, ja tā ir materiāla un konkrētajos apstākļos var maldināt patērētājus, kas rīkojas saprātīgi ([2]).Darbība vai prakse ir negodīga, ja tā rada vai var radīt patērētājiem būtisku kaitējumu, kas nav samērīgi novēršams un ko neatsver labums, kuru patērētājs gūst vai kurš ietekmē konkurenci ([3]). FTK arī piemēro mērķtiecīgus likumus, kas aizsargā ar veselības aprūpi, kredītiem un citiem finanšu aspektiem saistītu informāciju, kā arī bērnu tiešsaistes informāciju, un ir pieņēmusi katra attiecīgā likuma īstenošanas noteikumus.

Atbilstīgi FTK likumam FTK ir jurisdikcija jautājumos, kas rodas "tirdzniecībā vai kas to ietekmē." FTK nav jurisdikcijas attiecībā uz kriminmāltiesību piemērošanā vai ar valsts drošību saistītos jautājumos. FTK arī nav kompetenta vairumā pārējo valdības darbību. Turklāt FTK jurisdikcija attiecībā uz komercdarbībām, tostarp banku, aviosabiedrību, apdrošināšanas nozares un publisko telesakaru operatoru darbībām, ir ierobežota. FTK pilnvaras neattiecas arī uz vairumu bezpeļņas organizāciju, taču tai ir jurisdikcija attiecībā uz fiktīvām labdarības vai citām bezpeļņas struktūrām, kas patiesībā strādā, lai gūtu peļņu. Tā ir kompetenta arī saistībā ar bezpeļņas organizācijām, kas darbojas, lai nodrošinātu peļņu to locekļiem, kuru mērķis ir peļņa, tostarp sniedzot tiem ievērojamus ekonomiskos ieguvumus ([4]). Atsevišķos gadījumos FTK jurisdikcija pārklājas ar citu tiesībaizsardzības aģentūru pilnvarām.

Esam izveidojuši nopietnas darba attiecības ar federālajām un štatu iestādēm un ar tām cieši sadarbojamies, lai koordinētu izmeklēšanas vai attiecīgos gadījumos sagatavotu pieprasījumus.

FTK pieejas privātuma aizsardzībai pamatā ir izpildes panākšana. Līdz šim FTK ir ierosinājusi vairāk nekā 500 lietu par patērētāju informācijas privātuma un drošības aizsardzību. Šis lietu kopums attiecas gan uz bezsaistes, gan tiešsaistes informāciju un ietver izpildes panākšanas darbības attiecībā uz lieliem un maziem uzņēmumiem, par kuriem uzskata, ka tie nav pienācīgi atbrīvojušies no sensitīviem patērētāju datiem, nav nodrošinājuši patērētāju personiskās informācijas drošību, ir maldinoši izsekojuši patērētājus tiešsaistē, sūtījuši patērētājiem surogātpastu, instalējuši spiegprogrammatūru vai citu ļaunprogrammatūru patērētāju datoros, pārkāpuši nezvanīšanas un citus pārdošanas pa tālruni noteikumus, kā arī neatbilstoši vākuši un koplietojuši mobilajos tālruņos glabāto patērētāju informāciju. FTK īstenotās izpildes panākšanas darbības – gan fiziskajā, gan digitālajā pasaulē – nodod uzņēmumiem būtisku vēstījumu par nepieciešamību aizsargāt klientu privātumu.

FTK arī ir īstenojusi vairākas politiskās iniciatīvas, kuru mērķis ir patērētāju privātuma palielināšana, un tās ir veicinājušas FTK darbu izpildes jomā. Tā ir rīkojusi darbseminārus un pieņēmusi ziņojumus ar paraugprakses ieteikumiem nolūkā uzlabot privātumu mobilo ierīču segmentā; palielināt datu brokeru nozares pārredzamību; maksimāli palielināt no lielajiem datiem izrietošos ieguvumus, vienlaikus mazinot ar tiem saistītos riskus, īpaši patērētājiem, kam ir mazi ienākumi un kas ir nepietiekami apkalpoti; kā arī inter alia norādīt uz privātuma un drošības apsvērumiem saistībā ar sejas atpazīšanu un lietisko internetu.

Lai veicinātu savu izpildes panākšanas un politikas izstrādes iniciatīvu ietekmi, FTK iesaistās arī patērētāju un uzņēmumu izglītošanā. Tā ir izmantojusi dažādus instrumentus – publikācijas, tiešsaistes resursus, darbseminārus un sociālos medijus –, lai sniegtu izglītojošus materiālus par plašu tematu klāstu, tostarp mobilajām lietotnēm, bērnu privātumu un datu drošību. Jaunākais komisijas darba rezultāts ir tās sāktā iniciatīva "Sāc ar drošību" (Start With Security), kuras satvarā uzņēmumiem sniedz jaunas norādes, pamatojoties uz secinājumiem, kas izriet no aģentūras datu drošības lietām, kā arī rīko darbsemināru kopumu visā valstī. Turklāt FTK ir ilgstoši bijusi galvenā patērētāju izglītotāja datordrošības pamatjautājumos. Pagājušajā gadā mūsu tīmekļa vietnei OnGuard un tās ekvivalentam spāņu valodā Alerta en Línea bija vairāk nekā pieci miljoni skatījumu.

B. **ASV juridiskās aizsardzības pasākumi, ko var izmantot patērētāji no ES**

Privātuma vairoga regulējums darbosies plašākā ASV privātuma regulējuma satvarā, ar ko vairākos veidos tiek aizsargāti arī ES patērētāji.

([1]) *15 U.S.C. § 45(a).*
([2]) Sk. *FTC Policy Statement on Deception*, pievienots *Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984)*, pieejams vietnē https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception
([3]) Sk. *15 U.S.C § 45(n); FTC Policy Statement on Unfairness*, pievienots *Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984)*, pieejams vietnē https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness
([4]) Sk. *California Dental Ass'n v. FTC, 526 U.S. 756 (1999).*

FTK likumā paredzētais negodīgu vai maldinošu darbību vai prakses aizliegums neaprobežojas ar ASV patērētāju aizsardzību no ASV uzņēmumu rīcības, jo tas attiecas uz praksi, kas 1) rada vai var radīt pamatoti paredzamu kaitējumu Amerikas Savienotajās Valstīs vai 2) ietver materiālu darbību Amerikas Savienotajās Valstīs. Turklāt, aizsargājot patērētājus no citām valstīm, FTK var izmantot visus vietējo patērētāju aizsardzībai pieejamos tiesiskās aizsardzības līdzekļus, arī atpakaļatdošanu.

FTK darbs izpildes panākšanas jomā patiešām nodrošina būtiskus ieguvumus gan ASV, gan citu valstu patērētājiem. Piemēram, mūsu īstenotās FTK likuma 5. panta izpildes panākšanas lietas ir nodrošinājušas ne tikai ASV, bet arī ārvalstu patērētāju privātuma aizsardzību. Pret informācijas brokeri *Accusearch* ierosinātajā lietā FTK apgalvoja, ka uzņēmums, pārdodot trešajām personām konfidenciālus tālruņa ierakstus bez patērētāju ziņas un piekrišanas, īstenoja negodīgu praksi un tādējādi pārkāpa FTK likuma 5. pantu. *Accusearch* pārdeva gan ar ASV, gan citu valstu patērētājiem saistītu informāciju ([1]). Tiesa attiecībā uz *Accusearch* pieņēma aizliegumu, nosakot, ka tas *inter alia* nedrīkst tirgot vai pārdot tā patērētāju personisko informāciju bez viņu rakstiskas piekrišanas, ja vien tā nav likumīgi iegūta no publiski pieejamas informācijas, un pieprasīja gandrīz 200 000 USD atmaksu ([2]).

Kā vēl vienu piemēru var minēt risinājumu, ko FTK panāca saistībā ar *TRUSTe*. Tas nodrošina, ka patērētāji, tostarp Eiropas Savienības iedzīvotāji, var paļauties uz apgalvojumiem, ko starptautiska pašregulatīva organizācija izsaka par tās īstenoto vietējo un ārvalstu tiešsaistes pakalpojumu pārbaudi un sertifikāciju ([3]). Svarīgi, ka ar mūsu prasību pret *TRUSTe*, arī tiek plašāk nostiprināta privātuma pašregulatīvā sistēma, nodrošinot to struktūru pārskatatbildību, kurām ir būtiska nozīme pašregulatīvo shēmu, tostarp pārrobežu privātuma regulējuma, īstenošanā.

FTK panāk arī citu tādu mērķtiecīgu tiesību aktu izpildi, kuros paredzētā aizsardzība attiecas arīdzan uz patērētājiem no citām valstīm, piemēram, Bērnu privātuma tiešsaistē aizsardzības likuma (*Children's Online Privacy Protection Act – COPPA*) izpildi. *COPPA* citstarp ir noteikts, ka uz bērniem vērstu tīmekļa vietņu un tiešsaistes pakalpojumu vai vispārīgai auditorijai paredzētu vietņu operatoriem, kuri apzināti vāc personisku informāciju no bērniem, kas nav sasnieguši 13 gadu vecumu, par to jāinformē vecāki un jāsaņem no viņiem pierādāma piekrišana. ASV bāzētām tīmekļa vietnēm un pakalpojumiem, kam piemēro *COPPA* un kas vāc personisku informāciju no ārvalstu bērniem, ir jāatbilst *COPPA* prasībām. Tam ir jāatbilst arī ārvalstīs bāzētām vietnēm un tiešsaistes pakalpojumiem, ja tie ir vērsti uz bērniem Amerikas Savienotajās Valstīs vai ar tiem apzināti vāc personisko informāciju no bērniem, kuri dzīvo Amerikas Savienotajās Valstīs. Papildus ASV federālajiem tiesību aktiem, kuru izpildi panāk FTK, ES patērētājus var aizsargāt arī konkrēti citi federālie un štatu patērētāju aizsardzības un privātuma tiesību akti.

C. **"Drošības zonas" izpildes panākšana**

Savas privātuma un drošības nodrošināšanas programmas satvarā FTK ir arīdzan centusies aizsargāt ES patērētājus, īstenojot izpildes panākšanas darbības attiecībā uz "drošības zonas" pārkāpumiem. FTK ir ierosinājusi 39 prasības par "drošības zonas" izpildi: 36 no tām attiecās uz, iespējams, nepatiesiem apgalvojumiem par sertifikāciju, un trīs – pret *Google*, *Facebook* un *Myspace* – uz iespējamiem "drošības zonas" privātuma principu pārkāpumiem ([4]). Šīs lietas ilustrē apliecinājumu izpildāmību un neatbilstības sekas. Saskaņā ar rīkojumiem par 20 gadus ilgu piekrišanu *Google*, *Facebook* un *Myspace* jāīsteno vispusīgas privātuma aizsardzības programmas, kas ir pienācīgi jāizstrādā, lai novērstu ar pašreizējo un jaunu produktu un pakalpojumu izstrādi un pārvaldību saistītos privātuma apdraudējumus un aizsargātu personiskās informācijas privātumu un konfidencialitāti Šajos rīkojumos pieprasītajās vispusīgajās privātuma aizsardzības programmās ir jānosaka prognozējamie būtiskie riski un jāievieš kontroles pasākumi to mazināšanai. Uzņēmumiem arī jāapņemas veikt pastāvīgus un neatkarīgus to privātuma programmu novērtējumus, kas ir jāiesniedz FTK. Rīkojumos šiem uzņēmumiem arī ir aizliegts sagrozīt informāciju par savu privātuma praksi un dalību jebkādā privātuma vai drošības programmā. Šis aizliegums attiektos arī uz uzņēmumu darbībām un praksi jaunā privātuma vairoga regulējuma satvarā. FTK var panākt šo rīkojumu izpildi, pieprasot civilsodus. Faktiski 2012. gadā uzņēmums *Google*, lai panāktu, ka

([1]) Sk. Kanādas Privātuma komisāra birojs, sūdzība, kas saskaņā ar Personiskās informācijas aizsardzības un elektronisko dokumentu likumu (*Personal Information Protection and Electronic Documents Act – PIPEDA*) iesniegta par *Accusearch, Inc.*, kas veic uzņēmējdarbību kā Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Kanādas Privātuma komisāra birojs FTK ierosinātās prasības pārsūdzības procesā iesniedza *amicus curiae* atzinumu un veica individuālu izmeklēšanu, kurā secināja, ka ar *Accusearch* praksi tika pārkāpti arī Kanādas tiesību akti.

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

([3]) Sk. *In the Matter of True Ultimate Standards Everywhere, Inc., Nr. C-4512 (F.T.C. Mar. 12, 2015*) (lēmums un rīkojums), pieejams https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf

([4]) *Google, Inc.* lietā sk. *Nr. C-4336 (F.T.C. Oct. 13 2011*) (lēmums un rīkojums), pieejams https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *Facebook, Inc.* lietā sk. *Nr. C-4365 (F.T.C. July 27, 2012*) (lēmums un rīkojums), pieejams https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *Myspace LLC* lietā sk. *Nr. C-4369 (F.T.C. May 20, 2011*) (lēmums un rīkojums), pieejams https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace

tiek atceltas apsūdzības par tam adresētā rīkojuma pārkāpšanu, samaksāja rekordlielu civilsodu – 22,5 miljonus USD. Tādējādi šie FTK rīkojumi palīdz aizsargāt vairāk nekā miljardu patērētāju visā pasaulē, tostarp vairākus simtus miljonus patērētāju, kuri dzīvo Eiropā.

FTK lietās uzsvars ir likts arī uz nepatiesiem, maldinošiem vai mānīgiem apgalvojumiem par dalību "drošības zonas" programmā. FTK šos apgalvojumus uztver nopietni. Piemēram, 2011. gadā FTK pret uzņēmēju, kas Amerikas Savienotajās Valstīs veic tirdzniecību internetā, ierosināja prasību (*FTC v. Karnani*), kurā apgalvoja, ka viņš un viņa uzņēmums, tostarp izmantojot tīmekļa paplašinājumus ".uk" un atsaucoties uz Lielbritānijas valūtu un Apvienotās Karalistes pasta sistēmu, radīja Lielbritānijas patērētājiem maldīgu priekšstatu, ka uzņēmums atrodas Apvienotajā Karalistē ([1]). Tomēr, kad patērētāji saņēma produktus, viņi konstatēja, ka jāmaksā neparedzētas importa nodevas, ka garantijas nav spēkā Apvienotajā Karalistē un, lai atgūtu naudu, ir jāmaksā nodevas. FTK arī apsūdzēja atbildētājus patērētāju maldināšanā par dalību "drošības zonas" programmā. Konkrētāk, visas no šīs prakses cietušās personas atradās Apvienotajā Karalistē.

Daudzas citas mūsu īstenotās "drošības zonas" izpildes panākšanas lietas attiecās uz organizācijām, kas pievienojās "drošības zonas" programmai, bet neveica ikgadējo sertifikācijas atjaunošanu un turpināja apgalvot, ka ir programmas dalībnieki. Kā sīkāk aprakstīts turpmāk, FTK arīdzan ir apņēmusies reaģēt uz nepatiesiem apgalvojumiem par dalību privātuma vairoga programmā. Šī stratēģiskā izpildes panākšanas darbība papildinās Tirdzniecības ministrijas pieaugošos centienus pārbaudīt programmas sertifikācijas un atkārtotās sertifikācijas prasību izpildi, tās īstenotos atbilstības uzraudzības pasākumus, tostarp izmantojot programmas dalībniekiem paredzētas anketas, kā arī tās pieaugošos centienus konstatēt nepatiesus apgalvojumus par dalību programmā un jebkādas programmas sertifikācijas zīmes ļaunprātīgu izmantošanu ([2]).

II. PIEPRASĪJUMU PRIORITĀRA IZSKATĪŠANA UN IZMEKLĒŠANA

Tāpat kā attiecībā uz "drošības zonas" programmu, FTK apņemas uzskatīt par prioritāti ar privātuma vairogu saistītus pieprasījumus no ES dalībvalstīm. Mēs arī prioritāri izskatīsim pieprasījumus par neatbilstību pašregulatīvām pamatnostādnēm attiecībā uz privātuma vairoga regulējumu no organizācijām, kas pašas reglamentē privātuma aizsardzību, un citām neatkarīgām strīdu izšķiršanas struktūrām.

Lai sekmētu ES dalībvalstu iesniegto ar regulējumu saistīto pieprasījumu izskatīšanu, FTK izstrādā standartizētu pieprasījumu procesu un sniedz ES dalībvalstīm norādes par to, kāda informācija FTK visvairāk noderētu pieprasījuma izpētē. Īstenojot šos centienus, FTK iecels aģentūras kontaktpersonu, pie kuras ES dalībvalstis varēs vērsties saistībā ar pieprasījumiem. Ir ļoti noderīgi, ja pieprasījuma iesniedzēja iestāde ir veikusi sākotnēju iespējamā pārkāpuma izpēti un var sadarboties ar FTK izmeklēšanā.

Saņemot pieprasījumu no ES dalībvalsts vai pašregulatīvas organizācijas, FTK var īstenot dažādas izvirzīto jautājumu risināšanas darbības. Mēs varam, piemēram, pārskatīt uzņēmuma privātuma politiku, iegūt papildu informāciju tieši no uzņēmuma vai trešajām personām, sniegt pieprasījuma iesniedzējai struktūrai jaunāko informāciju, izvērtēt, vai pastāv pārkāpumu pazīmes un vai ir ietekmēts liels patērētāju skaits, noteikt, vai pieprasījumā skartie jautājumi ir Tirdzniecības ministrijas kompetencē, novērtēt, vai patērētāju un uzņēmumu izglītošana būtu noderīga, un, attiecīgā gadījumā, ierosināt izpildes procesu.

FTK arīdzan apņemas, ievērojot konfidencialitātes tiesību aktus un ierobežojumus, sniegt pieprasījuma iesniedzējām tiesībaizsardzības iestādēm attiecīgu informāciju, tostarp par pieprasījumu statusu. Ciktāl praksē iespējams un atkarībā no saņemto pieprasījumu skaita un veida, sniegtajā informācijā tiks iekļauts pieprasījumā norādīto aspektu novērtējums, tostarp aprakstīti būtiski izvirzītie jautājumi un visas darbības, kas veiktas, lai reaģētu uz tiesību aktu pārkāpumiem, kuri ir FTK jurisdikcijā. Lai palielinātu nelikumīgas rīcības apkarošanas centienu rezultativitāti, FTK arī sniegs pieprasītājai

([1]) Sk. *FTC v. Karnani, Nr. 2:09-cv-05276 (C.D. Cal. May 20, 2011*) (paredzēts galīgais rīkojums), pieejams https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; *sk. arī* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways,* https://www.ftc.gov/blog/2011/06/around-world-shady-ways (2011. gada 9. jūnijs).

([2]) Tirdzniecības ministra starptautiskās tirdzniecības jautājumos vietnieka pienākumu izpildītāja *Ken Hyatt* vēstule Tieslietu, patērētāju un dzimumu līdztiesības komisārei Verai Jourovai.

iestādei atsauksmes par saņemto pieprasījumu veidiem. Ja pieprasījuma iesniedzēja iestāde vēlas saņemt informāciju par konkrēta pieprasījuma statusu, lai pati īstenotu izpildes procesu, FTK atbildēs, ņemot vērā izskatīto pieprasījumu daudzumu un ievērojot konfidencialitātes un citas juridiskās prasības.

FTK arī cieši sadarbosies ar ES datu uzraudzības iestādēm, sniedzot tām ar izpildes panākšanu saistītu palīdzību. Piemēram, attiecīgos gadījumos tā varētu dalīties ar informāciju un palīdzēt izmeklēšanā atbilstīgi ASV Tīmekļa drošības likumam (*SAFE WEB Act*), kurā FTK ir atļauts palīdzēt citu valstu tiesībaizsardzības aģentūrām tādu tiesību aktu izpildes panākšanā, kuros aizliegtā prakse būtiski līdzinās FTK piemērotajos tiesību aktos aizliegtajām darbībām ([1]). Šīs palīdzības satvarā FTK var sniegt informāciju, kas iegūta saistībā ar FTK izmeklēšanu, ierosināt obligātu procesu tās ES DAI vārdā, kas pati veic individuālu izmeklēšanu, kā arī lūgt mutiskas liecinieku vai atbildētāju liecības saistībā ar DAI īstenoto izpildes procesu, ievērojot ASV Tīmekļa drošības likuma prasības. FTK regulāri izmanto šīs pilnvaras, lai palīdzētu citu pasaules valstu iestādēm privātuma un patērētāju aizsardzības lietu īstenošanā ([2]).

Papildus tam,ka ES dalībvalstu un privātuma pašregulatīvo organizāciju iesniegtie ar privātuma vairogu saistītie pieprasījumi tiks izskatīti kā prioritāte ([3]), FTK apņemas izmeklēt iespējamus regulējuma pārkāpumus pēc savas iniciatīvas, attiecīgajā gadījumā izmantojot dažādus instrumentus.

Krietni ilgāk par desmitgadi FTK ir uzturējusi spēcīgu programmu ar komercorganizācijām saistītu privātuma un drošības pārkāpumu izmeklēšanai. Attiecīgajās izmeklēšanās FTK regulāri pārbaudīja, vai izmeklētā struktūra izteica apgalvojumus par "drošības zonu". Ja struktūra šādus apgalvojumus izplatīja un izmeklēšanā tika konstatēti acīmredzami "drošības zonas" privātuma principu pārkāpumi, FTK ierosinātajās izpildes panākšanas prasībās iekļāva arī apsūdzības "drošības zonas" pārkāpumos. Mēs turpināsim šīs proaktīvās pieejas īstenošanu arī attiecībā uz jauno regulējumu. Jāuzsver, ka FTK īstenoto izmeklēšanu skaits ir daudz lielāks nekā no tām izrietošo publisko izpildes procesu daudzums. Daudzas FTK veiktās izmeklēšanas ir slēgtas, jo darbinieki nekonstatē acīmredzamu tiesību akta pārkāpumu. Tā kā FTK izmeklēšanas nav publiskas un norit konfidenciāli, sabiedrībai bieži netiek paziņots par izmeklēšanas slēgšanu.

Gandrīz 40 izpildes prasību, ko FTK ierosināja saistībā ar "drošības zonas" programmu, apliecina aģentūras apņēmību proaktīvi panākt pārrobežu privātuma programmu izpildi. Īstenojot regulārās privātuma un drošības izmeklēšanas, FTK pievērsīs uzmanību arī iespējamiem regulējuma pārkāpumiem.

III. REAĢĒŠANA UZ NEPATIESIEM VAI MALDINOŠIEM APGALVOJUMIEM PAR DALĪBU PRIVĀTUMA VAIROGA PROGRAMMĀ

Kā norādīts iepriekš, FTK vērsīsies pret struktūrām, kas sagroza informāciju par savu dalību regulējuma īstenošanā. FTK prioritāri izskatīs Tirdzniecības ministrijas pieprasījumus par organizācijām, kuras, kā uzskata ministrija, nepamatoti uzdodas par pašreizējām privātuma vairoga programmas dalībniecēm vai bez atļaujas izmanto kādu ar regulējumu saistītu sertifikācijas zīmi.

Turklāt mēs atzīmējam, ka, ja organizācijas privātuma politikā ir apgalvots, ka tā ievēro privātuma vairoga principus, tomēr nav reģistrējusies vai nav saglabājusi reģistrāciju Tirdzniecības ministrijā, šis fakts vien neatbrīvos organizāciju no FTK centieniem panākt regulējumā paredzēto saistību izpildi.

([1]) Nosakot, vai īstenot savas pilnvaras, kas izriet no ASV Tīmekļa drošības likuma, FTK *inter alia* izvērtē: "A) vai pieprasītāja aģentūra ir piekritusi sniegt vai sniegs savstarpēju palīdzību komisijai; B) vai pieprasījuma izpilde neapdraudētu Amerikas Savienoto Valstu sabiedrības intereses; un C) vai pieprasītājas aģentūras īstenotā izmeklēšana vai izpildes process attiecas uz darbībām vai praksi, kas rada vai varētu radīt kaitējumu ļoti lielam cilvēku skaitam." *15 U.S.C. § 46(j)(3)*. Šīs pilnvaras neattiecas uz konkurences tiesību aktu izpildes panākšanu.

([2]) Piemēram, 2012.–2015. fiskālajā gadā FTK izmantoja savas no ASV Tīmekļa drošības likuma izrietošās pilnvaras, lai sniegtu informāciju, atbildot gandrīz uz 60 pieprasījumiem no ārvalstu aģentūrām un pieņēma teju 60 civiltiesiskās izmeklēšanas pieprasījumu (līdzvērtīgi administratīvajām pavēstēm), palīdzot 25 ārvalstu izmeklēšanās.

([3]) Lai gan FTK nerisina individuālas patērētāju sūdzības un nedarbojas kā šādu sūdzību izskatīšanas starpnieks, tā apstiprina, ka prioritāri izskatīs ES ar privātuma vairogu saistītos DAI pieprasījumus. Turklāt FTK, pamatojoties uz savā patērētāju aizsardzības datubāzē Consumer Sentinel (pieejama daudzām tiesībaizsardzības aģentūrām) iekļautajām sūdzībām, apzina tendences, izvirza ar izpildes panākšanu saistītas prioritātes un nosaka potenciālos izmeklēšanas subjektus. ES iedzīvotāji, izmantojot to pašu sūdzību sistēmu, kas ir pieejama ASV pilsoņiem, var iesniegt sūdzību FTK vietnē www.ftc.gov/complaint. Tomēr, ja ES iedzīvotājiem ir individuālas ar privātuma vairogu saistītas sūdzības, iespējams, visnoderīgāk būtu iesniegt tās savas dalībvalsts DAI vai strīdu alternatīvas izšķiršanas pakalpojumu sniedzējam.

IV. RĪKOJUMU IZPILDES UZRAUDZĪBA

FTK arī apstiprina savu apņemšanos uzraudzīt izpildes rīkojumu īstenošanu, lai nodrošinātu atbilstību privātuma vairoga regulējumam.

Mēs pieprasīsim regulējuma ievērošanu, turpmākajos ar regulējumu saistītajos FTK rīkojumos paredzot dažādus atbilstošus aizlieguma noteikumus. Tas ietver aizliegumu sagrozīt informāciju par regulējumu un citām privātuma aizsardzības programmām, ja tās ir attiecīgās FTK prasības pamatā.

FTK lietas, ar ko panāk sākotnējās "drošības zonas" programmas izpildi, ir pamācošas. No 36 lietām, kas saistītas ar nepatiesiem vai maldinošiem apgalvojumiem par "drošības zonas" sertifikāciju, pilnīgi visos rīkojumos atbildētājam tika aizliegts sagrozīt informāciju par tā dalību "drošības zonas" vai jebkādā citā privātuma vai drošības programmā un prasīts darīt FTK pieejamus atbilstības ziņojumus. Lietās, kas attiecās uz "drošības zonas" privātuma principu pārkāpumiem, uzņēmumiem pieprasīja īstenot visaptverošas privātuma aizsardzības programmas un 20 gadu periodā katru otro gadu saņemt par tām neatkarīgus, trešo personu veiktus novērtējumus, kas jāiesniedz FTK.

Par FTK administratīvo rīkojumu pārkāpšanu var piespriest civilsodu līdz 16 000 USD par pārkāpumu vai 16 000 USD par pārkāpuma turpināšanas dienu, ([1]) un, ja prakse ietekmē lielu patērētāju skaitu, kopsumma var sasniegt vairākus miljonus dolāru. Katrā piekrišanas rīkojumā ir arī noteikumi par ziņošanu un atbilstību. Struktūrām, kurām rīkojums ir adresēts, norādīto gadu skaitu jāglabā dokumenti, kas apliecina to atbilstību. Par rīkojumu saturu arī jāinformē darbinieki, kas nodrošina to izpildi.

FTK sistemātiski uzrauga visu tās pieņemto rīkojumu, arī ar "drošības zonu" saistīto, ievērošanu. FTK savu privātuma un datu drošības rīkojumu izpildes panākšanu uztver nopietni un, ja vajadzīgs, ierosina to izpildes prasības. Piemēram, kā norādīts iepriekš, uzņēmums *Google* samaksāja 22,5 miljonus USD lielu civilsodu, lai tiktu atceltas apsūdzības par tam adresētā FTK rīkojuma pārkāpšanu. Jāuzsver, ka FTK rīkojumi arī turpmāk nodrošinās aizsardzību visiem attiecīgā uzņēmuma klientiem neatkarīgi no to atrašanās vietas, nevis tikai tiem, kuri ir iesnieguši sūdzības.

Visbeidzot, FTK turpinās uzturēt tiešsaistes sarakstu ar uzņēmumiem, uz kuriem attiecas "drošības zonas" programmas vai jaunā privātuma vairoga regulējuma piespiedu izpildes procesā pieņemti rīkojumi ([2]). Turklāt patlaban atbilstīgi privātuma vairoga principiem uzņēmumiem, kuriem principu neievērošanas dēļ piemēro FTK vai tiesas rīkojumu, ir jāpublisko visas komisijai iesniegta atbilstības vai novērtējuma ziņojuma sadaļas, kas ir saistītas ar regulējumu, ciktāl tas nav pretrunā konfidencialitātes tiesību aktiem un noteikumiem.

V. MIJIEDARBĪBA AR ES DAI UN SADARBĪBA IZPILDES JOMĀ

FTK atzīst ES DAI būtisko nozīmi regulējuma atbilstības jomā un aicina paplašināt apspriešanos un ar izpildes panākšanu saistīto sadarbību. Papildus visām apspriedēm ar pieprasītāju DAI par konkrētas lietas aspektiem FTK apņemas piedalīties periodiskās sanāksmēs ar ieceltiem 29. panta darba grupas pārstāvjiem, lai vispārīgi pārspriestu, kā uzlabot sadarbību regulējuma izpildes panākšanas jomā. FTK arī kopā ar Tirdzniecības ministrijas, Eiropas Komisijas un 29. panta darba grupas pārstāvjiem piedalīsies regulējuma ikgadējā pārskatīšanā, lai apspriestu tā īstenošanu.

FTK arī mudina izstrādāt instrumentus, kas uzlabotu sadarbību izpildes jomā gan ar ES DAI, gan citām privātuma aizsardzības iestādēm no visas pasaules. Konkrētāk, FTK kopā ar izpildes partneriem no Eiropas Savienības un citām pasaules valstīm pagājušajā gadā laida klajā brīdinājuma sistēmu, kas darbojas Globālā privātuma aizsardzības tīkla (GPEN) satvarā un kuras mērķis ir kopīgot informāciju par izmeklēšanām un veicināt piespiedu izpildes koordinēšanu. Šis GPEN brīdināšanas instruments varētu sevišķi noderēt privātuma vairoga regulējuma kontekstā. FTK un ES DAI to varētu izmantot, lai saskaņotu ar regulējumu saistītās darbības un citas privātuma izmeklēšanas un arī kā informācijas kopīgošanas sākumpunktu, lai varētu nodrošināt patērētājiem koordinētu un rezultatīvāku privātuma aizsardzību. Mēs

([1]) *15 U.S.C. § 45(m)*; *16 C.F.R. § 1.98*.
([2]) Sk. *FTC, Business Center, Legal Resources,* https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251

ceram arī turpmāk sadarboties ar iesaistītajām ES iestādēm pie izvietotās GPEN brīdinājuma sistēmas paplašināšanas un citu instrumentu izstrādes, lai uzlabotu sadarbību privātuma aizsardzības lietās, tostarp tajās, kas ir saistītas ar regulējumu.

FTK ar gandarījumu apstiprina savu apņemšanos panākt jaunā privātuma vairoga regulējuma izpildi. Mēs arī labprāt turpināsim kopā ar mūsu ES kolēģiem strādāt pie patērētāju privātuma aizsardzības abpus Atlantijas okeānam.

Ar cieņu

FTK priekšsēdētāja

Edith Ramirez

A papildinājums

ES un ASV privātuma vairoga konteksts – pārskats par situāciju ASV privātuma un drošības jomā

Aizsardzība, ko nodrošina ES un ASV privātuma vairoga shēma ("shēma") pastāv plašākā – privātās dzīves aizsardzības, ko nodrošina ASV tiesību sistēma kopumā –, kontekstā. Pirmkārt, Federālās tirdzniecības komisijai ("FTK") ir spēcīga privātuma un datu drošības programma, kas paredzēta ASV komercorganizācijām, un aizsargā patērētājus visā pasaulē. Otrkārt, situācija patērētāju privātuma un drošības aizsardzības jomā ASV ir būtiski uzlabojusies kopš 2000. gada, kad tika pieņemta sākotnējā ES un ASV "drošības zonas" programma. Kopš tā laika ir stājušies spēkā daudzi federālie un štatu tiesību akti privātuma un drošības jomā, un būtiski ir palielinājies privāto un publisko tiesvedību skaits saistībā ar privātuma tiesību izmantošanu. ASV tiesiskās aizsardzības attiecībā un patērētāju privātumu un drošību, ko praksē piemēro komercdatiem, plašais tvērums papildinās to aizsardzību, ko ES iedzīvotājiem sniedz shēma.

I. FTK VISPĀRĒJĀ PRIVĀTUMA UN DROŠĪBAS NODROŠINĀŠANAS PROGRAMMA

FTK ir vadošā ASV patērētāju aizsardzības aģentūra, kuras darbība koncentrējas uz privātuma ieverošanu komercdarbības jomā. FTK ir pilnvaras ierosināt lietu par negodīgu vai maldinošu darbību vai praksi, ar ko tiek pārkāpts patērētāju privātums, kā arī īstenot mērķorientētākus tiesību aktus privātuma jomā, kas aizsargā konkrētus finanšu datus un informāciju par veselības stāvokli, bērniem, kā arī informāciju, ko izmanto konkrētu lēmumu par patērētāju atbilstību pieņemšanā.

FTK ir nesalīdzināma pieredze patērētāju privātuma nodrošināšanā. FTK izpildes darbības ir bijušas vērstas pret nelikumīgām darbībām bezsaistes un tiešsaistes vidē. Piemēram, FTK ir vērsusi izpildes darbības pret plaši pazīstamiem uzņēmumiem, piemēram, *Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC*, un *Snapchat*, kā arī pret mazāk zināmiem uzņēmumiem. FTK ir vērsusies tiesā pret uzņēmumiem, kuri ar nolūku sūtījuši patērētājiem surogātpastu, instalējuši spiegprogrammatūru datoros, nav nodrošinājuši patērētāju personiskās informācijas drošību, ir maldinoši izsekojuši patērētājus tiešsaistē, pārkāpuši bērnu privātumu, pretlikumīgi vākuši mobilajos tālruņos glabāto patērētāju informāciju un nav nodrošinājuši internetam pieslēgto ierīču, kurās tiek glabāta personiskā informācija, drošību. Iepriekš minētā rezultātā pieņemtajos rīkojumos parasti noteikts, ka FTK veiks pastāvīgu uzraudzību divdesmit gadu garumā, aizliegts pārkāpt likumu un uzņēmumiem paredzētas būtiskas finansiālas sankcijas par rīkojuma pārkāpšanu ([1]). Svarīgi, ka FTK rīkojumi ne tikai aizsargā indivīdus, kuri, iespējams, ir sūdzējušies par kādu problēmu; drīzāk tie aizsargā visus patērētājus, kuri ir iesaistīti darījumdarbībās. Pārrobežu kontekstā FTK ir jurisdikcija aizsargāt patērētājus visā pasaulē pret darbībām, kas veiktas Amerikas Savienotajās Valstīs ([2]).

Līdz šim brīdim FTK ir ierosinājusi vairāk nekā 130 lietas par surogātpastu un spiegprogrammatūru, vairāk nekā 120 lietas par "nezvanīšanas" principa pārkāpumiem pārdošanas pa telefonu jomā, vairāk nekā 100 lietas saistībā ar Likuma par taisnīgu kreditēšanu (*Fair Credit Reporting Act)* pārkāpumiem, gandrīz 60 lietas par datu drošību, vairāk nekā 50 vispārējā privātuma pārkāpuma lietas, gandrīz 30 lietas par *Gramm-Leach-Bliley* likuma pārkāpumiem un vairāk nekā 20 lietas, lai panāktu Bērnu privātuma tiešsaistē aizsardzības likuma ("COPPA") izpildi. ([3]) Papildus minētajām lietām FTK izdod un publisko brīdinajuma vēstules ([4]).

([1]) Ikvienai struktūrai, kas neizpilda FTK rīkojumu, piemēro civilsodu līdz 16 000 USD apmērā par katru pārkāpumu vai sodu 16 000 USD apmērā dienā, ja pārkāpums turpinās. Sk. *15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).*

([2]) Kongress ir viennozīmīgi apstiprinājis FTK pilnvaras izmantot tiesiskās aizsardzības līdzekļus, arī atpakaļatdošanu, attiecībā uz visām darbībām, kurās iesaistīti ārvalstu tirgotāji, ja šādas darbības 1) rada vai var radīt pamatoti paredzamu kaitējumu Amerikas Savienotajās Valstīs vai 2) ietver materiālu darbību Amerikas Savienotajās Valstīs. Sk. *15 U.S.C. § 45(a)(4).*

([3]) Dažos gadījumos Komisijas privātuma un datu drošības lietās tiek apgalvots, ka uzņēmums piekopj gan maldinošu, gan negodīgu praksi; turklāt šajās lietās dažreiz ir konstatējami iespējami vairāku tiesību aktu pārkāpumi, piemēram, Likuma par taisnīgu kreditēšanu, *Gramm-Leach-Bliley* likuma, un COPPA.

([4]) Sk., piemēram, paziņojums presei, *Fed. Trade Comm'n, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations* (2014. gada 22. decembris), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; paziņojums presei, *Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations* (2013. gada 7. maijs), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; paziņojums presei ,*Fed. Trade Comm'n, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act* (2013. gada 3. aprīlis), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may

Atskatoties uz līdzšinējo pieredzi stingrā privātuma aizsardzības panākšanā, FTK regulāri sekoja līdzi tam, vai netiek pārkāpta "drošības zonas" programma. Kopš "drošības zonas" programmas pieņemšanas brīža, FTK pēc savas iniciatīvas ir veikusi vairākas izmeklēšanas attiecībā uz "drošības zonas" atbilstību un ir ierosinājusi 39 lietas pret ASV uzņēmumiem par "drošības zonas" pārkāpumiem. FTK turpinās šo proaktīvo pieeju, jaunās shēmas izpildes nodrošināšu īstenojot kā prioritāti.

II. PATĒRĒTĀJU PRIVĀTUMA AIZSARDZĪBA FEDERĀLĀ UN ŠTATU LĪMENĪ

Pārskatā par "drošības zonas" īstenošanu, kas kā pielikums pievienots Eiropas Komisijas Lēmumam par "drošības zonas" pietiekamību, ir sniegts kopsavilkums par tiesību aktiem privātuma jomā federālā un štatu līmenī, kuri bija spēkā brīdī, kad 2000. gadā tika pieņemta "drošības zonas" programma ([1]). Tajā laikā, papildus FTK likuma 5. pantam, daudzos federālos likumos tika reglamentēta personiskas informācijas vākšana un izmantošana, tostarp šādos: *the Cable Communications Policy Act, the Driver's Privacy Protection Act, the Electronic Communications Privacy Act, the Electronic Funds Transfer Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Right to Financial Privacy Act, the Telephone Consumer Protection Act, and the Video Privacy Protection Act*. Daudzos štatos šajās jomās bija līdzīgi tiesību akti.

Kopš 2000. gada ir vērojamas vairākas attīstības tendences federālā un štatu līmenī, kas nodrošina papildu aizsardzību patērētāju privātumam ([2]). Piemēram, federālajā līmenī FTK 2013. gadā izdarrīja labojumus *COPPA*, lai nodrošinātu papildu aizsardzību bērnu personiskajai informācijai. Tāpat FTK pieņēma divus aktus, ar kuriem īsteno *Gramm- Leach-Bliley* likumu – Privātuma aktu un Aizsardzības pasākumu aktu –, ar ko noteikts, ka finanšu iestādēm ([3]) ir jāatklāj to prases informācijas apmaiņas jomā un jāievieš visaptveroša informācijas drošības programma patērētāju informācijas aizsardzībai. ([4]) Līdzīgi 2003. gadā pieņemtais Likums par taisnīgiem un rūpīgiem kredītdarījumiem (*Fair and Accurate Credit Transactions Act*,"FACTA") papildina agrāk pieņemtos ASV tiesību aktus kreditēšana jomā, nosakot prasības attiecībā uz konkrētu sensitīvu finanšu datu maskēšanu, lietošanu un iznīcināšanu. Saskaņā ar *FACTA* FTK izsludināja vairākus aktus, tai skaitā par patērētāju tiesībām uz bezmaksas ikgadēju kredīta pārskatu; patērētāju pārskatu informācijas drošas iznīcināšanas noteikumiem; patērētāju tiesībām atteikties no konkrētu kredītu un apdrošināšanas piedāvājumu saņemšanas; patērētāju tiesībām atteikties no informācijas saņemšanas, ko savu produktu un pakalpojumu pārdošanai piedāvā saistīts uzņēmums; ka arī prasības finanšu iestādēm un kreditoriem ieviest identitātes zādzības atklāšanas un noveršanas programmas ([5]). Turklāt saskaņā ar Veselības apdrošināšanas parnesamības un pārskatatbildības likumu (*Health Insurance Portability and Accountability Act*) pieņemtie akti 2013. gadā tika pārskatīti, papildinot tos ar jauniem aizsardzības līdzekļiem informācijas par personas veselības stāvokli privātuma aizsardzībai un drošībai ([6]). Ir stājušies spēkā arī noteikumi par patērētaju aizsardzību pret negribētu pārdošanu pa telefonu, automatizetiem zvaniem un surogātpastu. Kongress ir pieņēmis arī tiesību aktus, ar kuriem konkrētiem uzņēmumiem, kuri vāc informāciju par personas veselības stāvokli, pārkāpuma gadījumā informēt patērētājus ([7]).

Arī štati ir bijuši ļoti aktīvi, pieņemot tiesību aktus saistība ar privātumu un drošību. Kopš 2000. gada 47 štati, Kolumbijas, Agaņas, Puertoriko apgabali un ASV Virdžīnu salas ir pieņemuši tiesību aktus, ar kuriem uzņēmumiem tiek

([1]) Sk. *U.S. Dep't of Commerce, Safe Harbor Enforcement Overview,* https://build.export.gov/main/safeharbor/eu/eg_main_018476

([2]) Plašāku pārskatu par tiesisko aizsardzību Amerikas Savienotajām Valstīs sk. *Daniel J. Solove & Paul Schwartz, Information Privacy Law* (5. izdevums, 2015. gads).

([3]) Finanšu iestādes *Gramm-Leach-Bliley* likumā ir definētas ļoti plaši, lai ietvertu visus uzņēmumus, kas ir "būtiskā apmērā iesaistīt" finanšu produktu vai pakalpojumu sniegšanā. Tas ietver, piemēram, uzņēmumus, kas izsniedz naudu pret čeku, īstermiņa kredītu izsniedzējus, hipotekāros māklerus, aizdevējus, kas nav bankas, mantas vai nekustamā īpašuma taksatorus un profesionālos nodokļu pārskatu sagatavotājus.

([4]) Saskaņā ar 2010. gada Patērētaju finanšu aizsardzības likumu (*Consumer Financial Protection Act*) ("CFPA"), *Title X of Pub. L. 111-203, 124 Stat. 1955* (2010. gada 21. jūlijs) (pazīstams arī kā "Dodd-Frank Wall Street Reform and Consumer Protection Act"), lielākā daļa no FTK reglamentēšanas pilnvarām saskaņā ar *Gramm-Leach-Bliley* likumu tika nodotas Patērētaju finanšu aizsardzības birojam (*Consumer Financial Protection Bureau*) ("CFPB"). FTK ir paturējusi izpildes pilnvaras saskaņā ar *Gramm-Leach- Bliley* likumu, kā arī reglamentēšanas pilnvaras saskaņā ar Aizsardzības pasākumu aktu un ierobežotas reglamentēšanas pilnvaras saskaņā ar Privātuma aktu attiecībā uz automašīnu tirgotājiem.

([5]) Saskaņā ar *CFPA* Komisija dala savas *FCRA* izpildes pilnvaras ar *CFPB*, savukārt reglamentēšanas pilnvaras lielā mērā ir nodotas *CFPB* (izņemot attiecībā uz brīdinājuma zīmēm un noteikumiem par [datu] iznīcināšanu).

([6]) Sk. *45 C.F.R. pts. 160, 162, 164.*

([7]) Sk., piemēram, *American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009)* un attiecīgos noteikumus, *45 C. F. R. § § 164.404–164.414; 16 C.F.R. pt. 318.*

prasīts informēt indivīdus par pārkāpumiem saistībā ar personisko informāciju. ([1]) Vismaz 32 štatos un Puertoriko apgabalā ir spēkā tiesību akti, ar kuriem nosaka prasības personiskas informācijas likvidēšanai vai iznīcināšanai ([2]). Vairākos štatos ir pieņemti vispārēji datu drošības tiesību akti. Turklāt Kalifornijā ir pieņemti vairāki tiesību akti privātuma jomā, tostarp likums, ar ko uzņemumiem prasa pieņemt privātuma politiku un atklāt to "neizsekošanas" praksi, ([3]) likums "*Shine the Light*", ar ko prasa lielāku pārredzamību no datu brokeriem, ([4]) un likums, kas prasa obligāti ieviest "pogu dzēšanai", lai nepilngadīgi bērni e varētu pieprasīt konkrētas sociālo plašsaziņas līdzekļu informācijas izdzēšanu. ([5]) Izmantojot šos tiesību aktus un citas pilnvaras, federālās un štatu valdības ir piemērojušas būtiskas sankcijas pret uzņēmumiem, kuri nav nodrošinājuši patērētāju privātuma aizsardzību un personiskās informācijas drošību ([6]).

Arī privātu prasību iztiesāšanas rezultātā ir pieņemti veiksmīgi spriedumi un izlīgumi, kas sniedz patērētajiem papildu privātuma un datu aizsardzību. Piemēram, 2015. gadā uzņēmums *Target* piekrita samaksāt 10 miljonus USD kā daļu no izlīguma ar patērētajiem, kuri bija iesnieguši prasību par to, ka viņu personiskā finanšu informācija ir tikusi kompromitēta plaša personas datu aizsardzības pārkāpuma rezultātā. 2013. gadā uzņēmums *AOL* piekrita samaksāt 5 miljonus USD kā izlīgumu, lai apmierinātu kolektīvu prasību par to, ka notikusi neatbilstīga anonimizācija, atklājot meklēšanas vaicājumus, kurus veikuši simtiem tūkstošu *AOL* dalībnieku. Arīdzan federālā tiesa apstiprināja uzņēmuma *Netflix* maksājumu 9 miljonu USD apmērā par to, kas tas glabājis nomas datu vēstures ierakstus, tādējādi pārkāpjot 1988. gada Video privātuma aizsardzības likumu (*Video Privacy Protection Act*). Federālās tiesas Kalifornijā apstiprināja divus atsevišķus izlīgumus ar *Facebook* – vienu par 20 miljoniem USD un otru par 9,5 miljoniem USD – saistībā ar to, kā uzņēmums vācis, izmantojis un lietojis savu lietotāju personisko informācijun. 2008. gadā Kalifornijas štata tiesa apstiprināja uzņēmuma *LensCrafters* izlīgumu par 20 miljoniem USD saistībā ar patērētāju medicīnas datu nelikumīgu izpaušanu.

Kopumā šis kopsavilkums raksturo to, ka Amerikas Savienotās Valstis nodrošina pietiekamu patērētāju privātuma un drošības aizsardzības līmeni. Jaunā privātuma vairoga shēma, kas nodrošina nozīmīgus aizsardzības pasākumus ES iedzīvotājiem, darbosies uz šā plašākā regulējuma fona, kurā patērētāju privātuma un drošības aizsardzība arī turpmāk būs svarīga prioritāte.

([1]) Skat., piemēram, *National Conference of State Legislatures* ("NCSL"), *State Security Breach Notification Laws* (2016. gada 4. janvāris), pieejami vietnē http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

([2]) *NCSL, Data Disposal Laws* (Jan. 12, 2016), pieejami vietnē http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

([3]) *Cal. Bus. & Professional Code §§ 22575-22579.*

([4]) *Cal. Civ. Code §§ 1798.80-1798.84.*

([5]) *Cal. Bus. & Professional Code § 22580-22582.*

([6]) Sk. *Jay Cline, U.S. Takes the Gold in Doling Out Privacy Fines, Computerworld* (2014. gada 17. februāris), pieejams vietnē http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1

V PIELIKUMS

Vēstule no ASV transporta ministra *Anthony Foxx*

2016. gada 19. februārī

Komisārei Verai Jourovai
Eiropas Komisija
Rue de la Loi/Wetstraat 200
1 049 l 049 Brisele
Beļģija

Par ES un ASV privātuma vairoga regulējumu

Cienījamā komisāres kundze!

Amerikas Savienoto Valstu Transporta ministrija ("ministrija" vai "TM") augstu vērtē iespēju aprakstīt savu lomu ES un ASV privātuma vairoga regulējuma izpildes panākšanā. Šis regulējums ievērojami veicina personas datu aizsardzību, ko nodrošina arvien savienotākā pasaulē veiktos komercdarījumos. Tas ļauj uzņēmumiem īstenot svarīgas darbības pasaules ekonomikā, vienlaikus nodrošinot, ka ES patērētāji nezaudē būtiskas privātuma aizsardzības garantijas.

TM pirmoreiz publiski pauda apņemšanos panākt "drošības zonas" regulējuma izpildi vēstulē, ko tā pirms 15 gadiem nosūtīja Eiropas Komisijai. TM šajā vēstulē solīja aktīvi veicināt "drošības zonas" privātuma principu izpildi. Ministrija šo apņemšanos joprojām ievēro, un tā tiek apstiprināta arī šajā vēstulē.

Konkrētāk, TM no jauna apstiprina savas saistības šādās galvenajās jomās: 1) apgalvojumu par privātuma vairoga pārkāpumiem prioritāra izmeklēšana; 2) atbilstošu izpildes panākšanas darbību īstenošana attiecībā uz struktūrām, kas izsaka nepatiesus vai maldinošus apgalvojumus par privātuma vairoga sertifikāciju; un 3) par privātuma vairoga pārkāpumiem pieņemto izpildes rīkojumu uzraudzība un publiskošana. Mēs sniedzam informāciju par katru saistību veidu un, lai ieskicētu kontekstu, attiecīgu pamatinformāciju par TM nozīmi patērētāju privātuma aizsardzībā un privātuma vairoga regulējuma izpildes panākšanā.

I. PAMATINFORMĀCIJa

A. **TM pilnvaras privātuma aizsardzības jomā**

Ministrija ir stingri apņēmusies nodrošināt tās informācijas privātumu, ko patērētāji sniedz aviosabiedrībām un biļešu pārdevējiem. TM pilnvaras rīkoties šajā jomā ir paredzētas U.S.C. 49. sadaļas 41712. iedaļā, kurā pārvadātājam vai biļešu pārdevējam ir aizliegts, pārdodot gaisa transporta pakalpojumus, iesaistīties "negodīgā vai maldinošā praksē vai negodīgā konkurences veidā", kas rada vai var radīt kaitējumu patērētājiem. 41712. iedaļa ir formulēta, pamatojoties uz Federālās tirdzniecības komisijas likuma (*Federal Trade Commission Act*) 5. pantu (*15 U.S.C. 45*). Saskaņā ar mūsu interpretāciju ASV likumā par negodīgu vai maldinošu praksi aviosabiedrībai vai biļešu pārdevējam ir aizliegts: 1) pārkāpt savas privātuma politikas noteikumus; vai 2) vākt vai izpaust privātu informāciju veidā, kas ir pretrunā sabiedriskajai politikai, ir amorāls vai rada būtisku kaitējumu patērētājam, ko nekompensē nekādas iegūtās priekšrocības. Atbilstīgi mūsu interpretācijai 41712. iedaļā pārvadātājiem un biļešu pārdevējiem ir aizliegts arī: l) pārkāpt ministrijas pieņemtos noteikumus, kuros konkrēta privātuma prakse atzīta par negodīgu vai maldinošu; vai 2) pārkāpt Likumu par bērnu privātās dzīves aizsardzību tiešsaistē (*Children's Online Privacy Protection Act – COPPA*) vai FTK pieņemtos *COPPA* īstenošanas noteikumus. Saskaņā ar federālajiem tiesību aktiem TM ir ekskluzīvas pilnvaras regulēt aviosabiedrību īstenoto privātuma aizsardzības praksi, un kopā ar FTK tai ir jurisdikcija attiecībā uz biļešu pārdevēju piemēroto privātuma praksi gaisa transporta pakalpojumu pārdošanas jomā.

Līdz ar to, tiklīdz pārvadātājs vai gaisa transporta pakalpojumu pārdevējs publiski apņemas ievērot privātuma vairoga regulējumā paredzētos privātuma principus, ministrija var izmantot savas likumiskās pilnvaras, kas izriet no 41712. iedaļas, lai nodrošinātu šo principu ievērošanu. Tāpēc, ja pasažieris ir sniedzis informāciju pārvadātājam vai biļešu pārdevējam, kas ir apņēmies ievērot privātuma vairoga regulējumā noteiktos privātuma principus, tos neievērojot, pārvadātājs vai biļešu pārdevējs pārkāptu 41712. iedaļu.

B. **Tiesībaizsardzības prakse**

Transporta ministrijas Birojs aviācijas tiesībaizsardzības un procesuālajos jautājumos ("Aviācijas tiesībaizsardzības birojs") izmeklē un uztur apsūdzību lietās saskaņā ar *49 U.S.C. 4171 2*. Tas panāk 41712. iedaļā paredzētā negodīgas un maldinošas prakses likumiskā aizlieguma izpildi, galvenokārt ar sarunām, pieņemot pretlikumīgas darbības pārtraukšanas rīkojumus, kā arī sagatavojot rīkojumus ar civilsodu izvērtējumu. Par iespējamiem pārkāpumiem birojs lielākoties uzzina no tam iesniegtajām indivīdu, ceļojumu aģentu, aviosabiedrību, kā arī ASV un ārvalstu valdības aģentūru sūdzībām. Patērētāji var iesniegt privātuma sūdzības par aviosabiedrībām un biļešu pārdevējiem, izmantojot TM tīmekļa vietni ([1]).

Ja lietā neizdodas panākt saprātīgu un atbilstošu risinājumu, Aviācijas tiesībaizsardzības birojam ir pilnvaras sākt izpildes procesu ar pierādījumu izskatīšanu, ko veic TM administratīvo tiesību tiesnesis (ATT). ATT ir pilnvarots pieņemt pretlikumīgas darbības pārtraukšanas rīkojumus un piespriest civilsodus. 41712. iedaļas pārkāpumu rezultātā var tikt pieņemti pretlikumīgas darbības pārtraukšanas rīkojumi un piemēroti civilsodi līdz 27 500 USD apmērā par katru šās iedaļas pārkāpumu.

Ministrijai nav pilnvaru pieņemt lēmumu par kaitējuma atlīdzināšanu vai finansiālu kompensāciju individuāliem sūdzību iesniedzējiem. Tomēr tā var apstiprināt izlīgumus, kas izriet no Aviācijas tiesībaizsardzības biroja ierosinātajām izmeklēšanām un tiek piedāvāti tieši patērētājiem (piemēram, nauda, kuponi), lai kompensētu naudas sodus, kurus citādi saņemtu ASV valdība. Tā ir darīts iepriekš un attiecīgos apstākļos tas būtu iespējams arī saistībā ar privātuma vairoga regulējuma principiem. Ja aviosabiedrība atkārtoti pārkāptu 41712. iedaļu, rastos jautājumi par tās spēju nodrošināt atbilstību, un līdz ar to ārkārtējās situācijās varētu atzīt, ka aviosabiedrība vairs nespēj darboties un tāpēc zaudē savas saimnieciskās darbības tiesības.

Līdz šim TM ir saņēmusi diezgan maz sūdzību par iespējamiem biļešu pārdevēju vai aviosabiedrību izdarītiem privātuma pārkāpumiem. Kad šādas sūdzības iesniedz, tās izmeklē saskaņā ar iepriekš izklāstītajiem principiem.

C. **TM īstenotie juridiskās aizsardzības pasākumi, ko var izmantot patērētāji no ES**

Saskaņā ar 41712. iedaļu aizliegums īstenot negodīgu vai maldinošu praksi gaisa pārvadājumu nozarē vai gaisa pārvadājumu pakalpojumu pārdošanas jomā attiecas gan uz ASV, gan ārvalstu gaisa pārvadātājiem un biļešu pārdevējiem. TM bieži vēršas pret ASV un citu valstu aviosabiedrībām saistībā ar praksi, kas ietekmē gan ārvalstu, gan ASV patērētājus, pamatojoties uz to, ka aviosabiedrība attiecīgo praksi īstenoja, kad nodrošināja pārvadājumus no Amerikas Savienotajām Valstīm vai uz tām. TM izmanto un turpinās izmantot visus pieejamos tiesiskās aizsardzības līdzekļus, lai aizsargātu ārvalstu un ASV patērētājus no negodīgas vai maldinošas prakses, ko gaisa pārvadājumu nozarē īsteno regulētas struktūras.

TM arīdzan gādā, lai aviosabiedrības ievērotu arī citus mērķvirzītus tiesību aktus, kuros paredzētā aizsardzība attiecas arīdzan uz patērētājiem no citām valstīm, piemēram, *COPPA*. *COPPA* cita starpā ir noteikts, ka uz bērniem vērstu tīmekļa vietņu un tiešsaistes pakalpojumu vai vispārīgai auditorijai paredzētu vietņu operatoriem, kuri apzināti vāc personisku informāciju no bērniem, kas nav sasnieguši 13 gadu vecumu, par to jāinformē vecāki un jāsaņem no viņiem pierādāma piekrišana. ASV bāzētām tīmekļa vietnēm un pakalpojumiem, kam piemēro *COPPA* un kas vāc personisku informāciju no ārvalstu bērniem, ir jāatbilst *COPPA* prasībām. Tam ir jāatbilst arī ārvalstīs bāzētām vietnēm un tiešsaistes pakalpojumiem, ja tie ir vērsti uz bērniem Amerikas Savienotajās Valstīs vai ar tiem apzināti vāc personisko informāciju no bērniem, kuri dzīvo Amerikas Savienotajās Valstīs. TM ir pilnvarota veikt izpildes panākšanas darbības attiecībā uz *COPPA* pārkāpumiem, ko izdarījušas ASV vai ārvalstu aviosabiedrības, kuras veic uzņēmējdarbību Amerikas Savienotajās Valstīs.

II. PRIVĀTUMA VAIROGA IZPILDES PANĀKŠANA

Ja aviosabiedrība vai biļešu pārdevējs ir nolēmis piedalīties privātuma vairoga regulējuma īstenošanā un ministrija saņem sūdzību, kurā apgalvots, ka attiecīgā aviosabiedrība vai biļešu pārdevējs ir pārkāpis regulējumu, TM, lai panāktu regulējuma ievērošanu, veiks turpmāk uzskaitītās darbības. A.

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

A. **Iespējamo pārkāpumu prioritāra izmeklēšana**

TM Aviācijas tiesībaizsardzības birojs izmeklēs katru sūdzību par iespējamiem privātuma vairoga pārkāpumiem (arī sūdzības no ES datu aizsardzības iestādēm) un, ja konstatēs pārkāpumu pierādījumus, veiks izpildes panākšanas darbības. Aviācijas tiesībaizsardzības birojs arī sadarbosies ar FTK un Tirdzniecības ministriju un prioritārā kārtībā izskatīs apgalvojumus par regulētām struktūrām, kuras neievēro privātuma saistības, ko uzņēmušās saistībā ar privātuma vairoga regulējumu.

Saņemot apgalvojumu par privātuma vairoga regulējuma pārkāpumu, Aviācijas tiesībaizsardzības birojs var īstenot dažādas ar izmeklēšanu saistītas darbības. Piemēram, tas var pārskatīt biļešu pārdevēja vai aviosabiedrības privātuma politiku, iegūt papildu informāciju no biļešu pārdevēja, aviosabiedrības vai trešajām personām, sniegt sūdzības iesniedzējai struktūrai jaunāko informāciju, kā arī izvērtēt, vai pastāv pārkāpumu pazīmes un vai ir ietekmēts liels patērētāju skaits. birojs noteiktu, vai sūdzībā skartie jautājumi nav Tirdzniecības ministrijas vai FTK kompetencē, novērtētu, vai noderētu patērētāju un uzņēmumu izglītošana, un, attiecīgā gadījumā, sāktu izpildes procesu.

Ja ministrija uzzinās par iespējamu privātuma vairoga pārkāpumu, ko, izdarījuši biļešu pārdevēji, tā saskaņos rīcību ar FTK. Mēs arī informēsim FTK un Tirdzniecības ministriju par visu privātuma vairoga izpildes panākšanas darbību iznākumu.

B. **Reaģēšana uz nepatiesiem vai maldinošiem apgalvojumiem par dalību programmā**

Ministrija joprojām ir apņēmusies izmeklēt privātuma vairoga pārkāpumus, tostarp nepatiesus vai maldinošus apgalvojumus par dalību privātuma vairoga programmā. Mēs prioritāri izskatīsim Tirdzniecības ministrijas pieprasījumus par organizācijām, kas, kā uzskata ministrija, nepamatoti uzdodas par pašreizējām privātuma vairoga programmas dalībniecēm vai bez atļaujas izmanto privātuma vairoga regulējuma sertifikācijas zīmi.

Turklāt jānorāda, ka, ja organizācijas privātuma politikā ir apgalvots, ka tā ievēro privātuma vairoga pamatprincipus, tomēr nav reģistrējusies vai saglabājusi reģistrāciju Tirdzniecības ministrijā, šis fakts vien, visticamāk, neatbrīvos organizāciju no TM centieniem panākt attiecīgo saistību izpildi. C.

C. **Par privātuma vairoga pārkapumiem pieņemto izpildes rīkojumu uzraudzība un publiskošana**

Lai nodrošinātu privātuma vairoga programmas ievērošanu, TM Aviācijas tiesībaizsardzības birojs joprojām ir apņēmies, ja nepieciešams, uzraudzīt izpildes rīkojumu īstenošanu. Konkrētāk, ja birojs pieņems rīkojumu, kurā aviosabiedrībai vai biļešu pārdevējam likts pārtraukt pretlikumīgu darbību un nepieļaut turpmākus privātuma vairoga un 41712. iedaļas pārkāpumus, tas uzraudzīs, vai struktūra ievēro rīkojuma noteikumu par pretlikumīgās darbības pārtraukšanu. Birojs arīdzan nodrošinās par privātuma vairoga lietām pieņemto rīkojumu pieejamību tā tīmekļa vietnē.

Mēs labprāt turpināsim sadarboties ar mūsu federālajiem partneriem un ES ieinteresētajām personām ar privātuma vairogu saistītu jautājumu risināšanā.

Es ceru, ka šī informācija būs noderīga. Ja Jums ir kādi jautājumi vai ir vajadzīga papildu informācija, lūdzu nekavējieties ar mani sazināties.

Ar cieņu

transporta ministrs

Anthony R. Foxx

VI PIELIKUMS

Vēstule no Nacionālās izlūkošanas direktora biroja galvenā juriskonsulta *Robert Litt*

2016. gada 22. februārī

Juriskonsultam
Justin S. Antonipillai
ASV Tirdzniecības ministrija
1401 Constitution Ave., NW
Washington, DC 20230

Ministra vietniekam
Ted Dean
Starptautiskās tirdzniecības administrācija
1401 Constitution Ave., NW
Washington, DC 20230

Godātais *Antonipillai* kungs un godātais *Dean* kungs!

Pēdējo divarpus gadu laikā saistībā ar sarunām par ES un ASV privātuma vairogu Amerikas Savienotās Valstis ir sniegušas būtisku informāciju par ASV izlūkdienesta veikto sakaru izlūkošanas darbību norisi. Tas ietver informāciju par piemērojamo tiesisko regulējumu, šo darbību daudzslāņaino pārraudzību, to plašo pārredzamību, kā arī vispārējiem privātuma un pilsonisko brīvību aizsardzības pasākumiem, lai palīdzētu Eiropas Komisijai noteikt, vai šie aizsardzības pasākumi ir pietiekami, jo tie ir saistīti ar izņēmumu, ko uz privātuma vairoga principiem attiecina valsts drošības apsvērumu dēļ. Sniegtā informācija ir rezumēta šajā dokumentā.

I. PPD-28 UN ASV SAKARU IZLŪKOŠANAS DARBĪBU VEIKŠANA

ASV izlūkdienests vāc ārējās izlūkošanas informāciju rūpīgi un kontrolēti, stingri ievērojot ASV tiesību aktus, īstenojot vairākus pārraudzības līmeņus un uzsvaru liekot uz būtiskām ārējās izlūkošanas un valsts drošības prioritātēm. ASV īstenoto sakaru izlūkošanas informācijas vākšanu reglamentē plašs tiesību aktu un politikas virzienu klāsts, tostarp ASV Konstitūcija, Ārējās izlūkošanas un novērošanas likums (*Foreign Intelligence Surveillance Act – FISA, 50 U.S.C. § 1801* un turpm. sadaļas), Izpildrīkojums Nr. 12333 (*E.O. 12333*) un tā īstenošanas procedūras, prezidenta norādes, kā arī daudzas *FISA* tiesas un ģenerālprokurora apstiprinātas procedūras un pamatnostādnes, kurās ir paredzēti papildu noteikumi, ar ko ierobežo ārējās izlūkošanas informācijas vākšanu, glabāšanu, izmantošanu un izplatīšanu ([1]).

a. **Pārskats par PPD-28**

ASV prezidents B. Obama 2014. gada janvārī teica runu, kurā ieskicēja dažādas ASV sakaru izlūkošanas darbību reformas, un pieņēma Prezidenta politikas direktīvu Nr. 28 (PPD-28), kas attiecas uz minētajām darbībām ([2]). Prezidents uzsvēra, ka ASV sakaru izlūkošanas darbības palīdz gādāt ne tikai par mūsu valsts drošību un mūsu brīvībām, bet arī par drošību un brīvībām citās valstīs, tostarp ES dalībvalstīs, kuras izmanto ASV izlūkaģentūru iegūto informāciju savu pilsoņu aizsardzībai.

PPD-28 ir noteikts principu un prasību kopums, kas attiecas uz visām ASV īstenotajām sakaru izlūkošanas darbībām un visiem indivīdiem neatkarīgi no to valstspiederības un atrašanās vietas. Konkrētāk, tajā ir noteiktas prasības, ko piemēro ASV veiktās sakaru izlūkošanas gaitā iegūtās citu valstu iedzīvotāju personiskās informācijas vākšanas, glabāšanas un izplatīšanas procedūrām. Šīs prasības ir sīkāk izklāstītas turpmāk, taču tās var rezumēt šādi:

— PPD tiek atkārtots, ka Amerikas Savienotās Valstis vāc sakaru izlūkdatus vienīgi tā, kā atļauts likumā, izpildrīkojumā vai citā prezidenta direktīvā.

([1]) Papildu informācija par ASV ārējās izlūkošanas darbībām ir publicēta tiešsaistē un publiski pieejama portālā *IC on the Record* (www.icontherecord.tumblr.com) – NIDB publiskajā tīmekļa vietnē, kuras mērķis ir veicināt lielāku sabiedrības informētību par valdības izlūkdarbībām.

([2]) Pieejama vietnē https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

— PPD ir noteiktas procedūras, ar ko nodrošināt, ka sakaru izlūkošanas darbības veic tikai tādēļ, lai sekmētu likumīgu un pilnvarotu mērķu īstenošanu valsts drošības jomā.

— Turklāt saskaņā ar PPD, plānojot sakaru izlūkdatus vākšanu, noteikti jānodrošina privātuma un pilsonisko brīvību ievērošana. Konkrētāk, Amerikas Savienotās Valstis nevāc izlūkošanas informāciju, lai apspiestu vai ierobežotu kritikas vai atšķirīga viedokļa paušanu, radītu indivīdiem neizdevīgu situāciju to etniskās izcelsmes, rases, dzimuma, seksuālās orientācijas vai reliģiskās pārliecības dēļ vai piešķirtu ASV uzņēmumiem un ASV uzņēmējdarbības nozarēm komerciālās konkurences priekšrocības.

— PPD ir noteikts, ka sakaru izlūkdati jāvāc pēc iespējas pielāgoti un ka lielapjomā savāktos sakaru izlūkdatus var izmantot tikai konkrētos un uzskaitītos nolūkos.

— PPD ir norādīts, ka izlūkdienests pieņem tādas procedūras, kas ir "pamatoti izstrādātas, lai līdz minimumam samazinātu sakaru izlūkošanas darbībās savāktās personiskās informācijas izplatīšanu un paturēšanu," un jo īpaši attiecinātu konkrētu ASV iedzīvotāju personiskajai informācijai piešķirtu aizsardzību arī uz citu valstu iedzīvotāju personisko informāciju.

— Aģentūru procedūras, ar ko īsteno PPD-28, ir pieņemtas un publiskotas.

Tajā noteikto procedūru un aizsardzības pasākumu attiecināmība uz privātuma vairogu ir skaidra. Ja dati Amerikas Savienoto Valstu uzņēmumiem ir pārsūtīti saskaņā ar privātuma vairogu vai citiem līdzekļiem, ASV izlūkaģentūras var uzņēmumiem tos prasīt vienīgi tad, ja pieprasījums atbilst *FISA* vai tiek izteikts saskaņā ar kādu no turpmāk aprakstītajiem likumiskajiem noteikumiem par vēstuli par valsts drošību ([1]). Turklāt, neapstiprinot un nenoliedzot plašsaziņas līdzekļu ziņas, kurās apgalvots, ka ASV izlūkdienests vāc datus no transatlantiskajiem kabeļiem, kamēr tos pārsūta uz Amerikas Savienotajām Valstīm, ja ASV izlūkdienests vāktu datus no transatlantiskajiem kabeļiem, tas to darītu, ievērojot noteiktos ierobežojumus un aizsardzības pasākumus, tostarp PPD-28 prasības.

b. **Informācijas vākšanas ierobežojumi**

PPD-28 ir noteikti vairāki būtiski vispārīgie principi, kas attiecas uz sakaru izlūkdatu vākšanu:

— sakaru izlūkdatu vākšanai jābūt atļautai ar likumu vai prezidenta atļauju, un tā jāveic atbilstīgi Konstitūcijai un tiesību aktiem,

— plānojot sakaru izlūkošanas darbības, noteikti jāņem vērā privātums un pilsoniskās brīvības,

— sakaru izlūkdatus drīkst vākt tikai tad, ja pastāv pamatots ārējās izlūkošanas vai pretizlūkošanas mērķis,

— Amerikas Savienotās Valstis nevāks sakaru izlūkdatus nolūkā apspiest vai ierobežot kritikas vai atšķirīga viedokļa paušanu,

— Amerikas Savienotās Valstis nevāks sakaru izlūkdatus, lai radītu indivīdiem neizdevīgu situāciju to etniskās izcelsmes, rases, dzimuma, seksuālās orientācijas vai reliģiskās pārliecības dēļ,

— Amerikas Savienotās Valstis nevāks sakaru izlūkdatus, lai piešķirtu komerciālu konkurences priekšrocību ASV uzņēmumiem un uzņēmējdarbības nozarēm,

— ASV sakaru izlūkošanas darbībai vienmēr jābūt pēc iespējas pielāgotai, ņemot vērā citu informācijas avotu pieejamību. Tas cita starpā nozīmē, ka sakaru izlūkdatu vākšanu, kad vien iespējams, veic mērķtiecīgi, nevis lielapjomā.

Prasība, ka sakaru izlūkošanas darbībai jābūt "pēc iespējas pielāgotai", attiecas uz sakaru izlūkdatu vākšanas veidu, kā arī faktiski savāktajiem datiem. Piemēram, nosakot, vai vākt sakaru izlūkdatus, izlūkdienestam jāņem vērā citas informācijas,

([1]) Tiesībaizsardzības vai regulatīvās aģentūras var pieprasīt uzņēmumiem informāciju Amerikas Savienotajās Valstīs veiktas izmeklēšanas vajadzībām saskaņā ar citām civiltiesiskām, krimināltiesiskām un regulatīvām pilnvarām, uz kurām šis dokuments, kurā aprakstītas tikai ar valsts drošību saistītas pilnvaras, neattiecas.

arī diplomātiskās vai publisko avotu, pieejamība un par prioritāti, ja iespējams un vajadzīgs, jāuzskata datu vākšana ar šiem līdzekļiem. Turklāt izlūkdienesta struktūrvienību politikā būtu jāparedz prasība, ka, ja vien tas ir izpildāms praksē, informācijas vākšanā uzsvars būtu jāliek uz konkrētiem ārējās izlūkošanas subjektiem vai tematiem, izmantojot diskriminantus (piemēram, konkrētus resursus, atlases vārdus un identifikatorus).

Ir būtiski uzlūkot Komisijai sniegto informāciju kopumā. To, kas ir "iespējams" vai "izpildāms" neizlemj indivīdi, šādus lēmumus pieņem atbilstīgi politikai, ko aģentūras pieņēmušas saskaņā ar PPD-28 – un kas ir publiskota –, un citiem tajā aprakstītiem procesiem ([1]). Kā noteikts PPD-28, lielapjomā savākti sakaru izlūkdati ir informācijas kopums, kas "tehnisku vai operatīvu apsvērumu dēļ ir iegūts, neizmantojot diskriminantus (piemēram, konkrētus identifikatorus, atlases vārdus u. c.)." Saistībā ar to PPD-28 ir atzīts, ka izlūkdienesta struktūrvienības var lielapjomā vākt sakaru izlūkdatus konkrētos apstākļos, lai noteiktu jaunus vai topošos apdraudējumus un citu būtisku informāciju par valsts drošību, kas nereti ir apslēpta plašajā un komplicētajā mūsdienu globālo sakaru sistēmā. Direktīvā ir atzītas arī bažas par privātuma un pilsonisko brīvību ievērošanu, kas paustas saistībā ar sakaru izlūkdatu lielapjoma vākšanu. Tāpēc saskaņā ar PPD-28 izlūkdienestam par prioritāti jāuzskata nevis sakaru izlūkdatu lielapjoma vākšana, bet gan alternatīvas, kas ļautu veikt mērķtiecīgu sakaru izlūkošanu. Līdz ar to izlūkdienesta struktūrvienībām, kad vien praksē iespējams, sakaru izlūkošanas darbības būtu jāveic mērķtiecīgi, nevis lielapjomā. ([2]) Šie principi nodrošina, ka uz datu lielapjoma vākšanu attiecināmais izņēmums nepārmāc vispārīgo noteikumu.

Viens no ASV tiesību aktu pamatprincipiem ir jēdziens "samērīgums". Tas norāda, ka izlūkdienesta struktūrvienībām būs nevis jāpieņem jebkurš teorētiski iespējamais pasākums, bet gan jālīdzsvaro to centieni ievērot likumīgās ar privātumu un pilsoniskajām brīvībām saistītās intereses un praktiskās vajadzības, kas izriet no sakaru izlūkošanas darbībām. Ir publiskota arī aģentūru politika attiecībā uz šo principu, tādējādi ir garantēts, ka jēdziens "pamatoti izstrādātas, lai līdz minimumam samazinātu personiskās informācijas izplatīšanu un paturēšanu" neierobežos vispārīgā noteikuma piemērošanu.

PPD-28 arīdzan ir noteikts, ka lielapjomā savāktos sakaru izlūkdatus var izmantot vienīgi sešiem konkrētiem mērķiem, proti, lai konstatētu konkrētas ārējas varas darbības un pret tām vērstos; apkarotu terorismu; apkarotu izplatīšanu; nodrošinātu kiberdrošību; konstatētu un vērstos pret apdraudējumiem ASV vai sabiedroto bruņotajiem spēkiem; apkarotu transnacionālus kriminālapdraudējumus, ieskaitot izvairīšanos no sankcijām. Prezidenta padomdevējs valsts drošības jautājumos, konsultējoties ar nacionālās izlūkošanas direktoru (NID), reizi gadā pārskatīs atļautos lielapjomā savākto sakaru izlūkdatu izmantojumus, lai noskaidrotu, vai tie būtu jāmaina. NID publiskos šo uzskaitījumu pēc iespējas lielākā apmērā un ievērojot valsts drošības apsvērumus. Tas ir būtisks un pārredzams sakaru izlūkdatu lielapjoma vākšanas ierobežojums.

Papildus tam jānorāda, ka izlūkdienesta struktūrvienības, kas īsteno PPD-28, ir nostiprinājušas līdzšinējo analītisko praksi un standartus attiecībā uz jautājumiem par nenovērtētiem sakaru izlūkdatiem ([3]). Analītiķiem jāstrukturē jautājumi vai citi meklējamie vārdi un metodes tā, lai ar tiem pienācīgi konstatētu izlūkošanas informāciju, kas ir saistīta ar likumīgu ārējās izlūkošanas vai tiesībaizsardzības uzdevumu. Šajā nolūkā, lai novērstu ar ārējo izlūkošanu vai tiesībaizsardzību saistītajām prasībām neatbilstīgas personiskās informācijas izmantošanu, ID struktūrvienībām vaicājumos par personām uzsvars jāliek uz tādām sakaru izlūkdatu kategorijām, kas ir ar šīm prasībām saistītas.

Jāuzsver, ka visas ar interneta sakariem saistītās informācijas lielapjoma vākšanas darbības, ko ASV izlūkdienests veic, īstenojot sakaru izlūkošanu, notiek nelielā interneta daļā. Turklāt, izmantojot mērķtiecīgus vaicājumus, kā aprakstīts iepriekš, tiek nodrošināts, ka analītiķi saņem izskatīšanai tikai tādus informācijas vienumus, kam varētu būt izlūkošanas vērtība. Šo ierobežojumu mērķis ir aizsargāt visu personu privātumu un pilsoniskās brīvības neatkarīgi no to valstspiederības un dzīvesvietas.

([1]) Pieejama vietnē www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Ar šīm procedūrām katrai ID struktūrvienībai piemērotā veidā tiek īstenoti šajā vēstulē aprakstītie mērķatlases un pielāgošanas principi.

([2]) Viens no piemēriem: atbilstīgi NDA procedūrām, ar ko īsteno PPD-28, "[k]ad vien tas ir izpildāms praksē, informāciju vāc, izmantojot vienu vai vairākus atlases vārdus, lai galvenokārt vāktu datus par konkrētiem ārējās izlūkošanas subjektiem (piemēram, konkrētu, zināmu starptautiska līmeņa teroristu vai teroristu grupējumu) vai konkrētām ārējās izlūkošanas jomām (piemēram, masu iznīcināšanas ieroču izplatīšanu, ko veic citas varas vai to pārstāvji)."

([3]) Pieejami vietnē http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf

Amerikas Savienotās Valstis ir izstrādājušas procesus, ar ko nodrošināt, ka sakaru izlūkošanas darbības īsteno tikai tādēļ, lai veicinātu atbilstošu valsts drošības mērķu izpildi. Valsts prezidents katru gadu pēc plaša un oficiāla starpaģentūru procesa nosaka valsts galvenās prioritātes ārējās izlūkošanas informācijas vākšanas jomā. NID pienākums ir šīs izlūkošanas prioritātes iestrādāt valsts izlūkošanas prioritāšu satvarā jeb VIPS. Ar PPD-28 starpaģentūru process tika nostiprināts un uzlabots, lai nodrošinātu, ka visas ID izlūkošanas prioritātes pārskata un apstiprina augsta līmeņa politikas veidotāji. Izlūkdienesta direktīvā (IDD) Nr. 204 ir paredzētas papildu norādes par VIPS, un 2015. gada janvārī tā tika atjaunināta, lai iestrādātu PPD-28 prasības ([1]). Lai gan VIPS saturs ir klasificēts, ar konkrētām ASV ārējās izlūkošanas prioritātēm saistīto informāciju ik gadu atspoguļo NID neklasificētajā Pasaules apdraudējumu novērtējumā, kas ir pieejams arī NIDB tīmekļa vietnē.

VIPS noteiktās prioritātes ir diezgan vispārīgas. Starp tematiem ir, piemēram, ārējo pretinieku centieni palielināt kodolieroču un ballistisko raķešu spējas, narkotiku tirgotāju karteļu radītās korupcijas sekas un cilvēktiesību pārkāpumi konkrētās valstīs. Turklāt tās attiecas uz visām izlūkošanas darbībām, ne tikai sakaru izlūkošanu. Organizācija, kurai VIPS uzskaitītās prioritātes jāpārveido reālā sakaru izlūkdatu vākšanā, ir Nacionālā Sakaru izlūkošanas komiteja jeb *SIGCOM*. Tā darbojas Nacionālās drošības aģentūras (NDA) direktora aizbildnībā, un viņš atbilstīgi Izpildrīkojumam Nr. 12333 ir iecelts par "sakaru izlūkošanas funkcionālo valdītāju," kura pienākums ir pārraudzīt un koordinēt sakaru izlūkošanu, ko izlūkdienestā veic gan aizsardzības ministra, gan NID pārraudzībā. *SIGCOM* darbojas visu ID struktūrvienību pārstāvji un līdz ar pilnīgu PPD-28 īstenošanu Amerikas Savienotajās Valstīs tajā būs pilnīgi pārstāvētas arī citas sakaru izlūkošanā politiski ieinteresētās ministrijas un aģentūras.

Visas ASV ministrijas un aģentūras, kas ir ārējās izlūkošanas "patērētāji", savus informācijas pieprasījumus iesniedz *SIGCOM*. *SIGCOM* tos izskata, pārliecinās par to atbilstību VIPS un nosaka to prioritāti, ņemot vērā, piemēram, turpmāk uzskaitītos kritērijus.

— Vai konkrētajā gadījumā sakaru izlūkošana var nodrošināt noderīgu informāciju vai arī šo prasību var izpildīt ar labākiem vai rentablākiem informācijas avotiem, piemēram, attēliem vai publiskos avotos pieejamu informāciju?

— Cik nepieciešama ir attiecīgā informācija? Ja dati ir saistīti ar augstu VIPS prioritāti, attiecīgā sakaru izlūkošanas prioritāte, visticamāk, būs augsta.

— Kādu sakaru izlūkošanas veidu varētu izmantot?

— Vai informācijas vākšana ir pēc iespējas pielāgota? Vai būtu jānosaka laika, ģeogrāfiskie vai citi ierobežojumi?

Ar ASV sakaru izlūkošanas prasībām saistītajā procesā arī skaidri jāņem vērā citi faktori, proti:

— Vai vācamās informācijas vai izmantotās vākšanas metodikas subjekts ir sevišķi sensitīvs? Ja tā, pieprasījums būs jāizskata augstāka līmeņa politikas veidotājiem.

— Vai datu vākšana nepamatoti apdraudēs personu privātumu un pilsoniskās brīvības neatkarīgi no valstspiederības?

— Vai privātuma vai valsts drošības interešu aizsardzības nolūkā ir jāīsteno ar informācijas izplatīšanu un glabāšanu saistīti papildu aizsardzības pasākumi?

Visbeidzot, procesa beigās apmācīti NDA darbinieki, ņemot vērā *SIGCOM* apstiprinātās prioritātes, izpēta un nosaka konkrētus atlases vārdus, piemēram, tālruņa numurus vai e-pasta adreses, ar ko varētu savākt šīm prioritātēm atbilstošus ārējās izlūkošanas rezultātus. Ikviens atlasītājs pirms ievadīšanas NDA informācijas vākšanas sistēmās ir jāpārskata un jāapstiprina. Tomēr arī tad tas, vai un kad notiks informācijas faktiskā vākšana, daļēji ir atkarīgs no papildu

([1]) Pieejamas vietnē http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf

apsvērumiem, piemēram, atbilstošu informācijas vākšanas resursu pieejamības. Ar šo procesu nodrošina, ka ASV sakaru izlūkdati tiek vākti tādēļ, lai īstenotu pamatotas un svarīgas ārējās izlūkošanas vajadzības. Protams, ja informāciju vāc atbilstīgi *FISA*, NDA un pārējām aģentūrām jāievēro papildu ierobežojumi, ko ir apstiprinājusi Ārējās izlūkošanas un novērošanas tiesa. Īsi sakot, nedz NDA, ne kāda cita ASV izlūkaģentūra pati nenolemj, kādu informāciju vākt.

Kopumā ar šo procesu nodrošina, ka visas ASV izlūkošanas prioritātes nosaka augstākā līmeņa politikas veidotāji, kas vislabāk var noteikt ASV ārējās izlūkošanas prasības, un ka viņi ņem vērā ne tikai vācamās informācijas potenciālo vērtību, bet arī ar vākšanu saistītos riskus, tostarp privātuma, valsts ekonomikas interešu un ārējo attiecību apdraudējumus.

Attiecībā uz datiem, ko Amerikas Savienotajām Valstīm pārsūta saskaņā ar privātuma vairogu, jānorāda, ka, lai gan ASV nevar ne apstiprināt, ne noliegt konkrētas izlūkošanas metodes vai darbības, PPD-28 prasības attiecas uz visām to veiktajām sakaru izlūkošanas darbībām neatkarīgi no vākto datu avota veida. Turklāt sakaru izlūkdatu vākšanai piemērojamie ierobežojumi un aizsardzības pasākumi attiecas uz jebkādā apstiprinātā nolūkā, tostarp gan ar ārējām attiecībām, gan ar valsts drošību saistītos nolūkos, vāktiem sakaru izlūkdatiem.

Iepriekš aprakstītās procedūras liecina par nepārprotamu apņemšanos novērst patvaļīgu un nekritisku sakaru izlūkdatu vākšanu, kā arī īstenot – sākot no ASV valdības augstākajiem līmeņiem – samērīguma principu. PPD-28 un aģentūru īstenošanas procedūrās ir precizēti jaunie un pastāvošie ierobežojumi, kā arī konkrētāk aprakstīts iemesls, kāpēc Amerikas Savienotās Valstis vāc un izmanto sakaru izlūkdatus. Šiem instrumentiem būtu jārada pārliecība, ka ASV veic un arī turpmāk veiks sakaru izlūkošanas darbības tikai likumīgu ārējās izlūkošanas mērķu īstenošanas nolūkā.

c. **Glabāšanas un izplatīšanas ierobežojumi**

PPD-28 4. pantā ir noteikts, ka ikvienai izlūkdienesta struktūrvienībai attiecībā uz personisko informāciju par citu valstu iedzīvotājiem, kas iegūta ar sakaru izlūkošanas darbībām, jāievēro skaidri glabāšanas un izplatīšanas ierobežojumi, kas ir pielīdzināmi ar ASV iedzīvotājiem saistītajiem ierobežojumiem. Šie noteikumi ir iekļauti katras ID aģentūras procedūrās, kas tika laistas klajā 2015. gada februārī un ir publiski pieejamas. Lai personisko informāciju varētu glabāt vai izplatīt kā ārējo izlūkošanas informāciju, tai jābūt saistītai ar iepriekš aprakstītajā VIPS procesā noteiktu apstiprinātu izlūkošanas prasību; ir jābūt pamatotam uzskatam, ka tā ir nozieguma pierādījums; vai tai jāatbilst kādam no pārējiem standartiem par ASV iedzīvotāju personiskās informācijas glabāšanu, kas noteikti Izpildrīkojuma Nr. 12333 2.3. sadaļā.

Informāciju, kas neatbilst kādam no šiem nosacījumiem, nevar glabāt ilgāk par pieciem gadiem, ja vien NID skaidri nenosaka, ka tās turpmāka glabāšana ir Amerikas Savienoto Valstu drošības interesēs. Līdz ar to ID struktūrvienībām ir jādzēš ar sakaru izlūkošanas darbībām savāktā citu valstu iedzīvotāju personiskā informācija, kad no tās savākšanas ir pagājuši pieci gadi, izņemot gadījumu, kad, piemēram, ir noteikts, ka informācija ir vajadzīga apstiprinātas ārējās izlūkošanas prasības izpildei, vai NID, ņemot vērā NIDB pilsonisko brīvību aizsardzības amatpersonas un aģentūras privātuma un pilsonisko brīvību amatpersonu viedokli, ir noteicis, ka turpmāka glabāšana ir valsts drošības interesēs.

Papildus tam ikvienas aģentūras politikā, ar ko īsteno PPD-28, patlaban ir skaidri noteikts, ka informāciju par personu nedrīkst izplatīt, pamatojoties vienīgi uz to, ka indivīds nav ASV iedzīvotājs, un NIDB ir pieņēmis direktīvu, kura, lai atspoguļotu šo prasību, attiecas uz visām ID struktūrvienībām ([1]). Izlūkdienesta darbiniekiem ir skaidri formulēts pienākums izlūkošanas ziņojumu izstrādē un izplatīšanā ņemt vērā citu valstu iedzīvotāju privātumu. Konkrētāk, informāciju, kas ar sakaru izlūkošanas darbībām iegūta par citas valsts iedzīvotāja ikdienas darbībām, neuzskatītu par ārējās izlūkošanas informāciju, ko varētu pastāvīgi izplatīt vai glabāt, pamatojoties uz šo faktu vien, ja tā nav citādi saistīta ar apstiprinātu ārējās izlūkošanas prasību. Ar to tiek atzīts būtisks ierobežojums un reaģēts uz Eiropas Komisijas bažām par Izpildrīkojumā Nr. 12333 noteiktās ārējās izlūkošanas definīcijas tvērumu.

([1]) *Intelligence Community Directive* (ICD) 203, pieejama vietnē http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf

d. **Atbilstība un pārraudzība**

No ASV ārējās izlūkošanas pārraudzības sistēmas izriet stingra un daudzslāņaina pārraudzība, ar ko nodrošina atbilstību piemērojamiem tiesību aktiem un procedūrām, tostarp saistībā ar tādas citu valstu iedzīvotāju personiskās informācijas vākšanu, glabāšanu un izplatīšanu, kas iegūta ar PPD-28 noteiktajām sakaru izlūkošanas darbībām. Piemēram:

— Izlūkdienests nodarbina vairākus simtus pārraudzības darbinieku. NDA vien ir vairāk nekā 300 darbinieku, kuru darbs ir saistīts ar atbilstību, un arī citām struktūrvienībām ir pārraudzības biroji. Plašu izlūkošanas darbību pārraudzību nodrošina Tieslietu ministrija; pārraudzību veic arīdzan Aizsardzības ministrija.

— Katrai izlūkdienesta struktūrvienībai ir savs ģenerālinspektora birojs, kura pienākums inter alia ir ārējās izlūkošanas darbību pārraudzība. Ģenerālinspektori ir likumiski neatkarīgi, tiem ir plašas pilnvaras izmeklēt, revidēt un pārbaudīt programmas, tostarp attiecībā uz krāpšanu un tiesību aktu ļaunprātīgu izmantošanu vai pārkāpšanu, un viņi var ieteikt korektīvas darbības. Lai arī ģenerālinspektora ieteikumi nav saistoši, tā ziņojumus nereti publisko un vienmēr nodod Kongresam; tas attiecas arī uz turpmākas uzraudzības ziņojumiem, ko sagatavo, ja vēl nav izpildītas iepriekšējos ziņojumos ieteiktās korektīvās darbības. Tādējādi Kongress ir informēts par visiem neatbilstības gadījumiem un var izdarīt spiedienu, tostarp ar budžeta līdzekļiem, lai panāktu korektīvās darbības īstenošanu. Ir publiskoti vairāki ģenerālinspektoru ziņojumi par izlūkošanas programmām ([1]).

— NIDB Pilsonisko brīvību un privātuma aizsardzības biroja (PBPAB) pienākums ir nodrošināt, lai ID darbības veids veicinātu valsts drošību un vienlaikus aizsargātu indivīdu pilsoniskās brīvības un tiesības uz privātumu. ([2]) Citām ID struktūrvienībām ir savas privātuma aizsardzības amatpersonas.

— Privātuma un pilsonisko brīvību pārraudzības padomei (PPBPP) – neatkarīgai un ar likumu izveidotai struktūrai – ir jāanalizē un jāizskata terorisma apkarošanas programmas un politika, tostarp sakaru izlūkošanas izmantošana, lai nodrošinātu, ka tās pienācīgi aizsargā privātumu un pilsoniskās brīvības. Tā ir pieņēmusi vairākus publiskus ziņojumus par izlūkošanas darbībām.

— Kā sīkāk aprakstīts turpmāk, par visu saskaņā ar *FISA* veikto sakaru izlūkdatu vākšanas darbību pārraudzību un atbilstību atbild Ārējās izlūkošanas un novērošanas tiesa, ko veido neatkarīgi federālie tiesneši.

— Visbeidzot, ASV Kongresam, jo īpaši Pārstāvju palātas un Senāta izlūkošanas un tieslietu komitejām, ir būtiski pārraudzības pienākumi attiecībā uz visām ASV ārējās izlūkošanas darbībām, tostarp ASV īstenoto sakaru izlūkošanu.

Papildus šiem oficiālajiem pārraudzības mehānismiem izlūkdienests īsteno daudzus mehānismus, ar kuriem nodrošina, ka ID ievēro iepriekš aprakstītos informācijas vākšanas ierobežojumus. Piemēram:

— Ministru kabineta amatpersonām katru gadu ir jāapstiprina to sakaru izlūkošanas prasības.

— NDA visa vākšanas procesa gaitā pārbauda sakaru izlūkošanas subjektus, lai noteiktu, vai tie patiešām sniedz vērtīgu un prioritātēm atbilstošu ārējās izlūkošanas informāciju, un pārtrauks šiem kritērijiem neatbilstošas informācijas vākšanu. Ar papildu procedūrām tiek nodrošināta periodiska atlases vārdu pārskatīšana.

([1]) Sk., piemēram, *U.S. Department of Justice Inspector General Report A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008* (2012. gada septembris), pieejams https://oig.justice.gov/reports/2016/o1601a.pdf

([2]) Sk. www.dni.gov/clpo

— Ņemot vērā ASV prezidenta B. Obamas ieceltas neatkarīgas pārbaudes grupas ieteikumu, NID ir izveidojis jaunu mehānismu, ar ko uzraudzīt tādu sakaru izlūkdatu vākšanu un izplatīšanu, kas ir sevišķi sensitīvi subjekta veida vai to vākšanas līdzekļu dēļ, lai tādējādi nodrošinātu atbilstību politikas veidotāju konstatējumiem.

— Visbeidzot, NIDB ik gadu izskata ID resursu sadalījumu VIPS prioritāšu un izlūkošanas uzdevumu kā kopuma īstenošanai. Šajā pārbaudē izvērtē visu savākto izlūkdatu, arī sakaru izlūkdatu, veidu vērtību un analizē gan pagātni, proti, cik veiksmīgi ID ir izdevies īstenot savus mērķus, gan nākotni – kādas būs ID turpmākās vajadzības? Šādi nodrošina, ka sakaru izlūkošanas resursus izmanto vissvarīgāko valsts prioritāšu īstenošanai.

Kā redzams šajā vispusīgajā pārskatā, izlūkdienests pats neizlemj, kuras sarunas noklausīties un vai censties savākt visu informāciju, un tā darbības tiek rūpīgi pārraudzītas. Tā īstenotie pasākumi ir vērsti uz politikas veidotāju izvirzītajām prioritātēm, kuru īstenošanas procesā piedalās visa valdība un ko pārrauga gan NDA, gan NIDB, Tieslietu ministrija un Aizsardzības ministrija.

PPD-28 ir paredzēti arī daudzi citi noteikumi, kas nodrošina ar sakaru izlūkošanas darbībām savāktās personiskās informācijas aizsardzību neatkarīgi no valstspiederības. Piemēram, PPD-28 ir noteiktas datu drošības, piekļuves un kvalitātes nodrošināšanas procedūras, ar ko aizsargāt personisko informāciju, kas savākta, veicot sakaru izlūkošanu, kā arī obligātas mācības, ar ko nodrošināt, ka darbinieki izprot savu pienākumu aizsargāt personisko informāciju neatkarīgi no tās subjekta valstspiederības. PPD ir iekļauti arī papildu uzraudzības un atbilstības mehānismi. Tie ietver attiecīgo pārraudzības un atbilstības amatpersonu veiktas periodiskas revīzijas un pārbaudes par sakaru izlūkošanas gaitā iegūtās personiskās informācijas aizsardzību. Pārbaudēs ir arī jāizvērtē, kā aģentūras ievēro šādas informācijas aizsardzības procedūras.

Turklāt PPD-28 ir noteikts, ka būtiski ar citu valstu iedzīvotājiem saistīti atbilstības jautājumi tiks risināti valdības augstākajos līmeņos. Ja rodas nopietna atbilstības problēma, kas ietver jebkāda indivīda personisko informāciju, kura savākta sakaru izlūkošanas darbību rezultātā, par to – papildus visu piemēroto ziņošanas prasību izpildei – ātri jāpaziņo NID. Ja problēma ir saistīta ar citas valsts iedzīvotāja personisko informāciju, NID, apspriežoties ar valsts sekretāru un attiecīgās ID struktūrvienības vadītāju, noteiks, vai būtu jārīkojas, lai informētu attiecīgās valsts valdību, vienlaikus nodrošinot avotu un metožu, kā arī ASV darbinieku aizsardzību. Turklāt, kā prasīts PPD-28, valsts sekretārs ir iecēlis augsta līmeņa amatpersonu – sekretāra vietnieci *Catherine Novelli* – par kontaktpersonu citu valstu valdībām, kuras vēlas paust bažas par Amerikas Savienoto Valstu īstenotajām sakaru izlūkošanas darbībām. Šī apņemšanās nodrošināt augsta līmeņa līdzdalību ir viens no piemēriem, kas apliecina ASV valdības pēdējo gadu centienus vairot pārliecību par daudzajiem privātuma aizsardzības pasākumiem, kas mēdz pārklāties un kurus īsteno, lai aizsargātu gan ASV, gan citu valstu iedzīvotāju personisko informāciju.

e. **Kopsavilkums**

Amerikas Savienoto Valstu īstenotie ārējās izlūkošanas informācijas vākšanas, glabāšanas un izplatīšanas procesi nodrošina būtiskas ikviena indivīda – neatkarīgi no valstspiederības – personiskās informācijas privātuma garantijas. Konkrētāk, ar tiem nodrošina, ka mūsu izlūkdienests koncentrējas uz piemērojamos tiesību aktos, izpildrīkojumos un prezidenta direktīvās atļautiem ar valsts drošību saistītiem uzdevumiem; sargā informāciju no neatļautas piekļuves, izmantošanas un izpaušanas; kā arī veic savas darbības vairāku līmeņu, tostarp Kongresa izveidotas pārraudzības komitejas, pārraudzībā un uzraudzībā. PPD-28 un tās īstenošanas procedūras atspoguļo mūsu centienus attiecināt konkrētus datu minimizācijas un citus būtiskus datu aizsardzības principus uz visu indivīdu personisko informāciju neatkarīgi no subjekta valstspiederības. Personiskajai informācijai, kas iegūta ar ASV īstenotajām sakaru izlūkošanas informācijas vākšanas darbībām, piemēro ASV tiesību aktos un prezidenta norādēs noteiktos principus un prasības, tostarp PPD-28 paredzētos aizsardzības pasākumus. Ar šiem principiem un prasībām tiek nodrošināta cieņpilna izturēšanās pret ikvienu neatkarīgi no personas valstspiederības un dzīvesvietas, kā arī atzīts, ka visiem indivīdiem ir likumīgas tiesības uz privātumu to personiskās informācijas apstrādē.

II. Ārējās izlūkošanas un novērošanas likums – 702. pants

Datu vākšana saskaņā ar Ārējās izlūkošanas un novērošanas likuma ([1]) 702. pantu ir nevis "masveidīga un nekritiska", bet gan šauri koncentrēta uz ārējās izlūkošanas informācijas vākšanu no individuāli noteiktiem un likumīgiem subjektiem; to ir skaidri atļāvusi konkrēta likumiska iestāde; un uz to vienmēr attiecina gan neatkarīgu tiesas veiktu uzraudzību, gan pamatīgu pārbaudi un uzraudzību, ko īsteno izpildvara un Kongress. Informācijas vākšanu saskaņā ar 702. pantu uzskata par sakaru izlūkošanu, kam piemēro PPD-28 prasības ([2]).

Saskaņā ar 702. pantu veikta informācijas vākšana ir viens no visvērtīgākajiem izlūkdatu avotiem, kas aizsargā gan Amerikas Savienotās Valstis, gan mūsu Eiropas partnerus. Plaša informācija par 702. panta darbību un tā īstenošanas pārraudzību ir pieejama publiski. Daudzi ar programmu saistīti iesniegumi tiesā, tiesu nolēmumi un pārraudzības ziņojumi ir atslepenoti un publiskoti NIDB publiskās informācijas vietnē www.icontherecord.tumblr.com. Turklāt PPBPP ir izstrādājusi vispusīgu 702. panta analīzes ziņojumu, kas ir pieejams tīmekļa vietnē https://www.pclob.gov/library/702-Report.pdf ([3]).

FISA 702. pants pēc plašām Kongresa publiskajām debatēm tika pieņemts kā daļa no *FISA* 2008. gada Grozījumu likuma (*FISA Amendments Act*) ([4]). Tajā tiek atļauts ar ASV elektronisko sakaru pakalpojumu sniedzējiem pieprasītu palīdzību iegūt ārējo izlūkošanas informāciju, novērojot citu valstu iedzīvotājus, kuri atrodas ārpus Amerikas Savienotajām Valstīm. Likuma 702. pantā ģenerālprokuroram un NID – divām Ministru kabineta līmeņa amatpersonām, ko iecēlis prezidents un apstiprinājis Senāts – ir atļauts katru gadu iesniegt apliecinājumus FISA tiesai ([5]). Šajos apliecinājumos ir noteiktas konkrētas vācamās ārējās izlūkošanas informācijas kategorijas, piemēram, ar terorisma apkarošanu vai masu iznīcināšanas līdzekļiem saistīta izlūkinformācija, kurai jāatbilst *FISA* noteiktajām ārējās izlūkošanas kategorijām ([6]). Kā ir norādījusi PPBPP, "[š]ie ierobežojumi neļauj neierobežoti vākt informāciju par ārvalstniekiem." ([7])

Apliecinājumos ir jāiekļauj arī "mērķatlases" un "minimizācijas" procedūras, kas ir jāpārbauda un jāapstiprina *FISA* tiesai ([8]). Mērķatlases procedūras ir izstrādātas, lai nodrošinātu vienīgi likumisku datu vākšanu un tās atbilstību apliecinājumu darbības jomai, savukārt datu minimizācijas procedūras ir izveidotas, lai ierobežotu informācijas par ASV iedzīvotājiem ieguvi, izplatīšanu un glabāšanu, taču to noteikumi arīdzan nodrošina būtisku informācijas par citu valstu iedzīvotājiem aizsardzību, kā aprakstīts turpmāk. Turklāt, kā izklāstīts iepriekš, ASV prezidents PPD-28 noteica, ka izlūkdienestam jānodrošina personiskās informācijas par citu valstu iedzīvotājiem papildu aizsardzība, un šie aizsardzības pasākumi attiecas arī uz informāciju, ko vāc saskaņā ar 702. pantu.

Kā ir norādījusi PPBPP, kad tiesa ir apstiprinājusi mērķatlases un minimizācijas procedūras, 702. pantā paredzēto informācijas vākšanu neveic lielapjomā vai nekonkrēti un tā "attiecas vienīgi uz tādām konkrētām personām, par kurām ir pieņemts individuāls konstatējums." ([9]). Vācamo informāciju atlasa, izmantojot individuālus atlasītājus, piemēram, e-pasta adreses vai tālruņa numurus, ko, kā konstatējuši ASV izlūkdarbinieki, iespējams, izmanto, lai nodotu ārējo

([1]) *50 U.S.C. § 1881a.*

([2]) Amerikas Savienotās Valstis var arī saņemt tiesas rīkojumus par datu, tostarp saskaņā ar privātuma vairogu pārsūtītu datu, ieguvi arī atbilstīgi citiem *FISA* noteikumiem. Sk. *50 U.S.C. § 1801 et seq*. *FISA* I un III daļā, kurā ir atļauta attiecīgi elektroniska novērošana un fiziska pārmeklēšana, ir noteikts, ka ir vajadzīgs tiesas rīkojums (izņemot ārkārtas apstākļos) un vienmēr prasīts pamatots iemesls uzskatīt, ka subjekts ir ārēja vara vai ārējas varas pārstāvis. *FISA* IV daļā ir atļauts atbilstīgi tiesas rīkojumam (izņemot ārkārtas apstākļos) izmantot zvanīto numuru reģistrētāju, kā arī uztveršanas un trasēšanas ierīces atļautā ārējā izlūkošanā, pretizlūkošanā vai ar terorisma apkarošanu saistītā izmeklēšanā. *FISA* V daļā FIB ir atļauts saskaņā ar tiesas rīkojumu (izņemot ārkārtas apstākļos) iegūt uzņēmumu datus, kas ir noderīgi atļautā ārējā izlūkošanā, pretizlūkošanā vai ar terorisma apkarošanu saistītā izmeklēšanā. Kā aprakstīts turpmāk, ASV Brīvības likumā ir skaidri aizliegts izmantot *FISA* atļauto zvanīto numuru reģistrētāju vai uzņēmējdarbības datu pieprasījumus datu lielapjoma vākšanai un noteikts, ka ir jālieto "konkrēts atlases vārds", lai nodrošinātu šo pilnvaru mērķtiecīgu izmantošanu.

([3]) Privātuma un pilsonisko brīvību pārraudzības padome, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014. gada 2. jūlijs) ("PPBPP ziņojums").

([4]) Sk. *Pub. L. No. 110-261, 122 Stat. 2436 (2008).*

([5]) Sk. *50 U.S.C. § 1881a(a)* un *(b).*

([6]) Skat. turpat *§ 1801(e).*

([7]) Sk. PPBPP ziņojumu, 99. lpp.

([8]) Sk. *50 U.S.C. § 1881a(d)* un *(e).*

([9]) Sk. PPBPP ziņojumu, 111. lpp.

izlūkošanas informāciju, kuras veids atbilst tiesai iesniegtajā apliecinājumā norādītajam ([1]). Subjekta atlases pamatojums ir jādokumentē, un par katru atlasītāju sagatavoto dokumentāciju pēcāk pārskata Tieslietu ministrija ([2]). ASV valdība ir publiskojusi informāciju, kurā norādīts, ka 2014. gadā saskaņā ar 702. pantu tika vākta aptuveni 90 000 indivīdu informācija – tā ir sīka daļiņa no vispasaules interneta lietotāju skaita, kas pārsniedz trīs miljardus ([3]).

Informācijai, ko vāc saskaņā ar 702. pantu, piemēro tiesas apstiprinātas minimizācijas procedūras, kas nodrošina gan ASV, gan citu valstu iedzīvotāju aizsardzību un ir publiskotas ([4]). Piemēram, gan ASV, gan citu valstu iedzīvotāju saziņas informāciju, kas iegūta atbilstīgi 702. pantam, glabā datubāzēs ar stingru piekļuves kontroli. Šo informāciju var pārskatīt tikai izlūkdarbinieki, kuri ir apmācīti par privātumu aizsargājošām datu minimizācijas procedūrām un ir saņēmuši konkrētu atļauju piekļūt šādai informācijai, lai pildītu savas apstiprinātās funkcijas ([5]). Šos datus izmanto vienīgi ārējās izlūkošanas informācijas vai nozieguma pierādījumu noteikšanai ([6]). Saskaņā ar PPD-28 šo informāciju var izplatīt tikai tad, ja pastāv likumīgs ārējās izlūkošanas vai tiesībaizsardzības nolūks; ar to vien, ka viena saziņas puse nav ASV iedzīvotājs, nepietiek ([7]). Turklāt no minimizācijas procedūrām un PPD-28 izriet arī atbilstīgi 702. pantam iegūto datu glabāšanas ilguma ierobežojumi ([8]).

Tiek īstenota FISA 702. panta īstenošanas plaša pārraudzība, un tā notiek visos trijos mūsu valdības atzaros. Aģentūrās, kas īsteno likumu, pastāv vairāki iekšējās pārbaudes līmeņi, arī neatkarīgi ģenerālinspektori, un piekļuve datiem tiek tehnoloģiski kontrolēta. Tieslietu ministrija un NIDB rūpīgi pārskata un izvērtē 702. panta izmantošanu, lai pārbaudītu atbilstību juridiskajiem noteikumiem; turklāt aģentūrām ir neatkarīgs pienākums paziņot par iespējamiem neatbilstības gadījumiem. Tos izmeklē, un par visiem attiecīgajiem incidentiem ziņo Ārējās izlūkošanas un novērošanas tiesai, Prezidenta Izlūkošanas pārraudzības padomei, kā arī Kongresam, un uz tiem atbilstoši reaģē. ([9]) Līdz šim nav konstatēti apzināti mēģinājumi pārkāpt tiesību aktus vai apiet juridiskās prasības ([10]).

FISA tiesai ir būtiska loma 702. panta īstenošanā. Tiesu veido neatkarīgi federālie tiesneši, kuri tajā strādā septiņus gadus ilgu periodu, taču, tāpat kā visi pārējie federālie tiesneši, ir iecelti par tiesnešiem uz mūžu. Kā norādīts iepriekš, šai tiesai ir jāpārskata ikgadējo apliecinājumu, kā arī mērķatlases un minimizācijas procedūru atbilstība tiesību aktiem. Turklāt, kā arīdzan norādīts iepriekš, ASV valdībai ir nekavējoties jāinformē *FISA* tiesa par iespējamas neatbilstības gadījumiem ([11]); vairāki šīs tiesas atzinumi ir atslepenoti un publiskoti un apliecina, ka tiesa šos incidentus izskata sevišķi rūpīgi un neatkarīgi.

FISA tiesas bijušais galvenais tiesnesis vēstulē Kongresam – publiski pieejama – ir aprakstījis tiesas īstenotos rūpīgos procesus ([12]). Turklāt saskaņā ar turpmāk aprakstīto ASV Brīvības likumu (*USA FREEDOM Act*) *FISA* tiesai tagad ir skaidri atļauts iecelt ārēju advokātu par neatkarīgu privātuma aizstāvi lietās, kas rada jaunus vai būtiskus juridiskos jautājumus ([13]). Tas, cik lielā mērā ārējās izlūkošanas darbībās, kas vērstas uz personām, kuras nav ne attiecīgās valsts pilsoņi, ne tajā atrodas, tiek iesaistīta valsts neatkarīgā tiesu vara ir neierasti un, iespējams, pat nepieredzēti un palīdz nodrošināt, ka, vācot informāciju saskaņā ar 702. pantu, tiek ievēroti attiecīgie juridiskie ierobežojumi.

([1]) Turpat.

([2]) Turpat 8. lpp. *50 U.S.C. § 1881a(l)*; sk. arī NDA Pilsonisko brīvību un privātuma aizsardzības biroja direktora ziņojuma "*NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*" (turpmāk tekstā "NDA ziņojums") 4. lpp., pieejams vietnē http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties

([3]) *Director of National Intelligence 2014 Transparency Report*, pieejams vietnē http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014

([4]) Informācija par minimizācijas procedūrām ir pieejama šādās vietnēs: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf ("NDA minimizācijas procedūras"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; un http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf

([5]) Sk. NDA ziņojumu, 4. lpp.

([6]) Sk., piemēram, NDA minimizācijas procedūras, 6. lpp.

([7]) Izlūkaģentūras procedūras PPD-28 īstenošanai ir pieejamas vietnē http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties

([8]) Sk. NDA minimizācijas procedūras; PPD-28 4. sadaļa.

([9]) Sk. *50 U.S.C. § 1881(l)*; sk. arī PPBPP ziņojuma 66.–76. lpp.

([10]) Sk. *Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, ko iesniedzis ģenerālprokurors un nacionālās izlūkošanas direktors (2. un 3. lpp.), pieejams vietnē http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf

([11]) Ārējās izlūkošanas un novērošanas tiesas Reglamenta 13. noteikums, pieejams vietnē http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf

([12]) Godātā *Reggie B. Walton* 2013. gada 29. jūlija vēstule godātajam *Patrick J. Leahy*, pieejama vietnē http://fas.org/irp/news/2013/07/fisc-leahy.pdf

([13]) Sk. ASV Brīvības likuma 401. pantu, *P. L. 114-23*.

Kongress īsteno pārraudzību, likumiski pieprasot ziņojumus izlūkošanas un tieslietu komitejām, kā arī bieži rīkojot iztaujāšanas un uzklausīšanas. Šie ziņojumi ir, piemēram, ģenerālprokurora pusgada ziņojums, kurā dokumentē 702. panta izmantošanu un visus neatbilstības gadījumus; ([1]) atsevišķs ģenerālprokurora un NID sagatavots novērtējums, kurā dokumentē mērķatlases un minimizācijas procedūru ievērošanu, tostarp tādu procedūru ievērošanu, kas izstrādātas, lai nodrošinātu informācijas vākšanu likumīgam ārējās izlūkošanas mērķim ([2]); kā arī izlūkošanas struktūrvienību vadītāju gada ziņojumi, kuros iekļauj apliecinājumu, ka, vācot informāciju saskaņā ar 702. pantu, joprojām tiek sagādāta ārējās izlūkošanas informācija ([3]).

Īsi sakot, informācijas vākšana saskaņā ar 702. pantu ir atļauta ar likumu; tai piemēro vairākus pārbaudes, tiesiskās uzraudzības un pārraudzības līmeņus; un, kā nesen atslepenotā atzinumā paziņoja *FISA* tiesa, to "veic nevis lielapjomā vai nekritiski," bet gan "pieņemot (..) diskrētus mērķatlases lēmumus par individuāliem [saziņas] resursiem" ([4]).

III. ASV BRĪVĪBAS LIKUMS

ASV Brīvības likums, kas tika pieņemts kā likums 2015. gada jūnijā, ievērojami mainīja ASV novērošanas un citas ar valsts drošību saistītas pilnvaras un palielināja to izmantošanas un *FISA* tiesas nolēmumu publisko pārredzamību, kā izklāstīts turpmāk ([5]). Šis likums nodrošina mūsu izlūkošanas un tiesībaizsardzības jomas darbiniekiem valsts aizsardzības nodrošināšanā nepieciešamās pilnvaras un vienlaikus garantē arī indivīdu privātuma pienācīgu aizsardzību šo pilnvaru izmantošanas gaitā. Tas pastiprina privātumu un pilsoniskās brīvības un palielina pārredzamību.

Likumā ir aizliegta jebkādu datu, tostarp gan ASV, gan citu valstu iedzīvotāju datu, lielapjoma vākšana, pamatojoties uz dažādiem *FISA* noteikumiem vai izmantojot vēstules par valsts drošību (likumā atļauts administratīvās pavēstes veids) ([6]). Šis aizliegums jo īpaši attiecas uz tālruņa metadatiem par zvaniem starp personām, kas atrodas ASV, un personām ārpus ASV, un tas attiektos arī uz privātuma vairoga informācijas vākšanu saskaņā ar šīm pilnvarām. ASV Brīvības likumā noteikts, ka valdībai visos šo pilnvaru īstenošanas nolūkā iesniegtajos datu ieguves pieteikumos jāizmanto "konkrēts atlases vārds", proti, vārds, ar ko konkrēti identificē personu, kontu, adresi vai personālo ierīci veidā, kas, cik vien praksē pamatoti iespējams, ierobežo meklētās informācijas apmēru ([7]). Savukārt šis nosacījums nodrošina izlūkošanas nolūkos vāktās informācijas precīzu noteikšanu un atlasi.

Šajā likumā tika noteiktas arī ievērojamas *FISA* tiesas procesu izmaiņas, kuras gan palielina pārredzamību, gan rada papildu pārliecību par privātuma aizsardzību. Kā norādīts iepriekš, likumā tika atļauts izveidot pastāvīgu advokātu komiteju, kuras locekļi ir izturējuši drošības pārbaudi, ir kompetenti ar privātumu un pilsoniskajām brīvībām, izlūkošanas informācijas vākšanu, sakaru tehnoloģijām vai citām attiecīgām jomām saistītos jautājumos un var tikt iecelti uzstāties tiesā kā *amicus curiae* lietās, kas ietver būtisku vai jaunu tiesību aktu interpretāciju. Šie advokāti drīkst izvirzīt juridiskos argumentus, kas veicina indivīdu privātuma un pilsonisko brīvību aizsardzību, un varēs piekļūt jebkādai informācijai, arī klasificētai, ko tiesa uzskata par nepieciešamu viņu pienākumu izpildē ([8]).

Likumā arī tiek regulēta nepieredzētā ASV valdības pārredzamība izlūkošanas darbību jomā, prasot, lai NID, apspriežoties ar ģenerālprokuroru, vai nu atslepeno, vai arī publicē atslepenotu kopsavilkumu par katru *FISA* tiesas vai Ārējās izlūkošanas un novērošanas apelācijas tiesas nolēmumu, rīkojumu vai atzinumu, kas ietver būtisku kādas tiesību normas skaidrojumu vai interpretāciju.

([1]) Sk. *50 U.S.C. § 1881f*.
([2]) Sk. turpat. *§ 1881a(l)(1)*.
([3]) Sk. turpat. *§ 1881a(l)(3)*. Daži no šiem ziņojumiem ir klasificēti.
([4]) *Mem.* atzinums un rīkojums, 26. lpp. (*FISC 2014*), pieejams vietnē http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf
([5]) Sk. 2015. gada ASV Brīvības likumu, *Pub. L. Nr. 114-23, § 401, 129 Stat. 268*.
([6]) Sk. turpat *§§ 103, 201, 501*. Vēstules par valsts drošību ir atļautas dažādos likumos, un tās sniedz FIB iespēju no dažādu veidu uzņēmumiem iegūt kredīta pārskatos, finanšu pārskatos, kā arī elektronisko abonentu un darījumu pārskatos iekļauto informāciju, tomēr tās drīkst izmantot vienīgi tādēļ, lai nodrošinātu aizsardzību pret starptautisko terorismu vai slepenām izlūkošanas darbībām. Sk. *12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709*. Ar vēstulēm par valsts drošību FIB parasti vāc būtisku nesatura informāciju agrīnos terorisma apkarošanas un pretizlūkošanas izmeklēšanas posmos, piemēram, cenšas uzzināt tāda konta abonenta identitāti, no kura, iespējams, notikusi saziņa ar teroristu grupējuma, piemēram, ISIL, pārstāvjiem. Valsts drošības vēstules saņēmējiem ir tiesības to apstrīdēt tiesā. Sk. *18 U.S.C. § 3511*;
([7]) Sk. turpat.
([8]) Sk. turpat *§ 401(e)*.

ASV Brīvības likumā ir paredzēta arīdzan plašas informācijas atklāšana par datu vākšanu saskaņā ar *FISA* un par valsts drošības vēstulē iesniegtajiem pieprasījumiem. Amerikas Savienotajām Valstīm ik gadu jāatklāj Kongresam un sabiedrībai pieprasīto un pieņemto *FISA* rīkojumu un apliecinājumu skaits; aplēses par plānoto un reāli novēroto ASV un citu valstu iedzīvotāju skaitu; un *amici curiae* iecelšanas reižu skaits, kā arī cita informācija ([1]). Likumā arī noteikts, ka valdībai jāsagatavo papildu publiskais pārskats par to, cik valsts drošības vēstuļu iesniegts par ASV un citu valstu iedzīvotājiem ([2]).

Attiecībā uz uzņēmumu pārredzamību jānorāda, ka ASV Brīvības likumā ir paredzēti vairāki veidi, kā uzņēmumi var publiski paziņot *FISA* rīkojumu un norāžu kopskaitu, no valdības saņemto vēstuļu par valsts drošību daudzumu, kā arī to, uz cik klientu kontiem šie rīkojumi attiecās ([3]). Vairāki uzņēmumi jau ir izpauduši šādu informāciju, kurā norādīts ierobežotais to klientu skaits, kuru dati ir prasīti.

Šie uzņēmumu pārredzamības ziņojumi liecina, ka ASV izlūkošanas pieprasījumi skar tikai pavisam nelielu datu daļu. Piemēram, nesen sagatavots kāda liela uzņēmuma pārredzamības pārskats liecina, ka uzņēmums periodā, kad tam bija vismaz 400 miljoni abonentu, saņēma ar valsts drošību saistītus pieprasījumus (saskaņā ar *FISA* vai vēstulēs par valsts drošību) attiecībā uz mazāk nekā 20 000 lietotāju kontu. Citādi sakot, visi ar valsts drošību saistītie ASV pieprasījumi, par kuriem ziņoja šis uzņēmums, skāra mazāk nekā 0,005 % tā abonentu. Arī tad, ja katrs attiecīgais pieprasījums būtu attiecies uz "drošības zonas" datiem, kā, protams, nebija, ir acīmredzams, ka pieprasījumi ir mērķtiecīgi un atbilstoši un nav ne lielapjoma, nedz nekritiski.

Visbeidzot, lai gan likumi, kuros ir atļautas vēstules par valsts drošību, jau stingri ierobežoja apstākļus, kādos šādas vēstules saņēmējam varētu liegt tās izpaušanu, ASV Brīvības likumā arīdzan tika noteikts, ka neizpaušanas prasības ir periodiski jāpārskata; prasīts paziņot vēstuļu par valsts drošību saņēmējiem, kad fakti vairs nepamato neizpaušanas prasību; un kodificētas procedūras, ar kurām saņēmēji var apstrīdēt neizpaušanas prasības ([4]).

Rezumējot jānorāda, ka ASV Brīvības likuma noteikumi, kuri būtiski groza ASV izlūkošanas iestāžu pilnvaras, skaidri apliecina ASV plašos centienus padarīt personiskās informācijas, privātuma, pilsonisko brīvību un pārredzamības aizsardzību par visu ASV izlūkošanas prakses veidu prioritāti.

IV. PĀRREDZAMĪBA

Papildus ASV Brīvības likumā paredzētajai pārredzamībai ASV izlūkdienests nodrošina sabiedrībai plašu papildu informācijas klāstu, rādot ļoti labu priekšzīmi tā izlūkošanas darbību pārredzamības jomā. Izlūkdienests ir publicējis daudzus savus politikas dokumentus, informāciju par tā īstenotajām procedūrām, Ārējās izlūkošanas un novērošanas tiesas nolēmumus un citus atslepenotus materiālus, tādējādi nodrošinot sevišķi lielu pārredzamību. Turklāt izlūkdienests ir būtiski palielinājis statistikas apmēru, ko izpauž par valdības izmantotajām ar valsts drošību saistītas informācijas vākšanas pilnvarām. Izlūkdienests 2015. gada 22. aprīlī laida klajā tā otro gada ziņojumu, kurā izklāstīti statistikas dati par to, cik bieži valstība šīs svarīgās pilnvaras izmanto. Arī NIDB ir publicējis – NIDB tīmekļa vietnē un portālā *IC On the Record* – konkrētu pārredzamības principu kopumu ([5]) un īstenošanas plānu, kurā principi ir iestrādāti konkrētās un izmērāmās iniciatīvās ([6]). Nacionālās izlūkošanas direktors 2015. gada oktobrī noteica, ka ikvienai izlūkaģentūrai jāieceļ tam pakļauta izlūkošanas pārredzamības amatpersona, kas veicinātu pārredzamību un vadītu pārredzamības iniciatīvu īstenošanu ([7]). Pārredzamības amatpersona cieši sadarbosies ar katras izlūkaģentūras privātuma un pilsonisko brīvību aizsardzības amatpersonu, lai kopā nodrošinātu, ka pārredzamība, privātums un pilsoniskās brīvības arī turpmāk ir galvenās prioritātes.

([1]) Sk. turpat *§ 602*.
([2]) Sk. turpat.
([3]) Sk. turpat *§ 603*.
([4]) Sk. turpat. *§§ 502(f)–503*.
([5]) Pieejams vietnē http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles
([6]) Pieejams vietnē http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf
([7]) Sk. turpat.

Šos centienus apliecina tas, ka NDA galvenā privātuma un pilsonisko brīvību aizsardzības amatpersona pēdējo pāris gadu laikā ir publiskojusi vairākus atslepenotus ziņojumus, arī ziņojumus par darbībām, kas īstenotas saskaņā ar *FISA* 702. pantu, Izpildrīkojumu Nr. 12333 un ASV Brīvības likumu ([1]). Papildus tam ID cieši sadarbojas ar PPBPP, Kongresu un ASV privātuma aizstāvju kopienu, lai nodrošinātu papildu pārredzamību saistībā ar ASV īstenotajām izlūkošanas darbībām, kad vien tas ir iespējams un savietojams ar sensitīvu izlūkošanas avotu un metožu aizsardzību. Kopumā jānorāda, ka ASV veiktās izlūkošanas darbības ir tikpat pārredzamas vai pārredzamākas kā jebkuras citas pasaules valsts īstenotā izlūkošana un tās ir tik pārredzamas, cik vien iespējams, vienlaicīgi ievērojot nepieciešamību aizsargāt sensitīvus avotus un metodes.

Rezumējot ASV īstenoto izlūkošanas darbību plašo pārredzamību, jānorāda turpmākais.

— ID ir laidis klajā un publicējis tiešsaistē kopumā vairākus tūkstošus lappušu garus tiesu atzinumus un aģentūras procedūru izklāstus, kuros aprakstītas konkrētas ar mūsu veiktajām izlūkošanas darbībām saistītas procedūras un prasības. Mēs arī esam publiskojuši ziņojumus par izlūkaģentūru darbības atbilstību piemērojamiem ierobežojumiem.

— Augstākā līmeņa izlūkošanas amatpersonas regulāri publiski izsakās par savu organizāciju funkcijām un darbībām, tostarp apraksta to darbam piemērojamos atbilstības režīmus un aizsardzības pasākumus.

— ID publiskoja vairākus papildu dokumentus par izlūkošanas darbībām, kas veiktas saskaņā ar ASV Likumu par informācijas brīvību.

— ASV prezidents pieņēma PPD-28, kurā ir publiski noteikti papildu ierobežojumi, kas jāievēro mūsu veiktajās izlūkošanas darbībās, savukārt NIDB ir laidis klajā divus publiskos ziņojumus par šo ierobežojumu īstenošanu.

— Atbilstīgi tiesību aktiem ID patlaban ir jāpublisko svarīgi *FISA* tiesas pieņemti juridiskie atzinumi vai to kopsavilkumi.

— Valdībai ik gadu ir jāziņo, cik lielā mērā tā ir izmantojusi konkrētas ar valsts drošību saistītas pilnvaras, un tas ir atļauts arī uzņēmumiem.

— PPBPP ir pieņēmusi vairākus sīki izstrādātus publiskos ziņojumus par izlūkošanas darbībām un tā darīs arī turpmāk.

— ID sniedz plašu klasificēto informāciju Kongresa izveidotām pārraudzības komitejām.

— Lai reglamentētu izlūkdienesta darbības, NID pieņēma pārredzamības principus.

Šī plašā pārredzamība tiks nodrošināta arī turpmāk. Visa publiskotā informācija, protams, būs pieejama gan Tirdzniecības ministrijai, gan Eiropas komisijai. Gada pārskatīšanā par privātuma vairoga īstenošanu, kurā piedalīsies gan Eiropas Komisija, gan Tirdzniecības ministrija, Eiropas Komisija varēs iztirzāt visus jautājumus, ko radīs jauna publiskota informācija, kā arī citus jautājumus par privātuma vairogu un tā darbību, un mēs saprotam, ka ministrija var pēc saviem ieskatiem aicināt šajā pārskatīšanā piedalīties arī citu aģentūru, tostarp ID, pārstāvjus. Tas, protams, papildina PPD-28 paredzēto mehānismu, ar ko ES dalībvalstis var paust ar novērošanu saistītas bažas īpašajai valsts departamenta amatpersonai.

V. TIESISKĀ AIZSARDZĪBA

ASV tiesību aktos ir paredzēti vairāki tiesiskās aizsardzības līdzekļi, ko var izmantot indivīdi, kuri tikuši pakļauti nelikumīgai elektroniskai novērošanai valsts drošības nolūkos. Atbilstīgi *FISA* tiesības pieprasīt tiesību aizsardzību ASV tiesā ir ne tikai ASV iedzīvotājiem. Indivīdam, kurš var pierādīt savu procesuālo tiesībspēju, būtu pieejami tiesiskās

([1]) Pieejams vietnē https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf

aizsardzības līdzekļi, ar ko apstrīdēt nelikumīgo elektronisko novērošanu saskaņā ar *FISA*. Piemēram, atbilstīgi *FISA* personas, kuras ir nelikumīgi elektroniski novērotas, drīkst personīgi iesūdzēt tiesā ASV valdības amatpersonas un pieprasīt finansiālu atlīdzību, tostarp advokāta maksas atlīdzību un sodošu zaudējumu atlīdzību. Sk. *50 U.S.C. § 1810*; Indivīdiem, kuri var pierādīt savas tiesības tiesāties, ir arī civiltiesisks pamatojums ierosināt pret Amerikas Savienotajām Valstīm prasību par finansiālu atlīdzību, tostarp tiesvedības izmaksu atlīdzību, ja informācija, kas par tiem iegūta, veicot elektronisku novērošanu saskaņā ar *FISA*, ir nelikumīgi un apzināti izmantota vai izpausta. Sk. *18 U.S.C. § 2712*; Ja valdība Amerikas Savienotajās Valstīs īstenotā tiesas vai administratīvajā procesā grasās pret personu izmantot vai izpaust jebkādu informāciju, kas iegūta vai atvasināta, veicot šīs personas elektronisku novērošanu saskaņā ar *FISA*, tai par savu nodomu iepriekš jāinformē gan tiesa, gan attiecīgā persona, kura var apstrīdēt novērošanas likumību un censties panākt šīs informācijas noklusēšanu. Sk. *50 U.S.C. § 1806*; Visbeidzot, *FISA* ir paredzēti arī krimināLsodi indivīdiem, kuri tiesību aktu aizsegā apzināti iesaistās nelikumīgā elektroniskajā novērošanā vai tīši izmanto vai izpauž nelikumīgā novērošanā iegūtu informāciju. Sk. *50 U.S.C. § 1809*;

ES pilsoņiem ir arī citas iespējas pieprasīt tiesisko aizsardzību pret ASV valdības amatpersonām, kuras valdības vārdā ir nelikumīgi izmantojušas datus vai tiem piekļuvušas, tostarp valdības amatpersonām, kuras pārkāpj tiesību aktus, kad nelikumīgi piekļūst informācijai vai to izmanto šķietamiem ar valsts drošību saistītiem mērķiem. Likumā par datorkrāpšanu un ļaunprātīgu izmantošanu (*The Computer Fraud and Abuse Act*) ir aizliegta apzināta un neatļauta piekļuve (vai atļautā piekļuves apmēra pārsniegšana) nolūkā iegūt informāciju no finanšu iestādes, ASV valdības datorsistēmas vai datora, kam piekļūts ar interneta starpniecību, kā arī draudi kaitēt aizsargātiem datoriem izspiešanas vai krāpšanas nolūkā. Sk. *18 U.S.C. § 1030*; Ikviena persona – neatkarīgi no valstspiederības –, kas cieš kaitējumu vai zaudējumus šā tiesību akta pārkāpuma dēļ, var iesūdzēt pārkāpēju (arī valdības amatpersonu) tiesā un pieprasīt zaudējumu atlīdzību un aizliegumu vai citu taisnīgu tiesību aizsardzības līdzekli saskaņā ar 1030. iedaļas g) daļu neatkarīgi no tā, vai ir īstenota krimināLvajāšana, ja vien attiecīgā rīcība iever vismaz vienu vai vairākus konkrētajā likumā noteiktos apstākļus. Elektroniskās saziņas privātuma likumā (*Electronic Communications Privacy Act – ECPA*) ir reglamentēta valdības piekļuve elektronisko sakaru un darījumu datiem un abonentu informācijai, ko glabā sakaru pakalpojumu sniedzēji, kas ir trešās personas. Sk. *18 U.S.C. §§ 2701-2712*. Atbilstīgi *ECPA* cietusī persona var valdības amatpersonas iesūdzēt tiesā par apzinātu un nelikumīgu piekļuvi glabātajiem datiem. *ECPA* tiek piemērots visām personām neatkarīgi no pilsonības, un cietušās personas var saņemt zaudējumu un advokāta maksas atlīdzību. Likums par tiesībām uz finanšu datu aizsardzību (*Right to Financial Privacy Act – RFPA*) ierobežo ASV valdības piekļuvi banku un brokeru-starpnieku datiem par individuāliem klientiem. Sk. *12 U.S.C. §§ 3401-3422*. Saskaņā ar *RFPA* bankas vai brokera-starpnieka klients var iesūdzēt ASV valdību tiesā un pieprasīt tiesību aktos paredzēto, faktiski radīto un sodošu zaudējumu atlīdzību par nelikumīgu piekļūšanu klienta datiem un, konstatējot, ka nelikumīgā piekļuve bija apzināta, tiek sākta izmeklēšana par iespējamu disciplinārlietas ierosināšanu pret attiecīgajiem valdības darbiniekiem. Sk. *12 U.S.C. § 3417*.

Visbeidzot, Likumā par informācijas brīvību (LIB) ir noteikti līdzekļi, ar ko ikviena persona var pieprasīt piekļuvi pašreizējiem federālās aģentūras datiem par jebkuru tematu, ievērojot konkrētas izņēmumu kategorijas. Sk. *5 U.S.C. § 552(b)*; Tie ir ierobežojumus attiecībā uz piekļuvi klasificētai valsts drošības informācijai, citu indivīdu personiskajai informācijai un informācijai par tiesībaizsardzības izmeklēšanu; un šie ierobežojumi ir pielīdzināmi ierobežojumiem, ko savos tiesību aktos par piekļuvi informācijai ir noteikušas citas valstis. Šie ierobežojumi vienādi attiecas gan uz amerikāņiem, gan indivīdiem ar citu valstspiederību. Strīdus par atbilstīgi LIB pieprasītas informācijas izpaušanu var pārsūdzēt administratīvi un pēc tam – federālajā tiesā. Tiesai ir jāpieņem *de novo* nolēmums par to, vai informācijas neizpaušana ir pamatota (*5 U.S.C. § 552(a)(4)(B)*), un tā var likt valdībai nodrošināt piekļuvi datiem. Atsevišķos gadījumos tiesas ir noraidījušas valdības apgalvojumus par to, ka informācija nebūtu jāizpauž, jo ir klasificēta ([1]). Lai gan finansiāla zaudējumu kompensācija nav paredzēta, tiesa var nolemt, ka ir jākompensē advokāta honorārs.

VI. SECINĀJUMS

Amerikas Savienotās Valstis atzīst, ka mūsu sakaru izlūkošanas un citu izlūkošanas veidu darbībās jāņem vērā tas, ka pret visām personām neatkarīgi no to valstspiederības un dzīvesvietas būtu jāizturas ar cieņu un ka visām personām ir likumīgas tiesības uz privātumu to personiskās informācijas apstrādē. Amerikas Savienotās Valstis izmanto sakaru izlūkošanu vienīgi tādēļ, lai veicinātu savu valsts drošības un ārpolitikas interešu īstenošanu, kā arī aizsargātu savus un savu sabiedroto un partneru pilsoņus no kaitējuma. Īsi sakot, ID neveic personu, tostarp parasto Eiropas pilsoņu, nekritisku novērošanu. Sakaru izlūkdatus vāc vienīgi tad, ja tas ir pienācīgi atļauts un tādā veidā, kas stingri atbilst visiem šiem ierobežojumiem; tikai pēc alternatīvu avotu, arī diplomātisku un publisku, pieejamības izskatīšanas; un

([1]) Sk., piemēram., *New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

veidā, kura prioritāte ir atbilstošas un praksē īstenojamas alternatīvas. Turklāt, kad vien praksē iespējams, sakaru izlūkošana notiek, tikai vācot ar konkrētiem ārējās izlūkošanas subjektiem vai tēmām saistītu informāciju, izmantojot diskriminantus.

Uz šo jomu attiecināmā ASV politika tika apstiprināta PPD-28. Šajā satvarā ASV izlūkaģentūrām nav juridisku pilnvaru, resursu, tehnisko spēju un vēlmes pārtvert visus pasaules sakarus. Aģentūru darbinieki nelasa visu Amerikas Savienoto Valstu vai pasaules iedzīvotāju e-vēstules. Atbilstīgi PPD-28 Amerikas Savienotās Valstis nodrošina stingrus aizsardzības pasākumus attiecībā uz citu valstu iedzīvotāju personisko informāciju, ko vāc, īstenojot sakaru izlūkošanas darbības. Cik vien iespējams un savietojams ar valsts drošības interesēm, šie aizsardzības pasākumi ietver politiku un procedūras, ar ko līdz minimumam samazināt citu valstu iedzīvotāju personiskās informācijas glabāšanu un izplatīšanu, kas ir līdzvērtīgi ASV iedzīvotājiem nodrošinātajiem aizsardzības pasākumiem. Turklāt, kā aprakstīts iepriekš, vispusīgajam pārraudzības režīmam, ko piemēro *FISA* 702. pantā piešķirto pilnvaru izmantošanai, nav līdzvērtīga. Visbeidzot, būtiskie ASV izlūkošanas tiesību aktu grozījumi, kas izriet no ASV Brīvības likuma, un NIDB vadītās iniciatīvas izlūkdienesta darbību pārredzamības veicināšanai ievērojami palielina visu indivīdu – neatkarīgi no valstspiederības – privātumu un pilsoniskās brīvības.

Ar cieņu

Robert S. Litt

2016. gada 21. jūnijs

Juriskonsultam
Justin S. Antonipillai
ASV Tirdzniecības ministrija
1401 Constitution Avenue, N.W.
Washington, DC 20230

Ministra vietniekam
Ted Dean
Starptautiskās tirdzniecības administrācija
1401 Constitution Avenue, N.W.
Washington, DC 20230

Godātais *Antonipillai* kungs un godātais *Dean* kungs!

Rakstu Jums, lai sniegtu papildu informāciju par veidu, kādā veidā Amerikas Savienotās Valstis veic sakaru izlūkdatu lielapjoma vākšanu. Kā paskaidrots Prezidenta politikas direktīva Nr. 28 (PPD-28) 5. zemsvītras piezīmē, "lielapjoma vākšana" attiecas uz sakaru izlūkošanas informācijas vai datu iegūšanu relatīvi lielā daudzumā apstākļos, kad izlūkdienesti vākšanas fokusēšanai nevar izmantot identifikatoru, kas saistīts ar konkrētu mērķi (piemēram, mērķa e-pasta adrese vai tālruņa numurs). Tomēr tas nenozīmē, ka šāda vākšana ir "masveida" vai "nekritiska". Patiesi, PPD-28 arī pieprasa, lai "[s]akaru izlūkošanas darbības ir pēc iespējas pielāgotas." Lai to sekmētu, izlūkdienesti veic pasākumus, lai nodrošinātu, ka pat tad, kad nav iespējams izmantot identifikatorus mērķtiecīgai vākšanai, vācamajos datos, iespējams, būs ārvalstu izlūkošanas dati, kas atbildīs politikas veidotāju izteiktajām prasībām saskaņa ar procesu, kurš izskaidrots manā iepriekšējā vēstulē, un samazina savāktās nederīgas informācijas apjomu.

Piemēram, izlūkdienestiem var lūgt iegūt sakaru izlūkdatus par teroristu grupas darbībās, kura darbojas kādas Tuvo Austrumu valsts reģionā un par kuru tiek uzskatīts, ka tā plāno uzbrukumus Rietumeiropas valstīm, bet dienesti var nezināt ar šo teroristu grupu saistīto personu vārdus, tālruņa numurus, e-pasta adreses vai citus konkrētus identifikatorus. Mēs varētu izvēlēties šo grupu par mērķi, vācot sakaru informāciju uz šo reģionu un no tā, lai to sīkāks pārskatītu un analizētu ar mērķi noteikt to saziņu, kas attiecas uz grupu. Šādi rīkojoties, izlūkdienesti centīsies iespējami sašaurināt datu vākšanu. Tā tiktu uzskatīta par "lielapjoma" vākšanu, jo diskriminantu izmantošana nav lietderīga, tomēr tā nebūtu "masveida" vai "nekritiska" vākšana; drīzāk tā ir tik precīza, cik vien iespējams.

Tādējādi, pat ja nav iespējama mērķtiecīga meklēšana, izmantojot konkrētus atlasītājus, Amerikas Savienotās valstis nevāc visus paziņojumus no visiem saziņas līdzekļiem visā pasaulē, bet izmanto filtrus un citus tehniskos rīkus, lai fokusētu vākšanu uz tiem objektiem, kuros varētu būt saziņas informācija ar ārvalstu izlūkošanas vērtību. Šādi rīkojoties, Amerikas Savienoto Valstu sakaru izlūkošanas darbības attiecas tikai uz daļu no saziņas, kas notiek internetā.

Turklāt, kā minēts manā iepriekšējā vēstulē, sakarā ar to, ka "lielapjoma" vākšana rada lielāku risku, ka tiks savākta nederīga informācija, PPD-28 ierobežo izmantošanu tā, ka izlūkdienesti "lielapjoma" vākšanā iegūtus sakaru izlūkdatus var izmantot sešiem konkrētiem mērķiem. PPD-28 un Aģentūras politika PPD-28 īstenošanai arī nosaka ierobežojumus personiskas informācijas, kas iegūta sakaru izlūkošanas darbībās, saglabāšanai un izplatīšanai – neatkarīgi no tā, vai informācija tika iegūta "lielapjoma" vai mērķtiecīgā vākšanā, un neatkarīgi no personas valstspiederības.

Tādējādi izlūkdienestu veiktā "lielapjoma" vākšana nav "masveida" vai "nekritiska", bet tajā tiek izmantotas metodes un rīki, lai filtrētu vākšanu nolūkā to fokusēt uz materiālu, kas būs atbilstošs politikas veidotāju izteiktajām ārvalstu izlūkošanas prasībām, vienlaikus samazinot nederīgas informācijas vākšanu, un tā paredz stingrus noteikumus, lai

aizsargātu nederīgo informāciju, kas varētu tikt iegūta. Šajā vēstulē aprakstītā politika un procedūras attiecas uz visu sakaru izlūkdatu "lielapjoma" vākšanu, tostarp saziņas uz Eiropu un no tās "lielapjoma" vākšanu, neapstiprinot vai nenoliedzot šādas vākšanas faktu.

Jūs lūdzāt arī sīkāku informāciju par Privātuma un pilsonisko brīvību pārraudzības padomi (PPBPP) un ģenerālinspektoriem, un to pilnvarām. PPBPP ir neatkarīga aģentūra izpildvaras ietvaros. Divu pušu izvirzītos piecus padomes locekļi ieceļ prezidents un apstiprina Senāts ([1]). Katrs Padomes loceklis ir iecelts uz sešu gadu termiņu. Padomes locekļiem un darbiniekiem ir atbilstoša drošības pielaide, lai tie varētu pilnībā īstenot savus likumā noteiktos pienākumus un pilnvaras ([2]).

PPBPP uzdevums ir nodrošināt, ka federālās valdības centieni novērst terorismu tiek līdzsvaroti ar nepieciešamību aizsargāt privāto dzīvi un pilsoniskās brīvības. Padomei ir divi pamatpienākumi – pārraudzība un padomu sniegšana. PPBPP nosaka savu darba kārtību un to, kādas pārraudzības un padomdevējas darbības tā vēlas veikt.

Pildot *pārraudzības* funkciju, PPBPP pārbauda un analizē izpildvaras darbības, ko ko tā veic, lai aizsargātu nāciju pret terorismu, nodrošinot, ka šādu pasākumu nepieciešamība tiek līdzsvarota ar nepieciešamību aizsargāt privāto dzīvi un pilsoniskās brīvības ([3]). PPBPP jaunākajā pārraudzības pārbaudē galvenā uzmanība bija vērsta uz uzraudzības programmām, ko ekspluatē saskaņā ar *FISA* 702. sadaļu ([4]). Pašlaik padome pārskata izlūkošanas darbības, ko veic saskaņā ar Izpildrīkojumu 12333 ([5]).

Pildot *padomdevējas* funkciju, PPBPP nodrošina, ka brīvība apsvērumi tiek pienācīgi ņemti vērā, izstrādājot un īstenojot normatīvos aktus un politiku saistībā ar centieniem aizsargāt nāciju no terorisma ([6]).

Lai veiktu savus uzdevumus, padomei ar likumu ir atļauta piekļuve visiem attiecīgo aģentūru reģistriem, ziņojumiem, revīziju materiāliem, pārskatiem, dokumentiem, materiāliem, ieteikumiem un citiem attiecīgiem materiāliem, tostarp klasificētai informācijai saskaņā ar tiesību aktiem ([7]). Turklāt padome Valde var izjautāt, nopratināt jebkuru izpildvaras amatpersonu vai darbinieku un pieņemt to oficiālas liecības ([8]). Turklāt padome var rakstiski pieprasīt, lai ģenerālprokurors padomes vārdā izdod pavēstes ar uzaicinājumu personām, kas nepieder pie izpildvaras, sniegt vajadzīgo informāciju ([9]).

Visbeidzot, PPBPP pilda likumā noteiktas pārredzamības prasības. Tas attiecas uz sabiedrības informēšanu par padomes darbību, atklātu izskatīšanu organizēšanu un tās ziņojumu publiskošanu, cik vien tas iespējams saskaņā ar klasificētas informācijas aizsardzības noteikumiem ([10]). Turklāt PPBPP ir jāziņo par gadījumiem, kad kāda izpildvaras aģentūra atsakās ņemt vērā tās ieteikumus.

Ģenerālinspektori (ĢI) izlūkdienestos (ID) veic revīzijas, inspekcijas, pārskatus par ID programmām un darbībām, lai apzinātu un novērstu sistēmiskus riskus, vājās vietas un nepilnības. Turklāt ĢI izmeklē sūdzības vai informāciju par iespējamiem tiesību aktu, noteikumu vai regulējuma pārkāpumiem vai nesaimniecisku rīcību; vērienīgu līdzekļu

([1]) *42 U.S.C. 2000ee(a), (h).*
([2]) *42 U.S.C. 2000ee(k).*
([3]) *42 U.S.C. 2000ee(d)(2).*
([4]) Sk. pamatā https://www.pclob.gov/library.html#oversightreports
([5]) Sk. pamatā https://www.pclob.gov/events/2015/may13.html
([6]) *42 U.S.C. 2000ee(d)(1); sk. arī PCLOB Advisory Function Policy and Procedure, Policy 2015-004, pieejama vietnē* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf
([7]) *42 U.S.C. 2000ee(g)(1)(A).*
([8]) *42 U.S.C. 2000ee(g)(1)(B).*
([9]) *42 U.S.C. 2000ee(g)(1)(D).*
([10]) *42 U.S.C. 2000eee(f).*

izšķērdēšanu; ļaunprātīgu pilnvaru izmantošanu vai būtisku un konkrētu apdraudējumu sabiedrības veselībai un drošībai ID programmās un darbībās. ĢI neatkarība ir būtisks elements katru ziņojuma, atzinuma un ieteikuma par IG jautājumiem objektivitātē un integritātē. Daži no svarīgākajiem elementiem, lai saglabātu ĢI neatkarību, ir IG iecelšanas un atcelšanas process; nodalītas darbības, budžeta un personāla pilnvaras; un dubultas ziņošanas prasības izpildvaras aģentūru vadītājiem un Kongresam.

Kongress ir izveidojis neatkarīgu ĢI biroju katrā izpildvaras aģentūras, tostarp katrā ID struktūrvienībā ([1]). Pēc likuma *Intelligence Authorization Act for Fiscal Year 2015* pieņemšanas gandrīz visus ĢI, kas pārrauga kādu ID struktūrvienību, ieceļ prezidents un apstiprina Senāts, tas attiecas arī uz Tieslietu ministriju, Centrālo izlūkošanas aģentūru, Nacionālās drošības aģentūru un izlūkdienestiem ([2]). Turklāt šie ĢI ir pastāvīgi, bezpartejiskai ierēdņi, kurus var atcelt tikai prezidents. Lai arī ASV konstitūcijā ir noteikts, ka prezidentam ir tiesības atcelt ĢI, tās reti ir tikušas izmantotas un paredz, ka prezidentam ir jāsniedz Kongresam rakstisks pamatojums 30 dienas pirms ĢI atcelšanas ([3]). Šis ĢI iecelšanas process nodrošina, ka izpildvaras amatpersonas nevar nepamatoti ietekmēt ĢI atlasi, iecelšanu amatā vai atcelšanu no amata.

Otrkārt, ĢI ir būtiskas ar likumu noteiktas pilnvaras veikt revīzijas, izmeklēšanu un pārskatīt programmas un darbības. Papildus izmeklēšanām saistībā ar pārraudzības un pārskatīšanām saskaņā ar likumu, ĢI ir plaša rīcības brīvība īstenot pārraudzības pilnvaras pēc to ieskatiem pārskatīt programmas un pasākumus ([4]). Īstenojot šīs pilnvaras, likums nodrošina, ka ĢI ir neatkarīgi resursi, lai varētu pildīt savus pienākumus, tostarp pilnvaras pieņemt darbā savus darbiniekus un atsevišķi iesniegt savus budžeta pieprasījumus Kongresam ([5]). Ar likumu nodrošināts, ka ĢI ir piekļuve informācijai, kas tiem vajadzīga savu pienākumu pildīšanai. Tas ietver tiesības uz tiešu piekļuvi visiem aģentūras reģistriem un detalizētai informāciju par aģentūras programmām un darbībām neatkarīgi no to klasifikācijas; tiesības pieprasīt informāciju un dokumentus; tiesības pieņemt zvērestus ([6]). Dažos gadījumos izpildvaras aģentūras vadītājs var aizliegt ĢI veikt kādu darbību, ja, piemēram, ĢI revīzija vai izmeklēšana būtiski ietekmētu ASV valsts drošības intereses. Taču arī šīs pilnvaras tiek izmantotas ļoti reti un tam nepieciešams, lai Aģentūras vadītājs 30 dienu laikā informē Kongresu par iemesliem šo pilnvaru izmantošanai. ([7]) Patiesi, Valsts izlūkošanas aģentūras direktors nekad nav izmantojis šīs tiesības ierobežot pilnvaras attiecībā uz kādu ĢI darbību.

Treškārt, ĢI ir pienākums pilnībā un aktuāli informēt izpildvaras aģentūras un Kongresa vadītājus, sniedzot ziņojumus par krāpšanu un citām nopietnām problēmām, pārkāpumiem, un nepilnībām, kas saistīti ar izpildvaras programmām un darbībām ([8]). Divkārša ziņošana atbalsta ĢI neatkarību, nodrošinot ĢI īstenotā pārraudzības procesa pārredzamību un aģentūru vadītājiem dodot iespēju īstenot ĢI ieteikumus, pirms Kongress var veikt likumdošanas darbības. Piemēram, ĢI ir ar likumu noteikts pienākums sagatavot pusgada ziņojumus, kuros aprakstītas šādas problēmas, kā arī līdz šim veiktie korektīvie pasākumi ([9]). Izpildvaras aģentūras nopietni izturas pret ĢI konstatējumiem un ieteikumiem, un bieži vien ĢI

([1]) *Sections 2 and 4 of the Inspector General Act of 1978*, ar grozījumiem (turpmāk"*IG Act*"); *Section 103H(b) and (e) of the National Security Act of 1947*, ar grozījumiem (turpmāk "*Nat'l Sec. Act*"); *Section 17(a) of the Central Intelligence Act* (turpmāk "*CIA Act*").

([2]) Sk. *Pub. L. No. 113-293, 128 Stat. 3990, (19.12.2014.)*. Tagad tikai Aizsardzības izlūkošanas aģentūras un Nacionālās ģeokosmosa izlūkaģentūras ĢI neieceļ prezidents; tomēr Aizsardzības ministrijas ĢI un ID ĢI ir vienlaicīga jurisdikcija attiecībā uz šīm aģentūrām.

([3]) *Section 3 of the IG Act of 1978*, ar grozījumiem; *Section 103H(c) of the Nat'l Sec. Act; Section 17(b) of the CIA Act*.

([4]) Sk. *Sections 4(a) and 6(a)(2) of the IG Act of 1947; Section 103H(e) and (g)(2)(A) of the Nat'l Sec. Act; Section 17(a) and (c) of the CIA Act*.

([5]) *Sections 3(d), 6(a)(7) and 6(f) of the IG Act; Sections 103H(d), (i), (j) and (m) of the Nat'l Sec. Act; Sections 17(e)(7) and (f) of the CIA Act*.

([6]) *Section 6(a)(1), (3), (4), (5), and (6) of the IG Act; Sections 103H(g)(2) of the Nat'l Sec. Act; Section 17(e)(1), (2), (4), and (5) of CIA Act*.

([7]) Sk., piemēram, *Sections 8(b) and 8E(a) of the IG Act; Section 103H(f) of the Nat'l Sec. Act; Section 17(b) of the CIA Act*.

([8]) *Section 4(a)(5) of the IG Act; Section 103H(a)(b)(3) and (4) of the Nat'l Sec. Act; Section 17(a)(2) and (4) of the CIA Act*.

([9]) *Section 2(3), 4(a), and 5 of the IG Act; Section 103H(k) of the Nat'l Sec. Act; Section 17(d) of the CIA Act*. Tieslietu ministrijas Ģenerālinspektora publiski pieejamie ziņojumi ir atrodami tīmekļa vietnē http://oig.justice.gov/reports/all.htm. Tāpat arī izlūkdienesta ģenerālinspektora pusgada ziņojumi ir publiski pieejami vietnē https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig

var iekļaut aģentūru apstiprinājumu par ĢI ieteikumu pieņemšanu un to īstenošanu šajos un citos ziņojumus Kongresam, un dažos gadījumos arī sabiedrībai ([1]). Papildus šai divkāršās ziņošanas struktūrai ĢI ir atbildīgi par izpildvaras ziņotāju novirzīšanu uz attiecīgo Kongresa Pārskata komiteju, kur tie sniegtu informāciju par iespējamu krāpšanu, izšķērēšanu, vai ļaunprātīgu izmantošanu saistībā ar izpildvaras programmām un darbībām. Ziņotāju identitāte ir aizsargāta pret atklāšanu izpildvarai, aizsargājot ziņotājus pret iespējamām aizliegtām ar personālu saistītām darbībām vai drošības pielaides darbībā, kas īstenotas kā represijas par ziņošanu ĢI ([2]). Tā kā ziņotāji bieži ir avots, no kura sākas ĢI izmeklēšana, iespēja viņiem ziņot par savām bažām tieši Kongresam un bez izpildvaras ietekmes palielina ĢI pārraudzības efektivitāti. Šīs neatkarības dēļ ĢI ar objektivitāti un integritāti var veicināt izpildvaras aģentūru ekonomiju, efektivitāti un pārskatatbildību.

Visbeidzot, Kongress ir izveidojis Ģenerālinspektoru integritātes un efektivitātes padomi. Šī padome, cita starpā, izstrādā ĢI revīziju, izmeklēšanu un pārskatu standartus; veicina apmācību; un ir pilnvarota veikt pārbaudes par iespējamiem ĢI pārkāpumiem, tādējādi pildot kritiska uzrauga lomu attiecībā uz ĢI, kuriem uzticēts pārraudzīt citus. ([3])

Ceram, ka šī informācija ir Jums noderīga.

Ar cieņu
Robert S. Litt,
Galvenais juriskonsults

([1]) *Section 2(3), 4(a), and 5 of the IG Act; Section 103H(k) of the Nat'l Sec. Act; Section 17(d) of the CIA Act*. Tieslietu ministrijas Ģenerālinspektora publiski pieejamie ziņojumi ir atrodami tīmekļa vietnē http://oig.justice.gov/reports/all.htm. Tāpat arī izlūkdienesta ģenerālinspektora pusgada ziņojumi ir publiski pieejami vietnē https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig

([2]) *Section 7 of the IG Act; Section 103H(g)(3) of the Nat'l Sec. Act; Section 17(e)(3) of the CIA Act.*

([3]) *Section 11 of the IG Act*.

VII PIELIKUMS

Vēstule no ģenerālprokurora vietnieka un starptautisko lietu padomnieka *Bruce Swartz* (ASV Tieslietu ministrija)

2016. gada 19. februārī

Juriskonsultam
Justin S. Antonipillai
ASV Tirdzniecības ministrija
1401 Constitution Ave., NW
Washington, DC 20230

Ministra vietniekam
Ted Dean
Starptautiskās tirdzniecības administrācija
1401 Constitution Ave., NW
Washington, DC 20230

Godātais *Antonipillai* kungs un godātais *Dean* kungs!

Šajā vēstulē ir sniegts īss pārskats par galvenajiem izmeklēšanas instrumentiem, ko izmanto, lai krimināltiesību piemērošanas vai sabiedrības interešu (civiltiesisku un regulatīvu) ievērošanas nolūkos iegūtu no Amerikas Savienoto Valstu uzņēmumiem komercdatus un citu reģistrēto informāciju, tostarp izklāstīti ar šīm pilnvarām saistītie piekļuves ierobežojumi ([1]). Šie juridiskie procesi ir nediskriminējoši, proti, tos izmanto, lai no Amerikas Savienoto Valstu uzņēmumiem, arī tādiem, kas pašsertificēs ASV un ES privātuma vairoga regulējuma ievērošanu, iegūtu informāciju neatkarīgi no datu subjekta valstspiederības. Turklāt, kā aprakstīts turpmāk, uzņēmumi, pret kuriem Amerikas Savienotajās Valstīs tiek vērsts juridiskais process, to var apstrīdēt tiesā ([2]).

Saistībā ar publisko iestāžu veiktu datu konfiscēšanu īpaši jānorāda uz Amerikas Savienoto Valstu Konstitūcijas Ceturto labojumu, kurā noteikts, ka "[n]av pārkāpjamas cilvēku tiesības uz personas aizsardzību, viņu māju, dokumentu un īpašuma aizsardzību no nepamatotām kratīšanām un aresta. Kratīšanas un aresta orderi var izdot tikai pietiekami pamatotā gadījumā, ko apstiprina zvērests vai svinīgs solījums. Šādā orderī jābūt kratīšanas vietas un arestējamās personas vai mantas sīkam aprakstam." ASV Konstitūcijas 4. labojums. Kā spriedumā lietā *Berger pret Ņujorkas štatu* norādīja Amerikas Savienoto Valstu Augstākā tiesa, "[š]ā labojuma galvenais mērķis, kā atzīts ļoti daudzos šīs tiesas nolēmumos, ir aizsargāt indivīdu privātumu un drošību pret valdības amatpersonu patvaļīgu iejaukšanos." *388 U.S. 41, 53 (1967)* (*citing Camara v. Mun. Court of San Francisco, 387 U.S. 523, 528 (1967)*). Attiecībā uz iekšzemes kriminālizmeklēšanu Ceturtais labojums parasti nozīmē to, ka tiesībaizsardzības darbiniekiem pirms kratīšanas ir jāsaņem tiesas izsniegts orderis. *Sk. Katz v. United States, 389 U.S. 347, 357 (1967).* Ja prasību par orderi nepiemēro, uz valdības darbību saskaņā ar Ceturto labojumu attiecina "saprātīguma" kritēriju. Tādējādi jau saskaņā ar Konstitūciju vien ASV valdībai nav neierobežotu vai patvaļīgu pilnvaru konfiscēt privātu informāciju.

Krimināltiesību piemērošanas pilnvaras

Federālie prokurori, kas ir Tieslietu ministrijas (TM) amatpersonas, un federālie izmeklēšanas aģenti, arī Federālā izmeklēšanas biroja (FIB) – TM tiesībaizsardzības aģentūras – aģenti var likt Amerikas Savienoto Valstu uzņēmumiem sagatavot dokumentus un citu reģistrētu informāciju kriminālizmeklēšanas vajadzībām, īstenojot dažādus obligātos

([1]) Šajā pārskatā nav aprakstīti valsts drošības izmeklēšanas instrumenti, ko tiesībaizsardzības iestādes izmanto terorisma un citās ar valsts drošību saistītās izmeklēšanās, tostarp vēstules par valsts drošību (*NSL*), ko iesniedz, lai iegūtu konkrētu informāciju no kredītu pārskatiem, finanšu pārskatiem, elektronisko abonentu un darījumu pārskatiem (sk. *12 U.S.C. § 3414*; *15 U.S.C. § 1681u*; *15 U.S.C. § 1681v*; *18 U.S.C. § 2709*, un attiecībā uz elektronisku novērošanu, kratīšanas orderi, uzņēmumu datiem un citu sakaru informācijas vākšanu, ko veic saskaņā ar Ārējās izlūkošanas un novērošanas likumu (sk. *50 U.S.C. § 1801* un turpm. sadaļas).

([2]) Šajā dokumentā ir aplūkotas federālās tiesībaizsardzības un regulatīvās pilnvaras; štata tiesību aktu pārkāpumus izmeklē attiecīgie štati un iztiesā štata tiesās. Štatu tiesībaizsardzības iestādes izmanto orderus un pavēstes, ko izsniedz saskaņā ar štata tiesību aktiem un pamatā tādā pašā veidā, kā aprakstīts šajā dokumentā, taču pastāv iespēja, ka uz štata juridisko procesu var attiekties štata konstitūcijā piešķirta aizsardzība, kas ir plašāka par ASV Konstitūcijā garantēto. Štatu tiesību aktos paredzētajai aizsardzībai jābūt vismaz līdzvērtīgai tai, kas paredzēta ASV konstitūcijā, tai skaitā (bet neaprobežojoties) ar ceturto labojumu.

juridiskos procesus, tostarp, iesniedzot zvērināto pavēstes, administratīvās pavēstes un kratīšanas orderus, kā arī iegūt citu sakaru informāciju, īstenojot federālās kriminālnoziedznieku noklausīšanās un zvanīto tālruņa numuru reģistrētāja izmantošanas pilnvaras.

Zvērināto vai tiesas pavēstes. Kriminālpavēstes izmanto, lai veicinātu mērķtiecīgas tiesībaizsardzības iestāžu izmeklēšanas. Zvērināto pavēste ir oficiāls zvērināto pieprasījums (parasti to izsniedz pēc federālā prokurora pieprasījuma), kas sekmē zvērināto veikto izmeklēšanu par konkrētu iespējamu krimināltiesību pārkāpumu. Lielā žūrija ir tiesas izmeklēšanas atzars, un tās sastāvu izvēlas tiesnesis vai miertiesnesis. Pavēstē var pieprasīt kādam liecināt tiesas procesā vai sagatavot vai darīt pieejamu uzņēmuma informāciju, elektroniski glabātu informāciju vai citus materiālus vienumus. Informācijai jābūt saistītai ar izmeklēšanu, un pavēste nedrīkst būt atzīstama par nesamērīgu, jo ir, piemēram, pārāk vispārīga vai patvaļīga, vai apgrūtinoša. Pavēstes saņēmējs, pamatojoties uz šiem faktoriem, var pavēsti apstrīdēt. *Sk. Fed. R. Crim. P. 17*. Ierobežotos apstākļos, kad zverinātie ir izvirzījuši lietā apsūdzību, dokumentu ieguvei var izmantot tiesas pavēstes.

Administratīvās pavēstes izmantošanas pilnvaras. Administratīvās pavēstes var izmantot krimināllietu un civillietu izmeklēšanās. Krimināltiesību piemērošanas kontekstā vairākos federālajos likumos ir atļauts izmantot administratīvās pavēstes, lai panāktu, ka tiek sagatavota vai darīta pieejama uzņēmumu informācija, elektroniski glabāta informācija vai citi materiāli vienumi, ko izmantot izmeklēšanās par krāpšanu veselības aprūpes jomā, vardarbīgu izturēšanos pret bērnu, slepenā dienesta aizsardzību, ar kontrolējamām vielām saistītām lietām un ģenerālinspektora veiktajās izmeklēšanās, kurās ir iesaistītas valdības aģentūras. Ja valdība cenšas panākt administratīvās pavēstes izpildi tiesā, tās, tāpat kā zvērināto pavēstes, saņēmējs var iebilst, ka pavēste ir nesamērīga, jo ir pārāk vispārīga vai patvaļīga, vai apgrūtinoša.

Tiesu rīkojumi par zvanīto numuru reģistrētāju un uztveršanas un trasēšanas ierīču izmantošanu. Saskaņā ar krimināltiesību noteikumiem par zvanīto numuru reģistrētāja un uztveršanas un trasēšanas ierīču izmantošanu, tiesībaizsardzības iestāde var saņemt tiesas rīkojumu, lai iegūtu reāllaika, nesatura zvanīšanas, maršrutēšanas, adresēšanas un sakaru datus par tālruņa numuru vai e-pasta adresi, apliecinot, ka sniegtā informācija ir vajadzīga notiekošajā krimināllizmeklēšanā. Sk. *18 U.S.C. §§ 3121-3127*. Šādas ierīces izmantošana vai uzstādīšana pretrunā tiesību aktiem ir federāls noziegums.

Elektroniskās saziņas privātuma likums (*ECPA*). Valdības piekļuvi abonentu informācijai, datplūsmas datiem un IPS tālruņu pakalpojumu uzņēmumu un citu pakalpojumu sniedzēju, kuri ir trešās personas, glabātajam sakaru saturam reglamentē papildu noteikumi, kas ir paredzēti *ECPA* – dēvēts arī par Saglabāto ziņojumu likumu (*Stored Communications Act* – *SCA*) – II daļā (*18 U.S.C. §§ 2701–2712*). *SCA* ir noteikta likumisko privātuma tiesību aizsardzības sistēma, kas ierobežo tiesībaizsardzības iestāžu piekļuvi datiem, kas nav tie dati, kuri interneta pakalpojumu sniedzēju klientiem un abonentiem jānorāda saskaņā ar konstitucionālajām tiesībām. *SCA* ir paredzēts pieaugošs privātuma aizsardzības līmenis, kas ir atkarīgs no tā, cik lielā mērā informācijas vākšana aizskar personas privātumu. Lai iegūtu abonentu reģistrācijas informāciju, IP adreses un saistītos laikspiedolus, kā arī norēķinu informāciju, krimināltiesību piemērošanas iestādēm ir vajadzīga pavēste. Attiecībā uz vairumu pārējās glabātās nesatura informācijas, piemēram, e-vēstuļu galvenēm bez tēmas rindiņas, tiesībaizsardzības iestādēm ir jāizklāsta tiesnesim konkrēti fakti, kas parāda, ka prasītā informācija ir saistīta ar notiekošo krimināllizmeklēšanu un tajā būtiski nepieciešama. Lai iegūtu glabātās elektroniskās saziņas saturu, krimināltiesību piemērošanas iestādes parasti saņem no tiesneša attiecīgu orderi, pamatojoties uz ticamu iemeslu uzskatīt, ka konkrētajā kontā ir pierādījumi par noziegumu. *SCA* ir paredzēta arī civiltiesiskā atbildība un krimināls odi.

Tiesu rīkojumi par novērošanu saskaņā ar Federālo Likumu par telefona sarunu noklausīšanos. Papildus iepriekš minētajam atbilstīgi federālajiem tiesību aktiem par telefona sarunu noklausīšanos tiesībaizsardzības iestādes ar krimināllizmeklēšanu saistītos nolūkos var reāllaikā pārtvert tālruņa, mutisko vai elektronisko saziņu. Sk. *18 U.S.C. §§ 2510-2522*. Šīs pilnvaras var izmantot vienīgi saskaņā ar tiesas rīkojumu, kurā tiesnesis *inter alia* konstatē, ka pastāv pamatots iemesls uzskatīt, ka sarunu noklausīšanās vai elektroniskās saziņas pārtveršana nodrošinās pierādījumus par federālu

noziegumu vai informāciju par personas, kura izvairās no kriminālvajāšanas, atrašanās vietu. Attiecīgajā likumā ir paredzēta civiltiesiskā atbildība un krimināsodi par sarunu noklausīšanās noteikumu pārkāpumiem.

Kratīšanas orderis – 41. noteikums. Tiesībaizsardzības iestādes Amerikas Savienotajās Valstīs var fiziski pārmeklēt telpas, ja ir saņēmušas attiecīgu tiesneša atļauju. Tiesībaizsardzības iestādēm, norādot "pamatotu iemeslu", ir jāpierāda tiesnesim, ka noziegums tika vai tiks izdarīts un ka ar noziegumu saistītie vienumi, iespējams, ir atrodami orderī precizētajā vietā. Šīs pilnvaras nereti izmanto, kad policijai telpas jāpārmeklē fiziski, jo pastāv risks, ka pierādījumus varētu iznīcināt, ja pavēsti vai citu informācijas sniegšanas rīkojumu adresēs uzņēmumam. Sk. ASV Konstitūcijas 4. labojumu. (sīkāk aprakstīts iepriekš), *Fed. R. Crim. P. 41*. Kratīšanas ordera subjekts var iesniegt tā anulēšanas prasību, pamatojoties uz to, ka orderis ir pārāk vispārīgs, apgrūtinošs vai citādi neatbilstoši iegūts, un cietušās puses, kam ir procesuālā tiesībspēja, var pieprasīt visu nelikumīgā kratīšanā iegūto pierādījumu neizmantošanu. *Sk. Mapp v. Ohio, 367 U.S. 643 (1961).*

TM pamatnostādnes un politika. Papildus aprakstītajiem konstitucionālajiem, likumiskajiem un noteikumos pamatotajiem ierobežojumiem, kas valdībai jāievēro saistībā ar piekļuvi datiem, ģenerālprokurors ir pieņēmis pamatnostādnes, kurās ir paredzēti papildu ierobežojumi attiecībā uz tiesībaizsardzības iestāžu piekļuvi datiem un noteikti arī privātuma un pilsonisko brīvību aizsardzības pasākumi. Piemēram, ģenerālprokurora izstrādātajās pamatnostādnēs par Federālā izmeklēšanas biroja iekšzemes operācijām (2008. gada septembris) (turpmāk "ĢP FIB" pamatnostādnes) – pieejamas vietnē http://www.justice.gov/archive/opa/docs/guidelines.pdf, ir ierobežota izmeklēšanas līdzekļu izmantošana, lai meklētu ar federālu noziegumu izmeklēšanu saistītu informāciju. Pamatnostādnēs ir noteikts, ka FIB jāizmanto visneuzbāzīgākās praksē iespējamās izmeklēšanas metodes, ņemot vērā to ietekmi uz privātumu un pilsoniskajām brīvībām un kaitējumu, ko tās var nodarīt reputācijai. Nostādnēs arī norādīts, ka: "ir pašsaprotami, ka FIB veic izmeklēšanas un citas darbības likumīgā un samērīgā veidā, ievērojot brīvību un privātumu un nepieļaujot nevajadzīgu iejaukšanos likumam pakļāvīgu cilvēku dzīvē." *Sk. AG FBI Guidelines at 5*. FIB ir īstenojusi minētās pamatnostādnes ar FIB iekšzemes izmeklēšanas un operāciju rokasgrāmatu (*DIOG*), pieejama https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), – visaptveroša rokasgrāmata, kurā ietverti sīki izstrādāti ierobežojumi izmeklēšanas rīku izmantošanai un norādījumi, lai nodrošinātu, ka pilsoņu brīvības un privātums tiek aizsargāti ikvienā izmeklēšanā. Papildu noteikumi un politika, no kā izriet federālo prokuroru izmeklēšanas darbību ierobežojumi, ir izklāstīti **Amerikas Savienoto Valstu Prokuroru rokasgrāmatā** (*USAM*), kas ir pieejama arī tiešsaistē http://www.justice.gov/usam/united-states-attorneys-manual

Civiltiesiskās un regulatīvās pilnvaras (sabiedrības intereses).

Pastāv arī būtiski ierobežojumi attiecībā uz piekļuvi Amerikas Savienoto Valstu uzņēmumu glabātajiem datiem civiltiesisku vai regulatīvu (t. i., ar "sabiedrības interesēm" saistītu) apsvērumu dēļ. Aģentūras, kam ir civiltiesiski un regulatīvi pienākumi, var izsniegt uzņēmumiem pavēstes, kurās pieprasa uzņēmumu informāciju, elektroniski glabātu informāciju vai citus materiālus vienumus. Šo aģentūru pilnvaras izmantot administratīvās vai civiltiesiskās pavēstes ierobežo ne tikai to izveides likumi, bet arī pavēstu izskatīšana neatkarīgā tiesā pirms to iespējamās tiesiskās izpildes. Sk., piemēram, *Fed. R. Civ. P. 45*. Aģentūras var mēģināt piekļūt vienīgi datiem par tādām lietām, kas saistītas ar to regulatīvo pilnvaru darbības jomu. Turklāt administratīvās pavēstes saņēmējs var apstrīdēt šīs pavēstes izpildi tiesā, iesniedzot pierādījumus par to, ka aģentūra nav rīkojusies atbilstīgi iepriekš aprakstītajam samērīguma pamatprincipam.

Uzņēmumi, ņemot vērā savas nozares specifiku un to rīcībā esošo datu veidus, var apstrīdēt no administratīvajām aģentūrām saņemtos datu pieprasījumus, arī atsaucoties uz citiem juridiskajiem pamatiem. Piemēram, finanšu iestādes var apstrīdēt administratīvās pavēstes, kurās prasīts sniegt konkrētu informācijas veidu, norādot, ka tās ir pretrunā Banku slepenības likumam (*Bank Secrecy Act*) un tā īstenošanas noteikumiem. Sk. *31 U.S.C. § 5318, 31 C.F.R. Part X*. Citi uzņēmumi var paļauties uz *Fair Credit Reporting Act*, sk. *15 U.S.C. § 1681b*, vai citiem nozaru aktiem. Sk., piemēram, Likumu par tiesībām uz finansiālo privātumu (Right to Financial Privacy Act), U.S.C. Sk., piemēram, *Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422*. Tādējādi Amerikas Savienoto Valstu tiesas nodrošina aizsardzību pret nepamatotiem regulatīviem pieprasījumiem un neatkarīgi pārrauga federālo aģentūru rīcību.

Visbeidzot, visas administratīvo iestāžu likumiskās pilnvaras pēc administratīvas kratīšanas fiziski konfiscēt Amerikas Savienoto Valstu uzņēmuma informāciju ir jāīsteno, ievērojot Konstitūcijas Ceturtā labojuma prasības. Sk. *See v. City of Seattle, 387 U.S. 541 (1967).*

Secinājumi

Visām Amerikas Savienotajās Valstīs īstenotajām tiesībaizsardzības un regulatīvajām darbībām ir jāatbilst piemērojamiem tiesību aktiem, tostarp ASV Konstitūcijai, normatīvajiem aktiem un noteikumiem. Šīs darbības arī jāveic saskaņā ar piemērojamo politiku, tostarp visām ģenerālprokurora pamatnostādnēm, kas reglamentē federālās tiesībaizsardzības darbības. Iepriekš aprakstītais tiesiskais regulējums ierobežo ASV tiesībaizsardzības un regulatīvo aģentūru spēju iegūt informāciju no Amerikas Savienoto Valstu uzņēmumiem – neatkarīgi no tā, vai dati attiecas uz ASV vai citu valstu pilsoņiem –, kā arī sniedz iespēju izskatīt tiesā visus datu pieprasījumus, ko valdība iesniegusi atbilstīgi šīm pilnvarām.

Ar cieņu

Ģenerālprokurora vietnieks un starptautisko lietu padomnieks

Bruce C. Swartz