# KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2023/1795

**(2023. gada 10. jūlijs)**

**kas pieņemts, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, par personas datu pietiekamu aizsardzības līmeni ES un ASV datu privātuma regulējuma ietvaros**

*(izziņots ar dokumenta numuru C(2023) 4745)*

**(Dokuments attiecas uz EEZ)**

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) 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) ([1]), un jo īpaši tās 45. panta 3. punktu,

tā kā:

## 1. IEVADS

(1) Ar Regulu (ES) 2016/679 ([2]) ir paredzēti noteikumi, saskaņā ar kuriem Savienībā esoši pārziņi vai apstrādātāji var nosūtīt personas datus trešām valstīm un starptautiskām organizācijām, ciktāl šāda nosūtīšana ietilpst regulas piemērošanas jomā. Noteikumi par datu starptautisko nosūtīšanu ir izklāstīti minētās regulas V nodaļā. Lai gan personas datu plūsma uz valstīm ārpus Eiropas Savienības un no tām ir būtiska pārrobežu tirdzniecības un starptautiskās sadarbības paplašināšanas nodrošināšanai, datu nosūtīšana uz trešām valstīm vai starptautiskām organizācijām nedrīkst samazināt Savienībā nodrošināto personas datu aizsardzības līmeni ([3]).

(2) Atbilstīgi Regulas (ES) 2016/679 45. panta 3. punktam Komisija ar īstenošanas aktu var nolemt, ka trešā valsts, trešās valsts teritorija vai viens vai vairāki konkrēti sektori nodrošina pietiekamu aizsardzības līmeni. Saskaņā ar šo nosacījumu personas datus var nosūtīt uz trešo valsti bez nepieciešamības saņemt jebkādu turpmāku atļauju, kā paredzēts Regulas (ES) 2016/679 45. panta 1. punktā un 103. apsvērumā.

(3) Kā norādīts Regulas (ES) 2016/679 45. panta 2. punktā, lēmums par aizsardzības līmeņa pietiekamību jāpieņem, pamatojoties uz visaptverošu trešās valsts tiesību sistēmas analīzi, gan attiecībā uz noteikumiem, kas piemērojami datu saņēmējiem, gan attiecībā uz ierobežojumiem un garantijām saistībā ar publisko iestāžu piekļuvi personas datiem. Komisijai novērtējumā jānosaka, vai attiecīgā trešā valsts garantē aizsardzības līmeni, kurš "pēc būtības ir līdzvērtīgs" Savienībā nodrošinātajam (Regulas (ES) 2016/679 104. apsvērums). Vai tas tā ir, ir jāvērtē, ņemot vērā Savienības tiesību aktus, jo īpaši Regulu (ES) 2016/679, kā arī Eiropas Savienības Tiesas (Tiesas) judikatūru ([4]).

([1]) OV L 119, 4.5.2016., 1. lpp.
([2]) Vienkāršības labad šajā lēmumā izmantoto saīsinājumu saraksts ir dots VIII pielikumā.
([3]) Sk. Regulas (ES) 2016/679 101. apsvērumu.
([4]) Sk. spriedumu jaunākajā lietā C-311/18 *Facebook Ireland* un *Schrems* (*Schrems II*), ECLI:EU:C:2020:559.

(4) Kā Tiesa paskaidroja 2015. gada 6. oktobra spriedumā lietā C-362/14 *Maximillian Schrems / Data Protection Commissioner* ([5]) *(Schrems)*, nav jākonstatē identisks aizsardzības līmenis. Konkrēti, attiecīgās trešās valsts izmantotie līdzekļi personas datu aizsardzībai var atšķirties no Savienībā izmantotajiem, ja vien tie praksē efektīvi nodrošina pietiekamu aizsardzības līmeni ([6]). Tāpēc aizsardzības līmeņa pietiekamības standarts neparedz Savienības noteikumu precīzu atkārtošanu. Drīzāk ir jāpārbauda, vai attiecīgās valsts tiesību sistēma spēj nodrošināt nepieciešamo aizsardzības līmeni, ņemot vērā tiesību uz privātumu būtību un to efektīvu īstenošanu, uzraudzību un izpildi ([7]). Turklāt saskaņā ar minēto spriedumu, piemērojot šo standartu, Komisijai jo īpaši būtu jānovērtē, vai attiecīgās trešās valsts tiesiskajā regulējumā ir paredzēti noteikumi, kuru mērķis ir ierobežot iespējamo iejaukšanos to personu pamattiesībās, kuru dati no Savienības ir nosūtīti uz attiecīgo valsti, – iejaukšanos, ko šīs valsts struktūras ir tiesīgas praktizēt, ja tā kalpo leģitīmam mērķim (piemēram, nacionālā drošība) un vai ir nodrošināta efektīva tiesiskā aizsardzība pret šāda veida iejaukšanos ([8]). Šajā saistībā norādījumi sniegti arī Eiropas Datu aizsardzības kolēģijas Pietiekamības atsaucēs, kuru mērķis ir sīkāk precizēt šo standartu ([9]).

(5) Piemērojamo standartu attiecībā uz šādu iejaukšanos pamattiesībās uz privātumu un datu aizsardzību Tiesa precizēja 2020. gada 16. jūlija spriedumā lietā C-311/18 *Data Protection Commissioner | Facebook Ireland Limited and Maximillian Schrems* (*"Schrems II"*), ar kuru tika atzīts par spēkā neesošu Komisijas Īstenošanas lēmums (ES) 2016/1250 ([10]) par iepriekšējo transatlantisko datu plūsmas sistēmu – ES un ASV privātuma vairogu (privātuma vairogs). Tiesa uzskatīja, ka personas datu aizsardzības ierobežojumi, kas izriet no ASV iekšējā tiesiskā regulējuma par ASV publisko iestāžu piekļuvi no Savienības uz Amerikas Savienotajām Valstīm drošības nolūkos nosūtītiem personas datiem un šādu datu izmantošanu, nav ierobežoti tādā veidā, lai atbilstu prasībām, kas būtībā ir līdzvērtīgas tām, kuras Savienības tiesību aktos ir izvirzītas attiecībā uz šādu iejaukšanos tiesībās uz datu aizsardzību nepieciešamību un samērīgumu ([11]). Tiesa arī uzskatīja, ka tas nesniedz iestādē izmantojamus tiesību aizsardzības līdzekļus, kas personām, kuru dati tiek nosūtīti uz ASV, sniegtu garantijas, kas būtībā ir līdzvērtīgas tām, kuras ir prasītas Hartas 47. pantā par tiesībām uz efektīvu tiesību aizsardzību ([12]).

(6) Pēc sprieduma lietā *Schrems II* Komisija uzsāka sarunas ar ASV valdību par iespējamu jaunu lēmumu par aizsardzības līmeņa pietiekamību, kas atbilstu Regulas (ES) 2016/679 45. panta 2. punkta prasībām, kā to interpretējusi Tiesa. Šo diskusiju rezultātā ASV 2022. gada 7. oktobrī pieņēma izpildrīkojumu Nr. 14086 "Drošības pasākumu uzlabošana ASV sakaru izlūkošanas darbībām" (IR Nr. 14086), ko papildina ASV Ģenerālprokurora izdotie noteikumi par Datu aizsardzības pārskatīšanas tiesu ("ĢP noteikumi") ([13]). Turklāt ir atjaunināts regulējums, kas attiecas uz komercsabiedrībām, kuras apstrādā datus, kas nosūtīti no Savienības saskaņā ar šo lēmumu, – "ES un ASV datu privātuma regulējums" ("ES un ASV DPR" jeb "DPR").

(7) Komisija ir rūpīgi izvērtējusi ASV tiesību aktus un praksi, tajā skaitā IR Nr. 14086 un ĢP noteikumus. Pamatojoties uz konstatējumiem, kas izklāstīti 9.–200. apsvērumā, Komisija secina, ka Amerikas Savienotās Valstis nodrošina pietiekamu to personas datu aizsardzības līmeni, kas no Savienībā esoša pārziņa vai apstrādātāja ([14]) tiek nosūtīti sertificētām Amerikas Savienoto Valstu organizācijām saskaņā ar ES un ASV DPR.

([5]) Lieta C-362/14 *Maximillian Schrems|Data Protection Commissioner* ("Schrems"), ECLI:EU:C:2015:650, 73. punkts.

([6]) *Schrems*, 74. punkts.

([7]) Sk. Komisijas paziņojumu Eiropas Parlamentam un Padomei "Apmaiņa ar personas datiem un šo datu aizsardzība globalizētā pasaulē", COM(2017) 7, 10.1.2017., 3.1. iedaļa, 6. un 7. lpp.

([8]) *Schrems*, 88. un 89. punkts.

([9]) Eiropas Datu aizsardzības kolēģija, Pietiekamības atsauces, WP 254 rev.01, pieejamas https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) 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 (OV L 207, 1.8.2016., 1. lpp.).

([11]) *Schrems II*, 185. punkts.

([12]) *Schrems II*, 197. punkts.

([13]) *CFR* 28. sadaļas 302. daļa.

([14]) Šis lēmums attiecas uz EEZ. Līgumā par Eiropas Ekonomikas zonu (EEZ līgums) paredzēta Eiropas Savienības iekšējā tirgus paplašināšana, iekļaujot trīs EEZ valstis: Islandi, Lihtenšteinu un Norvēģiju. EEZ Apvienotā komiteja 2018. gada 6. jūlijā pieņēma Apvienotās komitejas lēmumu, ar ko Regulu (ES) 2016/679 iekļauj EEZ līguma XI pielikumā, un tas stājās spēkā 2018. gada 20. jūlijā. Tādējādi uz regulu attiecas minētais līgums. Tāpēc šajā lēmumā atsauces uz ES un ES dalībvalstīm ir jāsaprot arī kā atsauces uz EEZ valstīm.

(8) Saskaņā ar šo lēmumu nav jāsaņem nekāda turpmāka atļauja datu nosūtīšanai no Savienībā iedibinātiem pārziņiem un apstrādātājiem ([15]) sertificētām organizācijām ASV. Tas neietekmē Regulas (ES) 2016/679 tiešu piemērošanu šādām organizācijām, ja ir izpildīti minētās regulas 3. pantā paredzētie nosacījumi attiecībā uz tās teritoriālo darbības jomu.

## 2. ES UN ASV DATU PRIVĀTUMA REGULĒJUMS

### 2.1. Personīgā un materiālā piemērošanas joma

#### 2.1.1. *Sertificētās organizācijas*

(9) ES un ASV DPR pamatā ir sertifikācijas sistēma, kuras ietvaros organizācijas ASV apņemas ievērot ASV Tirdzniecības ministrijas (*DoC*) izdoto un šā lēmuma I pielikumā iekļauto privātuma principu kopumu – ES un ASV datu privātuma regulējumu, ieskaitot papildprincipus (kopā saukti "Principi") ([16]). Lai varētu saņemt sertifikāciju saskaņā ar ES un ASV DPR, uz organizāciju jāattiecina Federālās tirdzniecības komisijas (*FTC*) vai ASV Satiksmes ministrijas (*DoT*) izmeklēšanas un izpildes pilnvaras ([17]). DPR principus sāk piemērot uzreiz pēc sertifikācijas. Kā sīkāk paskaidrots 48.–52. apsvērumā, ES un ASV DPR organizācijām katru gadu ir atkārtoti jāiegūst sertifikācija, ka tās ievēro DPR principus ([18]).

#### 2.1.2. *Jēdzienu "personas dati", "pārzinis" un "pārstāvis" definīcijas*

(10) Aizsardzība, ko nodrošina ES un ASV DPR attiecas uz visiem personas datiem, kas no Savienības tiek nosūtīti ASV esošām organizācijām, kuras ir apliecinājušas, ka atbilst DPR principiem *DoC*, izņemot datus, kas ir savākti publicēšanai, pārraidīšanai vai citām žurnālistikas materiālu publiskas paziņošanas formām, kā arī informāciju iepriekš publicētos materiālos, kas tiek izplatīti no mediju arhīviem ([19]). Tāpēc šādu informāciju nevar nosūtīt, pamatojoties uz ES un ASV DPR.

(11) DPR principos personas dati ir definēti tāpat kā Regulā (ES) 2016/679, t. i., kā "jebkādā formā reģistrēti dati, kas attiecas uz identificētu vai identificējamu personu, kura ietilpst VDAR darbības jomā un ko organizācija Amerikas Savienotajās Valstīs ir saņēmusi no ES." ([20]) Attiecīgi tie attiecas arī uz pseidonimizētiem (jeb ar šifru kodētiem) pētniecības datiem (arī gadījumos, kad atslēga netiek izpausta ASV saņēmējai organizācijai) ([21]). Tāpat personas datu "apstrāde" ir definēta kā "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." ([22])

(12) ES un ASV DPR attiecas uz organizācijām ASV, kas kvalificējamas kā pārziņi (t. i., kā persona vai organizācija, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus) ([23]) vai apstrādātāji (t. i., pārstāvji, kas darbojas pārziņa vārdā) ([24]). ASV iedibinātiem apstrādātājiem ir jābūt līgumiski saistītiem rīkoties tikai saskaņā ar ES pārziņa norādījumiem un palīdzēt tam sniegt atbildes fiziskām personām, kas īsteno savas tiesības

([15]) Šis lēmums neietekmē Regulas (ES) 2016/679 prasības, kas attiecas uz Savienībā iedibinātām vienībām (pārziņiem un apstrādātājiem), kuras nosūta datus, piemēram, par apstrādes nolūka ierobežošanu, datu minimizēšanu, pārredzamību un datu drošību (sk. arī Regulas (ES) 2016/679 44. pantu).

([16]) Šajā sakarā sk. sprieduma *Schrems* 81. punktu, kurā Tiesa apstiprināja, ka pašsertifikācijas sistēma var nodrošināt pietiekamu aizsardzības līmeni.

([17]) I pielikuma I.2. iedaļa. *FTC* ir plaša jurisdikcija tirdzniecības jautājumos ar atsevišķiem izņēmumiem, piemēram, attiecībā uz bankām, aviosabiedrībām, apdrošināšanas nozari un telekomunikāciju pakalpojumu sniedzēju kopējām operatoru darbībām (lai arī ASV Devītā apgabala apelācijas tiesa 2018. gada 26. februāra lēmumā lietā *FTC / AT&T* apstiprināja, ka *FTC* ir jurisdikcija attiecībā uz šādu uzņēmumu darbībām, kas nav kopējās operatoru darbības). Sk. arī IV pielikuma 2. zemsvītras piezīmi. *DoT* ir kompetence nodrošināt aviosabiedrību un biļešu pārdevēju (gaisa transporta jomā) atbilstību. Sk. V pielikuma A iedaļu.

([18]) I pielikuma III.6. iedaļa.

([19]) I pielikuma III.2. iedaļa.

([20]) I pielikuma I.8.a iedaļa.

([21]) I pielikuma III.14.g iedaļa.

([22]) I pielikuma I.8.b iedaļa.

([23]) I pielikuma I.8.c iedaļa.

([24]) Sk., piemēram, I pielikuma II.2.b. iedaļu un II.3.b. un 7.d. iedaļu, kur ir skaidri norādīts, ka pārstāvji rīkojas pārziņa vārdā saskaņā ar tā norādījumiem un konkrētām līgumsaistībām.

atbilstoši DPR principiem ([25]). Turklāt, ja apstrādi veic apakšuzņēmums, apstrādātājam ir jānoslēdz līgums ar apakšapstrādātāju, kas garantē tādu pašu aizsardzības līmeni, ko nodrošina DPR principi, un jāveic darbības, lai nodrošinātu tā pienācīgu īstenošanu ([26]).

### 2.2. **ES un ASV datu privātuma regulējuma principi**

#### 2.2.1. ***Nolūka ierobežojums un izvēle***

(13) Personas dati būtu jāapstrādā likumīgi un godprātīgi. Personas dati būtu jāvāc konkrētā nolūkā un pēc tam tos var izmantot, ja šāda izmantošana nav nesaderīga ar apstrādes nolūku.

(14) Saskaņā ar ES un ASV DPR tas tiek nodrošināts, izmantojot dažādus DPR principus. Pirmkārt, saskaņā ar *datu integritātes un nolūka ierobežošanas principu*, līdzīgi kā saskaņā ar Regulas (ES) 2016/679 5. panta 1. punkta b) apakšpunktu, organizācija nedrīkst apstrādāt personas datus veidā, kas ir nesaderīgs ar nolūku, kuram tie sākotnēji vākti vai kuram datu subjekts pēc tam atļāvis tos izmantot ([27]).

(15) Otrkārt, lai personas datus izmantotu jaunam (mainītam) nolūkam, kas ir būtiski atšķirīgs, bet joprojām saderīgs ar sākotnējo nolūku, vai izpaustu tos trešai personai, organizācijai ir jānodrošina datu subjektiem iespēja iebilst (atteikties) saskaņā ar *izvēles principu* ([28]), izmantojot skaidru, pamanāmu un viegli pieejamu mehānismu. Svarīgi, ka šis princips neaizstāj skaidro aizliegumu attiecībā uz nesaderīgu apstrādi ([29]).

([25]) I pielikuma III.10.a iedaļa. Sk. arī *DoC* sadarbībā ar Eiropas Datu aizsardzības kolēģiju izstrādātos norādījumus privātuma vairoga kontekstā, kuros ir precizēti ASV iedibināto apstrādātāju, kuri saņem personas datus no Savienības šā regulējuma ietvaros, pienākumi. Tā kā šie noteikumi nav mainījušies, šie norādījumi / BUJ joprojām attiecas uz ES un ASV DPR (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) I pielikuma II.3.b iedaļa.

([27]) I pielikuma II.5.a iedaļa. Saderīgi nolūki var būt revīzija, krāpšanas novēršana vai citi nolūki, kas atbilst saprātīgas personas gaidām, ņemot vērā datu vākšanas kontekstu (sk. I pielikuma 6. zemsvītras piezīmi).

([28]) I pielikuma II.2.a iedaļa. Tas neattiecas uz gadījumiem, kad organizācija sniedz personas datus apstrādātājam, kas darbojas tās vārdā un saskaņā ar tās norādījumiem (I pielikuma II.2.b iedaļa). Tomēr šajā gadījumā organizācijai ir jābūt noslēgtam līgumam un jānodrošina atbilstība *atbildības par tālāku nosūtīšanu* principam, kā sīkāk aprakstīts 43. apsvērumā. Turklāt *izvēles* principu (kā arī *paziņošanas* principu) var ierobežot, ja personas datus apstrādā pienācīgas pārbaudes (kā daļu no iespējamas apvienošanās vai pārņemšanas) vai revīzijas kontekstā vienīgi tiktāl un tikai tādu laikposmu, kas ir vajadzīgs, lai izpildītu likumā noteiktās vai ar sabiedrības interesēm saistītās prasības, un citos apstākļos, kad šo DPR principu piemērošana kaitētu organizācijas likumīgajām interesēm pienācīgas pārbaudes izmeklēšanas vai revīzijas konkrētajā kontekstā (I pielikuma III.4. iedaļa). 15. papildprincips (I pielikuma III.15.a un b iedaļa) paredz arī izņēmumu no *izvēles* principa (kā arī no *paziņošanas* principa un *atbildības par tālāku nosūtīšanu* principa) attiecībā uz personas datiem no publiski pieejamiem avotiem (ja vien ES datu nosūtītājs nenorāda, ka uz šo informāciju attiecas ierobežojumi, kuru dēļ ir jāpiemēro minētie principi) vai personas datiem, kas iegūti no plašākai sabiedrībai pieejamiem reģistriem (ja vien tie nav apvienoti ar nepublisku informāciju un ir ievēroti visi izmantošanas nosacījumi). Tāpat 14. papildprincips (I pielikuma III.14.f iedaļa) paredz izņēmumu no *izvēles* principa (kā arī no *paziņošanas* principa un *atbildības par tālāku nosūtīšanu* principa) attiecībā uz personas datu apstrādi, ko veic farmācijas vai medicīnisko ierīču uzņēmums produktu drošuma un efektivitātes uzraudzības darbībām, ciktāl DPR principu ievērošana traucē ievērot normatīvās prasības.

([29]) Tas attiecas uz visām datu nosūtīšanas darbībām ES un ASV DPR ietvaros, arī ja tās attiecas uz datiem, kas savākti saistībā ar darba tiesiskajām attiecībām. Lai arī sertificēta ASV organizācija tādēļ principā var izmantot cilvēkresursu datus atšķirīgiem mērķiem, kas nav saistīti ar darba tiesiskajām attiecībām (piemēram, konkrētiem tirgvedības paziņojumiem), tai ir jāievēro nesaderīgas apstrādes aizliegums, turklāt organizācija to var darīt tikai saskaņā ar *paziņošanas* principu un *izvēles* principu. Izņēmuma gadījumā organizācija personas datus var izmantot papildu saderīgam nolūkam bez *paziņošanas* un *izvēles* nodrošināšanas, taču tikai tiktāl un tādā periodā, kā tas nepieciešams, neskarot organizācijas spēju īstenot darbinieku paaugstināšanu amatā, norīkošanu vai citu tamlīdzīgu nodarbinātības lēmumu pieņemšanu (sk. I pielikuma III.9.b. iedaļas iv) punktu). Aizliegums ASV organizācijai īstenot jebkādu represīvu darbību pret darbinieku, kas izdarījis šādu izvēli, tajā skaitā noteikt jebkādus ierobežojumus attiecībā uz darba iespējām, nodrošinās, ka, neraugoties uz subordinācijas un pakļautības attiecībām, uz darbinieku netiks izdarīts spiediens un tādējādi viņš var izdarīt patiešām brīvu izvēli. Sk. I pielikuma III.9.b iedaļas i) punktu.

2.2.2. ***Īpašu kategoriju personas datu apstrāde***

(16) Būtu vajadzīgas īpašas garantijas gadījumos, kad tiek apstrādāti "īpašu kategoriju" dati.

(17) Saskaņā ar *izvēles principu* īpašas garantijas piemēro "sensitīvas informācijas" apstrādei, t. i., personas datiem, 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 fiziskās personas seksuālo dzīvi vai jebkādu citu informāciju, kas saņemta no trešās personas un ko šī persona identificē un uzskata par sensitīvu ([30]). Tas nozīmē, ka jebkurus datus, kas saskaņā ar Savienības datu aizsardzības tiesību aktiem tiek uzskatīti par sensitīviem (arī datus par seksuālo orientāciju, ģenētiskos datus un biometriskos datus), sertificētās organizācijas uzskatīs par sensitīviem saskaņā ar ES un ASV DPR.

(18) Parasti organizācijām no fiziskām personām ir jāsaņem apstiprinoša un nepārprotama piekrišana, lai izmantotu sensitīvu informāciju citiem nolūkiem, nevis tiem, kuriem tā sākotnēji tika vākta vai kuriem to vēlāk atļāvusi persona (ar piekrišanu), vai lai izpaustu to trešām personām ([31]).

(19) Šāda piekrišana nav jāsaņem noteiktos apstākļos, kas ir līdzīgi Savienības datu aizsardzības tiesību aktos paredzētajiem izņēmumiem, piemēram, ja sensitīvu datu apstrāde ir personas sevišķi svarīgās interesēs; vajadzīga, lai celtu likumīgas prasības; vajadzīga, lai sniegtu medicīnisko aprūpi vai noteiktu diagnozi ([32]).

2.2.3. ***Datu precizitāte, minimizēšana un drošība***

(20) Datiem vajadzētu būt precīziem un nepieciešamības gadījumā atjauninātiem. Tiem vajadzētu būt arī adekvātiem, atbilstīgiem un nevajadzētu būt pārmērīgiem, ņemot vērā nolūkus, kādos tie tiek apstrādāti, un tie principā nebūtu jāglabā ilgāk nekā nepieciešams nolūkiem, kādos personas datus apstrādā.

(21) Saskaņā ar *datu integritātes un nolūka ierobežojumu principu* ([33]) personas dati ir jāierobežo tādā apmērā, lai tie atbilstu apstrādes nolūkam. Ciktāl tas ir vajadzīgs apstrādes nolūkiem, organizācijai jāveic samērīgi pasākumi, lai nodrošinātu, ka personas dati saistībā ar paredzētajiem nolūkiem ir ticami, precīzi, pilnīgi un atjaunināti.

(22) Turklāt personas datus var glabāt formā, kas identificē fizisku personu vai padara tās identificēšanu iespējamu, (un tādējādi personas datu formā) ([34]) tikai tik ilgi, kamēr tas nepieciešams nolūkam(-iem), kam dati sākotnēji tika vākti vai ko fiziskā persona vēlāk atļāva saskaņā ar *izvēles principu*. Šis pienākums neliedz organizācijām turpināt apstrādāt personas datus ilgāku laiku, bet tikai tik ilgi un tādā mērā, ciktāl šāda apstrāde ir pamatota ar vienu vai vairākiem šādiem īpašiem nolūkiem, kas ir pielīdzināmi Savienības datu aizsardzības tiesību aktos paredzētajiem izņēmumiem: arhivēšana sabiedrības interesēs, žurnālistika, literatūra un māksla, zinātniskā un vēstures pētniecība un statistiskā analīze ([35]). Ja personas dati tiek saglabāti kādam no šiem nolūkiem, uz to apstrādi attiecas DPR principos paredzētie aizsardzības pasākumi ([36]).

(23) Personas dati arī būtu jāapstrādā tā, ka tiek nodrošināta to drošība, kas ietver aizsardzību pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai bojāšanu. Tālab pārziņiem un apstrādātājiem būtu jāveic atbilstoši tehniskie vai organizatoriskie pasākumi, lai aizsargātu personas datus no iespējamiem apdraudējumiem. Šie pasākumi būtu jāizvērtē, ņemot vērā jaunākos sasniegumus, saistītās izmaksas un apstrādes raksturu, apjomu, kontekstu un nolūkus, kā arī riskus attiecībā uz fizisku personu tiesībām.

([30]) I pielikuma II.2.c iedaļa.
([31]) I pielikuma II.2.c iedaļa.
([32]) I pielikuma III.1. iedaļa.
([33]) I pielikuma II.5. iedaļa.
([34]) Sk. I pielikuma 7. zemsvītras piezīmi, kurā precizēts, ka fizisku personu uzskata par "identificējamu", ja organizācija vai trešā persona varētu pamatoti identificēt šo fizisko personu, ņemot vērā identifikācijas līdzekļus, kurus pamatoti varētu izmantot (cita starpā ņemot vērā izmaksas un laiku, kas vajadzīgs identifikācijai, un apstrādes laikā pieejamo tehnoloģiju).
([35]) I pielikuma II.5.b iedaļa.
([36]) Turpat.

(24) Saskaņā ar ES un ASV DPR to garantē *drošības princips*, kas, līdzīgi kā noteikts Regulas (ES) 2016/679 32. pantā, paredz veikt saprātīgus un atbilstīgus drošības pasākumus, ņemot vērā ar apstrādi saistītos riskus un datu veidu ([37]).

2.2.4. ***Pārredzamība***

(25) Datu subjektiem vajadzētu būt informētiem par viņu personas datu apstrādes galvenajām iezīmēm.

(26) Tas tiek nodrošināts ar *paziņošanas principu* ([38]), kas, līdzīgi kā Regulā (ES) 2016/679 noteiktās pārredzamības prasības, paredz, ka organizācijām ir pienākums informēt datu subjektus cita starpā par i) organizācijas dalību DPR, ii) savākto datu veidu, iii) apstrādes nolūku, iv) to trešo personu veidu vai identitāti, kurām personas dati var tikt izpausti, un šādas izpaušanas nolūkiem, v) viņu individuālajām tiesībām, vi) saziņas veidiem ar organizāciju un vii) pieejamajiem tiesiskās aizsardzības līdzekļiem.

(27) Šis paziņojums ir jāsniedz skaidrā un viegli saprotamā valodā, kad fiziskas personas pirmo reizi tiek lūgtas sniegt personas datus vai cik drīz vien iespējams pēc tam, bet jebkurā gadījumā pirms dati tiek izmantoti būtiski atšķirīgam (bet saderīgam) nolūkam, nevis tam, kādam tie tika vākti, vai pirms tie tiek izpausti trešai personai ([39]).

(28) Papildus tam organizācijām ir jāpublisko sava privātuma politika, kas atspoguļo DPR principus (vai – cilvēkresursu datu gadījumā – jānodrošina, lai tā būtu viegli pieejama attiecīgajām fiziskajām personām), un jānodrošina saites uz *DoC* tīmekļa vietni (ar plašāku informāciju par sertifikāciju, datu subjektu tiesībām un pieejamajiem tiesību aizsardzības mehānismiem), datu privātuma regulējuma sarakstu (DPR saraksts), kurā uzskaitītas iesaistītās organizācijas, un atbilstoša strīdu alternatīvas izšķiršanas pakalpojumu sniedzēja tīmekļa vietni ([40]).

2.2.5. ***Individuālās tiesības***

(29) Datu subjektiem būtu jābūt noteiktām tiesībām, kas ir īstenojamas attiecībā uz pārzini vai apstrādātāju, jo īpaši tiesībām piekļūt datiem, tiesībām iebilst pret apstrādi un tiesībām panākt datu labošanu vai dzēšanu.

(30) Šādas tiesības fiziskām personām nodrošina ES un ASV DPR *piekļuves princips* ([41]). Jo īpaši datu subjektiem ir tiesības bez pamatojuma iegūt no organizācijas apstiprinājumu par to, vai tā apstrādā ar viņiem saistītus personas datus, saņemt informāciju par šiem datiem un iegūt informāciju par apstrādes nolūku, apstrādājamo personas datu kategorijām un tiem saņēmējiem (vai to saņēmēju kategorijām), kuriem dati tiek izpausti ([42]). Organizācijām ir pienākums atbildēt uz piekļuves pieprasījumiem samērīgā termiņā ([43]). Organizācija var noteikt saprātīgus

([37]) I pielikuma II.4.a iedaļa. Turklāt attiecībā uz cilvēkresursu datiem ES un ASV DPR paredz, ka darba devējiem ir jāievēro darbinieku vēlmes attiecībā uz privātumu, ierobežojot piekļuvi personas datiem, noteiktus datus padarot anonīmus vai piešķirot kodus vai pseidonīmus (I pielikuma III.9.b iedaļas iii) punkts).

([38]) I pielikuma II.1. iedaļa.

([39]) I pielikuma II.1.b. iedaļa. 14. papildprincips (I pielikuma III.14.b un c iedaļa) paredz īpašus noteikumus par personas datu apstrādi saistībā ar veselības pētniecību un klīniskajiem izmēģinājumiem. Jo īpaši šis princips ļauj organizācijām apstrādāt klīnisko izmēģinājumu datus arī pēc tam, kad persona ir pārtraukusi dalību izmēģinājumā, ja tas ir skaidri norādīts paziņojumā, kas sniegts, kad fiziskā persona piekrita piedalīties. Tāpat, ja ES un ASV DPR organizācija saņem personas datus veselības pētniecības nolūkos, tā drīkst tos izmantot tikai jaunai pētniecības darbībai saskaņā ar *paziņošanas* un *izvēles* principu. Šādā gadījumā paziņojumā fiziskajai personai principā būtu jāsniedz informācija par jebkādu turpmāku konkrētu datu izmantošanu (piemēram, saistītiem pētījumiem). Ja no paša sākuma nav iespējams iekļaut visus turpmākos datu izmantošanas veidus (jo jauns izmantošanas gadījums pētniecības nolūkos varētu rasties jaunas izpratnes vai medicīnas/pētniecības attīstības rezultātā), jāiekļauj paskaidrojums, ka datus var izmantot turpmākās neparedzētās medicīnas un farmaceitiskās pētniecības darbībās. Ja šāda turpmāka izmantošana neatbilst vispārīgajiem pētniecības nolūkiem, kam dati vākti (t. i., ja jaunais nolūks būtiski atšķiras, taču joprojām ir saderīgs ar sākotnējo nolūku (sk. 14. un 15. apsvērumu)), ir jāsaņem jauna piekrišana. Sk. arī 28. zemsvītras piezīmē aprakstītos īpašos *paziņošanas* principa ierobežojumus/izņēmumus.

([40]) I pielikuma III.6.d. iedaļa.

([41]) Sk. arī papildprincipu par piekļuvi (I pielikuma III.8. iedaļa).

([42]) I pielikuma III.8.a iedaļas i)–ii) punkts.

([43]) I pielikuma III.8.i iedaļa.

ierobežojumus attiecībā uz to, cik reižu noteiktā laikposmā tiks izpildīti konkrētas fiziskas personas piekļuves pieprasījumi, un var iekasēt maksu, kas nav pārmērīga, piemēram, ja pieprasījumi ir acīmredzami pārmērīgi, jo īpaši to atkārtošanās dēļ ([44]).

(31) Piekļuves tiesības var ierobežot tikai ārkārtas apstākļos, kas ir līdzīgi Savienības datu aizsardzības tiesību aktos paredzētajiem, jo īpaši, ja ar šādu piekļuvi tiktu pārkāptas citu personu likumīgās tiesības; ja piekļuves nodrošināšanas slogs vai izdevumi būtu nesamērīgi ar riskiem, kas konkrētajā gadījumā apdraud fiziskas personas privātumu (lai gan, nosakot, vai piekļuves nodrošināšana ir saprātīga, izdevumi un slogs nav noteicošie faktori); ciktāl informācijas izpaušana varētu būt pretrunā svarīgu sabiedrības interešu aizsardzībai, piemēram, nacionālajai drošībai, sabiedrības drošībai vai aizsardzībai; ja informācija satur konfidenciālu komercinformāciju vai informācija tiek apstrādāta tikai pētniecības vai statistikas nolūkos ([45]). Jebkādam tiesību izmantošanas atteikumam vai ierobežojumam ir nepieciešams obligāts un pienācīgs pamatojums, un organizācijas pienākums ir pierādīt, ka šīs prasības ir izpildītas ([46]). Veicot šo novērtējumu, organizācijai ir jo īpaši jāņem vērā fiziskās personas intereses ([47]). Ja informāciju ir iespējams nošķirt no citiem datiem, uz kuriem attiecas kāds ierobežojums, organizācijai aizsargātā informācija ir jārediģē un pārējā informācija jāatklāj ([48]).

(32) Turklāt datu subjektiem ir tiesības panākt neprecīzu datu labošanu vai grozīšanu, kā arī to datu dzēšanu, kas apstrādāti, pārkāpjot DPR principus ([49]). Turklāt, kā paskaidrots 15. apsvērumā, fiziskām personām ir tiesības iebilst pret savu datu apstrādi, ja to veic nolūkos, kas būtiski atšķiras no (bet ir saderīgi ar) nolūkiem, kādiem dati tika vākti, un pret savu datu izpaušanu trešām personām. Ja personas dati tiek izmantoti tiešās tirgvedības nolūkos, fiziskām personām ir vispārīgas tiesības jebkurā laikā atteikties no to apstrādes ([50]).

(33) DPR principos nav konkrēti skatīts jautājums par lēmumiem, kuri skar datu subjektu un ir balstīti vienīgi uz personas datu apstrādi automatizētā veidā. Tomēr attiecībā uz personas datiem, kas vākti Savienībā, ikvienu lēmumu, pamatojoties uz automatizētu apstrādi, parasti pieņems Savienībā esošs pārzinis (kam ir tieša saistība ar attiecīgo datu subjektu), un tam attiecīgi piemēro Regulu (ES) 2016/679 ([51]). Tas ietver nosūtīšanas scenārijus, kuros apstrādi veic ārvalstu (piemēram, ASV) uzņēmējs, kas rīkojas kā pārstāvis (apstrādātājs) Savienībā esoša pārziņa vārdā (vai kā apakšapstrādātājs, kas rīkojas Savienībā esoša apstrādātāja vārdā, kurš ir saņēmis datus no Savienībā esoša pārziņa, kas tos savācis), kurš uz šā pamata pieņem lēmumu.

(34) To apstiprināja pētījums, ko Komisija pasūtīja 2018. gadā saistībā ar otro ikgadējo privātuma vairoga darbības pārskatu ([52]), kurā secināts, ka tolaik nebija pierādījumu, kas liecinātu, ka privātuma vairoga organizācijas parasti veic automatizētu lēmumu pieņemšanu, pamatojoties uz personas datiem, kas nosūtīti saskaņā ar privātuma vairogu.

([44]) I pielikuma III.8.f iedaļas i)–ii) punkts un III.8.g iedaļa.
([45]) I pielikuma III.4. iedaļa; 8.b, c, e; 14.e, f un 15.d.
([46]) I pielikuma III.8.e iedaļas ii) punkts. Organizācijai jāinformē fiziskā persona par atteikuma/ierobežojuma iemesliem un jānorāda kontaktpunkts papildu informācijas saņemšanai (III.8.a iedaļas iii) punkts).
([47]) I pielikuma III.8.a iedaļas ii)–iii) punkts.
([48]) I pielikuma III.8.a iedaļas i) punkts.
([49]) I pielikuma II.6. iedaļa un III.8.a iedaļas i) punkts.
([50]) I pielikuma III.8.12. iedaļa.
([51]) Turpretī izņēmuma gadījumā, kad ASV organizācijai ir tieša saistība ar datu subjektu no Savienības, šāda saistība parasti ir rezultāts tam, ka ASV organizācija ir mērķtiecīgi vērsusies tieši pie šīs fiziskās personas Savienībā, piedāvājot tai preces vai pakalpojumus vai vērojot tās uzvedību. Šajā scenārijā uz ASV organizāciju attiecas Regulas (ES) 2016/679 piemērošanas joma (3. panta 2. punkts) un tāpēc tai ir tieši jāievēro ES datu aizsardzības tiesību akti.
([52]) SWD(2018) 497 final, 4.1.5. iedaļa. Pētījumā galvenā uzmanība tika pievērsta tam, i) cik lielā mērā ASV privātuma vairoga organizācijas pieņem fiziskas personas ietekmējošus lēmumus, pamatojoties uz tādu personas datu apstrādi automatizētā veidā, kuri nosūtīti no ES uzņēmumiem saskaņā ar privātuma vairogu, un ii) fiziskām personām paredzētajiem aizsardzības pasākumiem, ko ASV federālie tiesību akti paredz šāda veida situācijām, un nosacījumiem, ar kādiem šie aizsardzības pasākumi piemērojami.

(35) Jebkurā gadījumā attiecība uz jomām, kurās uzņēmumi visdrīzāk izmantotu personas datu automatizētu apstrādi, lai pieņemtu lēmumus, kas skar atsevišķu fizisku personu (piemēram, aizdevumu izsniegšana, hipotēku piedāvājumi, nodarbinātība, mājokļi un apdrošināšana), ASV tiesību aktos ir paredzēta īpaša aizsardzība pret nelabvēlīgiem lēmumiem ([53]). Šajos tiesību aktos parasti noteikts, ka fiziskām 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 pieprasīt tiesisko aizsardzību. Patērētāju kreditēšanas jomā Likumā par godīgu kredītinformāciju (*FCRA*) un Likumā par vienlīdzīgām kreditēšanas iespējām (*ECOA*) ir ietverti aizsardzības pasākumi, kas patērētājiem nodrošina zināmas tiesības saņemt paskaidrojumu un apstrīdēt lēmumu. Šie tiesību akti attiecas uz daudzām jomām, tajā skaitā kreditēšanu, nodarbinātību, mājokļiem un apdrošināšanu. Turklāt daži diskriminācijas novēršanas likumi, piemēram, Pilsonisko tiesību likuma (*Civil Rights Act*) VII sadaļa un Likums par taisnīgumu mājokļu jautājumos (*Fair Housing Act*), nodrošina fiziskām personām aizsardzību attiecībā uz automatizētā lēmumu pieņemšanā izmantotajiem modeļiem, kas varētu izraisīt diskrimināciju noteiktu pazīmju dēļ, un piešķir fiziskām personām tiesības apstrīdēt šādus (arī automatizētos) lēmumus. Attiecībā uz veselības informāciju Likuma par veselības apdrošināšanas datu pārnesamību un pārskatatbildību (*HIPAA*) privātuma noteikumos ir paredzētas noteiktas tiesības, kas ir līdzīgas Regulā (ES) 2016/679 paredzētajām tiesībām attiecībā uz piekļuvi personas veselības informācijai. Turklāt ASV iestāžu norādījumu dokumentā noteikts, ka medicīnas pakalpojumu sniedzējiem ir jāsaņem informācija, kas tiem dod iespēju informēt fiziskas personas par medicīnas nozarē izmantotajām automatizētajām lēmumu pieņemšanas sistēmām ([54]).

(36) Tāpēc šie noteikumi nodrošina aizsardzību, kas ir līdzīga aizsardzībai, ko nodrošina Savienības datu aizsardzības tiesību akti, maz ticamajā situācijā, kad automatizētus lēmumus pieņemtu pati ES un ASV DPR organizācija.

### 2.2.6. ***Tālākas nosūtīšanas ierobežojumi***

(37) Aizsardzības līmeni, kāds piešķirts personas datiem, kurus no Savienības nosūta organizācijām Amerikas Savienotajās Valstīs, nedrīkst samazināt šādu datu tālāka nosūtīšana saņēmējiem Amerikas Savienotajās Valstīs vai citā trešā valstī.

(38) Saskaņā ar *atbildības par tālāku nosūtīšanu principu* ([55]) īpašus noteikumus piemēro tā sauktajai "tālākai nosūtīšanai", proti ES un ASV DPR organizācijas veiktai personas datu nosūtīšanai pārzinim vai apstrādātājam, kas ir trešā persona, neatkarīgi no tā, vai pēdējais minētais atrodas Amerikas Savienotajās valstīs vai trešā valstī ārpus Amerikas Savienotajām Valstīm (un Savienības). Jebkura tālāka nosūtīšana var notikt tikai i) ierobežotos un konkrētos nolūkos, ii) pamatojoties uz līgumu starp ES un ASV DPR organizāciju un trešo personu ([56]) (vai salīdzināmu vienošanos uzņēmumu grupā ([57])), un iii) tikai tad, ja šajā līgumā ir noteikts, ka trešā persona nodrošina tādu pašu aizsardzības līmeni, kādu garantē DPR principi.

(39) Šis pienākums nodrošināt tādu pašu aizsardzības līmeni, kādu garantē DPR principi, lasīti kopā ar *datu integritātes un nolūka ierobežojuma principu*, konkrēti nozīmē, ka trešā persona drīkst apstrādāt tai nosūtītos personas datus tikai tādiem nolūkiem, kas nav nesaderīgi ar nolūkiem, kādiem tie ir vākti vai kādiem tos fiziskā persona vēlāk atļāvusi (saskaņā ar *izvēles principu*).

([53]) Sk., piemēram, Likumu par vienlīdzīgām kreditēšanas iespējām (15 U.S.C. 1691 et seq.), Likumu par godīgu kredītinformāciju (15 USC § 1681 et seq.) vai Likums par taisnīgumu mājokļu jautājumos (42 U.S.C. 3601 et seq.). Turklāt Amerikas Savienotās Valstis ir pievienojušās Ekonomiskās sadarbības un attīstības organizācijas mākslīgā intelekta principiem, kas cita starpā ietver pārredzamības, paskaidrošanas spējas, drošības un pārskatatbildības principus.

([54]) Sk., piemēram, norādījumus, kas pieejami 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

([55]) Sk. I pielikuma II.3. iedaļu un papildprincipu "Obligāti līgumi par tālāku nosūtīšanu" (I pielikuma III.10. iedaļa).

([56]) Saskaņā ar izņēmumu no šā vispārējā principa organizācija var tālāk nosūtīt neliela skaita darbinieku personas datus, neslēdzot līgumu ar saņēmēju, lai īstenotu ar nodarbinātību saistītas gadījuma rakstura operatīvas vajadzības, piemēram, lai rezervētu lidojumu vai numuru viesnīcā vai iegādātos apdrošināšanu. Tomēr arī šajā gadījumā organizācijai joprojām ir jāievēro *paziņošanas* un *izvēles* princips (sk. I pielikuma III.9.e iedaļu).

([57]) Sk. papildprincipu "Obligāti līgumi par tālāku nosūtīšanu" (I pielikuma III.10.b iedaļa). 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 DPR principiem". Turklāt, ņemot vērā to, ka sertificēta ASV organizācija ir atbildīga par DPR principu ievērošanu, tai būs spēcīgs stimuls izmantot tos instrumentus, kas ir patiešām rezultatīvi praksē.

(40) *Atbildības par tālāku nosūtīšanu princips* būtu jālasa saistībā ar *paziņošanas principu* un gadījumā, kad tiek veikta tālāka nosūtīšana pārzinim, kas ir trešā persona ([58]), – ar *izvēles principu*, saskaņā ar kuru datu subjekti ir jāinformē (cita starpā) par jebkura saņēmēja – trešās personas tipu/identitāti, tālākas nosūtīšanas nolūku, kā arī par piedāvāto izvēli un iespēju iebilst (atteikums) pret tālāku nosūtīšanu vai sensitīvu datu gadījumā – nepieciešamību sniegt "skaidru piekrišanu" (piekrišana) tālākai nosūtīšanu.

(41) Pienākums nodrošināt tādu pašu aizsardzības līmeni, kādu nosaka DPR 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, kas ir trešā persona, nosūta minētos datus citam saņēmējam, kurš ir trešā persona, piemēram, apakšapstrādes nolūkiem.

(42) Visos gadījumos līgumā ar saņēmēju, kas ir trešā persona, ir jāparedz, ka saņēmējs informē ES un ASV DPR organizāciju, ja tas konstatē, ka vairs nevar izpildīt savu pienākumu. Ja tas tiek konstatēts, trešajai personai jāpārtrauc apstrāde vai ir jāveic citi pamatoti un atbilstoši pasākumi, lai labotu situāciju ([59]).

(43) Papildu aizsardzība ir piemērojama gadījumā, kad tiek veikta tālāka nosūtīšana pārstāvim (t. i., apstrādātājam), kas ir trešā persona. Šādā gadījumā ASV organizācijai ir jānodrošina, ka pārstāvis rīkojas tikai saskaņā ar tās norādījumiem, un jāveic pamatoti un atbilstoši pasākumi, lai i) nodrošinātu, ka pārstāvis faktiski apstrādā nosūtītos personas datus veidā, kas saskan ar organizācijas saistībām atbilstoši DPR principiem, un ii) lai, saņemot paziņojumu, apturētu un labotu neatļautu apstrādi ([60]). *DoC* var pieprasīt, lai organizācija iesniedz līguma privātuma noteikumu kopsavilkumu vai to reprezentatīvu kopiju ([61]). Ja (apakš)apstrādes ķēdē rodas noteikumu ievērošanas problēmas, principā atbildību nes organizācija, kas darbojas kā personas datu pārzinis, kā to paredz *tiesību aizsardzības, izpildes un atbildības princips*, izņemot gadījumus, kad tā pierāda, ka nav atbildīga par kaitējumu izraisījušo notikumu ([62]).

2.2.7. ***Pārskatatbildība***

(44) Saskaņā ar pārskatatbildības principu vienībām, kas apstrādā datus, ir jāievieš atbilstoši tehniskie un organizatoriskie pasākumi, lai tās efektīvi izpildītu savus datu aizsardzības pienākumus, un jāspēj pierādīt šādu izpildi, konkrēti – kompetentajai uzraudzības iestādei.

(45) Tiklīdz organizācija ir brīvprātīgi nolēmusi iegūt sertifikāciju ([63]) saskaņā ar ES un ASV DPR, tās faktiskā atbilstība DPR principiem ir obligāta un izpildāma. Saskaņā ar *tiesību aizsardzības, izpildes un atbildības principu* ([64]) ES un ASV DPR organizācijām ir jānodrošina iedarbīgi mehānismi, ar ko nodrošināt atbilstību DPR principiem. Organizācijām arī jāveic pasākumi, lai apliecinātu ([65]), ka to publicētā privātuma politika atbilst DPR principiem un faktiski tiek ievērota. To var īstenot vai nu ar pašnovērtēšanas sistēmu, kurā jāiekļauj iekšējās procedūras, ar ko tiek nodrošināts, ka darbinieki 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, vai arī tehnoloģisku rīku izmantošanu.

([58]) Fiziskām 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 DPR principiem.

([59]) 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 ES un ASV DPR organizācijai, jo tā kontrolē apstrādi, saskaņā ar kuras norādēm pārstāvis darbojas. Sk. I pielikuma II.3. iedaļu.

([60]) I pielikuma II.3.b iedaļa.

([61]) Turpat.

([62]) I pielikuma II.7.d iedaļa.

([63]) Sk. arī papildprincipu "Pašsertifikācija" (I pielikuma III.6. iedaļa).

([64]) Sk. arī papildprincipu "Strīdu izšķiršana un izpilde" (I pielikuma III.11. iedaļa).

([65]) Sk. arī papildprincipu "Verifikācija" (I pielikuma III.7. iedaļa).

(46) Turklāt organizācijām ir jāsaglabā uzskaites dati par ES un ASV DPR prakses īstenošanu un pēc pieprasījuma tie jādara pieejami neatkarīgai strīdu izšķiršanas struktūrai vai kompetentajai izpildes iestādei, ja tiek veikta izmeklēšana vai iesniegta sūdzība par neatbilstību ([66]).

### 2.3. **Pārvaldība, pārraudzība un izpilde**

(47) ES un ASV DPR pārvaldīs un pārraudzīs *DoC*. Regulējums paredz pārraudzības un izpildes mehānismus, lai pārbaudītu un nodrošinātu, ka ES un ASV DPR organizācijas ievēro DPR principus un ka tiek novērsta to neievērošana. Šie mehānismi ir izklāstīti DPR principos (I pielikums) un saistībās, ko uzņēmusies *DoC* (III pielikums), *FTC* (IV pielikums) un *DoT* (V pielikums).

#### 2.3.1. ***Atkārtota sertifikācija***

(48) Lai iegūtu sertifikāciju saskaņā ar ES un ASV DPR (vai katru gadu veiktu atkārtotu sertifikāciju), organizācijām ir publiski jāpaziņo par apņemšanos ievērot DPR principus, jādara pieejama sava privātuma politika un tā pilnībā jāīsteno ([67]). Iesniedzot (atkārtotas) sertifikācijas pieteikumu, organizācijām ir jāiesniedz *DoC* informācija, kas cita starpā ietver attiecīgās organizācijas nosaukumu, aprakstu par nolūkiem, kādos organizācija apstrādās personas datus, personas dati, uz kuriem attieksies sertifikācija, kā arī informāciju par izvēlēto pārbaudes metodi, attiecīgo neatkarīgo tiesību aizsardzības mehānismu un oficiālo iestādi, kuras jurisdikcijā ir nodrošināt atbilstību DPR principiem ([68]).

(49) Organizācijas var saņemt personas datus, pamatojoties uz ES un ASV DPR, no dienas, kad *DoC* tās ir iekļāvusi DPR sarakstā. Lai nodrošinātu juridisko noteiktību un izvairītos no "viltus apgalvojumiem", organizācijām, kas sertifikāciju iegūst pirmo reizi, nav atļauts publiski atsaukties uz to, ka tās ievēro DPR principus, pirms *DoC* nav konstatējusi, ka organizācijas sertifikācijas pieteikums ir pilnīgs, un iekļāvusi organizāciju DPR sarakstā ([69]). Lai varētu turpināt izmantot ES un ASV DPR personas datu saņemšanai no Savienības, šādai organizācijai ik gadu ir atkārtoti jāsertificē sava dalība regulējuma īstenošanā. Ja organizācija kāda iemesla dēļ izstājas no ES un ASV DPR, tai ir jādzēš visi paziņojumi, kas norāda, ka organizācija turpina piedalīties regulējuma īstenošanā ([70]).

(50) Kā atspoguļots III pielikumā izklāstītajās saistībās, *DoC* pārbaudīs, vai organizācijas atbilst visām sertifikācijas prasībām un ir ieviesušas (publisku) privātuma politiku, kurā ietverta saskaņā ar *paziņošanas principu* prasītā informācija ([71]). Pamatojoties uz pieredzi, kas gūta (atkārtotas) sertifikācijas procesā saskaņā ar privātuma vairogu, *DoC* veiks vairākas pārbaudes, tajā skaitā pārbaudīs, vai organizāciju privātuma politikās ir hipersaite uz pareizo sūdzību iesniegšanas veidlapu attiecīgā strīdu izšķiršanas mehānisma tīmekļa vietnē un, ja sertifikācijas pieteikumā ir iekļautas vairākas vienas organizācijas struktūras un meitasuzņēmumi, vai visu šo struktūru privātuma politikas atbilst sertifikācijas prasībām un ir viegli pieejamas datu subjektiem ([72]). Turklāt vajadzības gadījumā *DoC* veiks savstarpējas pārbaudes ar *FTC* un *DoT*, lai pārliecinātos, ka uz organizācijām attiecas to (atkārtotas) sertifikācijas pieteikumos norādītā pārraudzības struktūra, un sadarbosies ar strīdu alternatīvas izšķiršanas struktūrām, lai pārliecinātos, ka organizācijas ir reģistrētas to (atkārtotas) sertifikācijas pieteikumos norādītajā neatkarīgajā tiesību aizsardzības mehānismā ([73]).

([66]) I pielikuma III.7. iedaļa.
([67]) I pielikuma I.2. iedaļa.
([68]) I pielikuma III.6.b iedaļa un III pielikums, sk. iedaļu "Pašsertifikācijas prasību izpildes pārbaude".
([69]) I pielikuma 12. zemsvītras piezīme.
([70]) I pielikuma III.6.h iedaļa.
([71]) I pielikuma III.6.a iedaļa un 12. zemsvītras piezīme, kā arī III pielikums, sk. iedaļu "Pašsertifikācijas prasību izpildes pārbaude".
([72]) III pielikuma iedaļa "Pašsertifikācijas prasību izpildes pārbaude".
([73]) Līdzīgi *DoC* sadarbosies ar trešo personu, kas būs datu DAI komisijas maksas veidā iekasēto līdzekļu turētājs (sk. 73. apsvērumu), lai pārbaudītu, vai organizācijas, kas izvēlējušās DAI par savu neatkarīgo tiesību aizsardzības mehānismu, ir samaksājušas maksu par attiecīgo gadu. Sk. III pielikuma iedaļu "Pašsertifikācijas prasību izpildes pārbaude".

(51) *DoC* informēs organizācijas, ka, lai pabeigtu (atkārtotu) sertifikāciju, tām ir jānovērš visas pārbaudē konstatētās problēmas. Ja organizācija nesniedz atbildi *DoC* noteiktajā termiņā (piemēram, attiecībā uz atkārtotu sertifikāciju būtu sagaidāms, ka šis process tiks pabeigts 45 dienu laikā) ([74]) vai sertifikāciju nepabeidz citu iemeslu dēļ, pieteikums tiek uzskatīts par atsauktu. Šādā gadījumā saistībā ar jebkādu sagrozītu informāciju par dalību vai atbilstību ES un ASV DPR *FTC* vai *DoT* var veikt izpildes panākšanas darbības ([75]).

(52) Lai nodrošinātu atbilstīgu ES un ASV DPR piemērošanu, ieinteresētajām personām, piemēram, datu subjektiem, datu nosūtītājiem un valsts datu aizsardzības iestādēm (DAI) jābūt spējīgām identificēt tās organizācijas, kuras ievēro DPR principus. Lai nodrošinātu šādu pārredzamību "ieejas punktā", *DoC* ir apņēmusies uzturēt un darīt sabiedrībai pieejamu to organizāciju sarakstu, kuras ir sertificējušas savu atbilstību DPR principiem un ir vismaz vienas no šā lēmuma IV un V pielikumā minētajām izpildes iestādēm jurisdikcijā ([76]). *DoC* atjaunināts sarakstu, pamatojoties uz organizācijas ikgadējo atkārtotas sertifikācijas pieteikumu, kā arī ikreiz, kad organizācija izstāsies vai tiks izslēgta no ES un ASV DPR. Turklāt, lai garantētu pārredzamību arī "izejas punktā", *DoC* uzturēs un darīs pieejamu sabiedrībai to organizāciju sarakstu, kas svītrotas no saraksta, un katrā ziņā norādīs šādas svītrošanas iemeslu ([77]). Visbeidzot, tā norādīs saiti uz *FTC* tīmekļa vietni, kas veltīta ES un ASV DPR, kurā būs uzskaitītas regulējumā paredzētās *FTC* izpildes panākšanas darbības ([78]).

2.3.2. ***Atbilstības uzraudzība***

(53) *DoC*, izmantojot dažādus mehānismus, pastāvīgi uzraudzīs, vai ES un ASV DPR organizācijas faktiski ievēro DPR principus ([79]). Jo īpaši tā veiks nejauši izvēlētu organizāciju izlases veida pārbaudes, kā arī konkrētu organizāciju izlases veida pārbaudes uz vietas, ja tiks konstatētas iespējamas atbilstības problēmas (piemēram, par kurām *DoC* ziņojušas trešās personas), lai pārbaudītu, vai i) ir pieejams(-i) kontaktpunkts(-i), kas izskata sūdzības un datu subjektu pieprasījumus; vai ii) organizācijas privātuma politika ir viegli pieejama gan tās tīmekļa vietnē, gan ar hipersaiti *DoC* tīmekļa vietnē; vai iii) organizācijas privātuma politika joprojām atbilst sertifikācijas prasībām, un vai iv) organizācijas izvēlētais neatkarīgais strīdu izšķiršanas mehānisms ir pieejams sūdzību izskatīšanai ([80]).

(54) Ja pastāvēs ticami pierādījumi, ka organizācija nepilda savas saistības saskaņā ar ES un ASV DPR (arī gadījumā, ja *DoC* saņem sūdzības vai organizācija sniedz neapmierinošas atbildes uz *DoC* jautājumiem), *DoC* prasīs, lai organizācija aizpilda un iesniedz detalizētu anketu ([81]). Par organizācijām, kas laikus un apmierinoši neatbildēs uz anketas jautājumiem, tiks ziņots attiecīgajai iestādei (*FTC* vai *DoT*), lai tās veiktu iespējamas izpildes panākšanas darbības ([82]). Veicot atbilstības uzraudzības darbības saskaņā ar privātuma vairogu, *DoC* regulāri veica

([74]) III pielikuma 2. zemsvītras piezīme.
([75]) Sk. III pielikuma iedaļu "Pašsertifikācijas prasību izpildes pārbaude".
([76]) Informācija par DPR saraksta pārvaldību ir atrodama III pielikumā (sk. ievadu sadaļā "Datu privātuma regulējuma programmas pārvaldība un uzraudzība, ko veic Tirdzniecības ministrija") un I pielikumā (I.3. iedaļa, I.4. iedaļa, III.6.d iedaļa un III.11.g iedaļa).
([77]) III pielikums, sk. ievadu sadaļā "Datu privātuma regulējuma programmas pārvaldība un uzraudzība, ko veic Tirdzniecības ministrija".
([78]) Sk. III pielikuma iedaļu "Datu privātuma regulējuma tīmekļa vietnes pielāgošana konkrētām mērķauditorijas grupām".
([79]) Sk. III pielikuma iedaļu "Datu privātuma regulējuma programmas periodiskas *ex officio* atbilstības pārbaudes un novērtējumi".
([80]) Veicot uzraudzības darbības, *DoC* var izmantot dažādus rīkus, arī pārbaudīt, vai nav bojātas saites uz privātuma politikām, vai arī aktīvi sekot līdzi ziņām, lai atklātu paziņojumus, kas sniedz ticamus pierādījumus par neatbilstību.
([81]) Sk. III pielikuma iedaļu "Datu privātuma regulējuma programmas periodiskas *ex officio* atbilstības pārbaudes un novērtējumi".
([82]) Sk. III pielikuma iedaļu "Datu privātuma regulējuma programmas periodiskas *ex officio* atbilstības pārbaudes un novērtējumi".

53. apsvērumā minētās izlases veida pārbaudes un nepārtraukti uzraudzīja publiskos paziņojumus, kas ļāva tai identificēt, risināt un novērst atbilstības problēmas ([83]). Organizācijas, kuras pastāvīgi pārkāps DPR principus, tiks dzēstas no DPR saraksta, un tām būs jānodod atpakaļ vai jāizdzēš regulējuma ietvaros saņemtie personas dati ([84]).

(55) Citos dzēšanas gadījumos, piemēram, brīvprātīga izstāšanās vai atkārtotas sertifikācijas neveikšanas gadījumā, organizācijai dati ir vai nu jāizdzēš, vai jāatgriež, vai jāsaglabā, ja tā *DoC* katru gadu apliecina savu apņemšanos turpināt piemērot DPR principus vai nodrošina pietiekamu personas datu aizsardzību citā atļautā veidā (piemēram, izmantojot līgumu, kurā ir pilnībā atspoguļotas attiecīgo līguma standartklauzulu prasības, kuras apstiprinājusi Komisija) ([85]). Tādā gadījumā organizācijai ir jānorāda arī organizācijas kontaktpunkts attiecībā uz visiem ar ES un ASV DPR saistītajiem jautājumiem.

2.3.3. ***Nepatiesu apgalvojumu par dalību meklēšana un reaģēšana uz tiem***

(56) *DoC* uzraudzīs jebkādus nepatiesus apgalvojumus par dalību ES un ASV DPR vai ES un ASV DPR sertifikācijas zīmes neatbilstošu izmantošanu gan *ex officio*, gan pamatojoties uz sūdzībām (piemēram, kas saņemtas no DAI) ([86]). Jo īpaši *DoC* pastāvīgi pārbaudīs, vai organizācijas, kas i) izstājas no dalības ES un ASV DPR, ii) neveic ikgadējo atkārtoto sertifikāciju (t. i., vai nu sāka, bet savlaicīgi nepabeidza ikgadējās atkārtotās sertifikācijas procesu, vai pat nebija sākušas ikgadējo atkārtotās sertifikācijas procesu), iii) ir izslēgtas no dalības noteikumu "pastāvīgas neievērošanas" dēļ vai iv) nav pabeigušas sākotnējo sertifikāciju (t. i., sāka, bet savlaicīgi nepabeidza sākotnējās sertifikācijas procesu), no jebkuras attiecīgās publicētās privātuma politikas svītro atsauces uz ES un ASV DPR, kas norāda, ka attiecīgā organizācija aktīvi piedalās regulējuma īstenošanā ([87]). *DoC* arī veiks meklējumus tīmeklī, lai identificētu atsauces uz ES un ASV DPR organizāciju privātuma politikā, ieskaitot lai identificētu organizāciju, kuras nekad nav piedalījušās ES un ASV DPR, nepatiesus apgalvojumus ([88]).

(57) Ja *DoC* konstatēs, ka atsauces uz ES un ASV DPR nav dzēstas vai ir izmantotas nepareizi, tā informēs organizāciju par iespējamo vēršanos *FTC*/*DoT* ([89]). Ja organizācija atbildi nesniegs, *DoC* jautājumu nodos attiecīgajai iestādei, lai tā veiktu iespējamas izpildes panākšanas darbības ([90]). *FTC*, *DoT* vai citas attiecīgās ASV izpildes iestādes var veikt izpildes panākšanas darbības, ja organizācija, sniedzot maldinošus paziņojumus vai īstenojot maldinošu praksi, sniedz sabiedrībai sagrozītu informāciju, ka ievēro DPR principus. Ja *DoC* tiek sniegta sagrozīta informācija, piemērojami izpildes pasākumi saskaņā ar Likumu par nepatiesu ziņu sniegšanu (18 U.S.C. § 1001).

([83]) Otrajā ikgadējā privātuma vairoga pārskatā *DoC* informēja, ka ir veikusi izlases veida pārbaudes 100 organizācijās un 21 gadījumā nosūtījusi atbilstības anketas (pēc tam konstatētās problēmas tika novērstas), sk. Komisijas dienestu darba dokumentu SWD (2018) 497 final, 9. lpp. Tāpat trešajā ikgadējā privātuma vairoga pārskatā *DoC* ziņoja, ka, sekojot līdzi publiskiem paziņojumiem, tā ir atklājusi trīs incidentus un sākusi praksi katru mēnesi izlases veidā pārbaudīt 30 uzņēmumus, kā rezultātā 28 % gadījumu tika veiktas turpmākas pārbaudes ar atbilstības anketām (pēc kurām atklātās problēmas tika nekavējoties novērstas vai trīs gadījumos atrisinātas pēc brīdinājuma vēstules nosūtīšanas); skatīt Komisijas dienestu darba dokumentu SWD (2019) 495 final, 8. lpp.

([84]) I pielikuma III.11.g iedaļa. Pastāvīga neatbilstība jo īpaši rodas tad, ja organizācija atsakās ievērot galīgo lēmumu, ko pieņēmusi jebkura privātuma pašregulējuma, neatkarīgas strīdu izšķiršanas vai izpildes iestāde.

([85]) I pielikuma III.6.f iedaļa.

([86]) III pielikuma iedaļa "Nepatiesu apgalvojumu par dalību meklēšana un reaģēšana uz tiem".

([87]) Turpat.

([88]) Turpat.

([89]) Turpat.

([90]) Privātuma vairoga ietvaros *DoC* trešajā ikgadējā regulējuma pārskatīšanā ziņoja, ka tā laikposmā no 2018. gada oktobra līdz 2019. gada oktobrim ir konstatējusi 669 gadījumus, kad pausti nepatiesi apgalvojumi par dalību, no tiem lielākā daļa tika atrisināti pēc *DoC* brīdinājuma vēstules saņemšanas, bet 143 gadījumi tika nodoti *FTC* (sk. 62. apsvērumu tālāk). Sk. Komisijas SWD (2019) 495 final, 10. lpp.

2.3.4. ***Izpilde***

(58) Lai nodrošinātu, ka arī praksē tiek garantēts pietiekams datu aizsardzības līmenis, vajadzētu būt izveidotai neatkarīgai uzraudzības iestādei, kurai uzticētas pilnvaras uzraudzīt un nodrošināt datu aizsardzības noteikumu izpildi.

(59) ES un ASV DPR organizācijām ir jābūt pakļautām ASV kompetento iestāžu – *FTC* un *DoT* – jurisdikcijai, kurām ir nepieciešamās izmeklēšanas un izpildes panākšanas pilnvaras, lai efektīvi nodrošinātu atbilstību DPR principiem ([91]).

(60) *FTC* ir neatkarīga iestāde, ko veido pieci komisāri, kurus ieceļ priekšsēdētājs ar Senāta ieteikumu un piekrišanu ([92]). Komisārus ieceļ uz septiņiem gadiem, un priekšsēdētājs viņus var atcelt no amata tikai par nerezultatīvu sniegumu, pienākumu nepildīšanu vai ļaunprātīgu rīcību, pildot amata pienākumus. *FTC* nedrīkst būt vairāk kā trīs komisāri no vienas politiskās partijas, un komisāri laikā, kad tie ir šajā amatā, nedrīkst nodarboties ar citu uzņēmējdarbību, strādāt citā profesijā vai algotā darbā.

(61) *FTC* var izmeklēt atbilstību DPR principiem, kā arī nepatiesus apgalvojumus par DPR principu ievērošanu vai dalību ES un ASV DPR, ko sniedz organizācijas, kuras vai nu vairs nav iekļautas DPR sarakstā, vai arī nekad nav saņēmušas attiecīgu sertifikātu ([93]). *FTC* var panākt atbilstību, pieprasot administratīvos vai federālās tiesas rīkojumus (arī "piekrišanas rīkojumus", kas panākti izlīguma ceļā) ([94]) par pagaidu vai pastāvīgiem aizliegumiem vai citiem koriģējošiem pasākumiem, un sistemātiski uzraudzīs šādu rīkojumu izpildi ([95]). Ja organizācijas šādus rīkojumus neievēro, *FTC* var nodot lietu tiesai, lai piemērotu civiltiesiskus sodus un citus tiesiskās aizsardzības līdzekļus, tajā skaitā par jebkādu kaitējumu prettiesiskas rīcības rezultātā. Katrā ES un ASV DPR organizācijai izdotā piekrišanas rīkojumā būs nosacījumi par patstāvīgu ziņošanu ([96]), un organizācijām būs jāpublisko visas attiecīgās ar ES un ASV DPR saistītās sadaļas, kas iekļautas jebkurā *FTC* iesniegtajā atbilstības vai novērtējuma ziņojumā. Visbeidzot, *FTC* uzturēs tiešsaistes sarakstu ar organizācijām, kurām ES un ASV DPR lietās piemēroti *FTC* vai tiesas rīkojumi ([97]).

(62) Attiecībā uz privātuma vairogu *FTC* ir sākusi izpildes panākšanas darbības aptuveni 22 gadījumos gan saistībā ar konkrētu regulējuma prasību pārkāpumiem (piemēram, ja organizācija nav apstiprinājusi *DoC*, ka turpina piemērot privātuma vairoga aizsardzību pēc izstāšanās no tā, vai ja, veicot pašnovērtējumu vai ārēju atbilstības pārbaudi, nav pārbaudīts, vai organizācija ievēro minēto regulējumu) ([98]), gan saistībā ar nepatiesiem apgalvojumiem par dalību regulējumā (piemēram, organizācijas, kas nav veikušas nepieciešamos pasākumus, lai iegūtu sertifikāciju, vai ir pieļāvušas to sertifikācijas izbeigšanos, bet, sagrozot informāciju, norādījušas, ka turpina dalību) ([99]). Šīs izpildes panākšanas darbības citu starpā izrietēja no proaktīvas administratīvu pavēstu izmantošanas ar nolūku iegūtu materiālus no konkrētiem privātuma vairoga dalībniekiem, lai pārbaudītu, vai nav pieļauti būtiski privātuma vairoga pienākumu pārkāpumi ([100]).

([91]) ES un ASV DPR organizācijai ir publiski jāpauž apņemšanās ievērot DPR principus, jāpublisko sava privātuma politika, kas atbilst šiem principiem, un tā pilnībā jāīsteno. To neievērošanas gadījumā piemēro izpildes darbības saskaņā ar *FTC* likuma 5. pantu, kas aizliedz negodīgas un maldinošas darbības, ko veic tirdzniecībā vai kas to ietekmē (15 U.S.C. §45) un 49 U.S.C. §41712, kas aizliedz pārvadātājam vai biļešu pārdevējam iesaistīties negodīgā vai maldinošā praksē gaisa pārvadājumu nozarē vai gaisa pārvadājumu pakalpojumu pārdošanas jomā.

([92]) 15 U.S.C. § 41.

([93]) IV pielikums.

([94]) No *FTC* saņemta informācija liecina, ka tai nav pilnvaru uz vietas veikt pārbaudes privātuma aizsardzības jomā. Tomēr tai ir pilnvaras likt organizācijām iesniegt dokumentus un sniegt liecības (sk. *FTC* likuma 20. pantu), un neatbilstības gadījumā tā var izmantot tiesu sistēmu, lai panāktu šādu rīkojumu izpildi.

([95]) Sk. IV pielikuma iedaļu "Rīkojumu pieprasīšana un uzraudzība".

([96]) *FTC* vai tiesas rīkojumos var būt prasība uzņēmumiem īstenot privātuma programmas un regulāri darīt *FTC* pieejamus atbilstības ziņojumus vai neatkarīgus šo programmu novērtējumus, ko veikušas trešās personas.

([97]) IV pielikuma iedaļa "Rīkojumu pieprasīšana un uzraudzība".

([98]) Komisijas SWD (2019) 495 final, 11. lpp.

([99]) Sk. lietas, kas uzskaitītas *FTC* tīmekļa vietnē: https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Sk. arī Komisijas SWD (2017) 344 final, 17. lpp; Komisijas SWD (2018) 497 final, 12. lpp. un Komisijas SWD (2019) 495 final, 11. lpp.

([100]) Sk., piemēram, Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

(63) Plašākā skatījumā *FTC* pēdējos gados ir īstenojusi izpildes panākšanas darbības vairākās lietās attiecībā uz atbilstību konkrētām arī ES un ASV DPR noteiktajām datu aizsardzības prasībām, piemēram, attiecībā uz nolūka ierobežojuma un datu saglabāšanas principiem ([101]), datu minimizēšanu ([102]), datu drošību ([103]) un datu precizitāti ([104]).

(64) *DoT* ir ekskluzīvas pilnvaras regulēt aviosabiedrību īstenoto privātuma praksi, un kopā ar *FTC* tai ir jurisdikcija attiecībā uz biļešu pārdevēju piemēroto privātuma praksi gaisa transporta pakalpojumu pārdošanas jomā. *DoT* amatpersonas vispirms cenšas panākt izlīgumu un, ja tas nav iespējams, var uzsākt izpildes procedūru, kas ietver pierādījumu izskatīšanu, ko veic *DoT* administratīvo tiesību tiesnesis, kurš ir pilnvarots izdot rīkojumus par darbības pārtraukšanu un noteikt civiltiesiskus sodus ([105]). Administratīvo tiesību tiesnešiem, lai nodrošinātu viņu neatkarību un objektivitāti, Administratīvā procesa likumā (*APA*) ir paredzēti vairāki aizsardzības līdzekļi. Piemēram, viņus var atlaist tikai ar pamatotu iemeslu; lietas viņiem tiek piešķirtas rotācijas kārtībā; viņi nedrīkst veikt pienākumus, kas nav savietojami ar viņu pienākumiem un atbildību kā administratīvo tiesību tiesnešiem; viņi nav pakļauti iestādes, kura viņus nodarbina (šajā gadījumā – *DoT*) izmeklēšanas komandas uzraudzībai; viņiem lietas ir jāiztiesā un izpildes funkcijas jāīsteno, ievērojot objektivitāti ([106]). *DoT* ir apņēmusies uzraudzīt izpildes rīkojumus un nodrošināt, lai ES un ASV DPR lietās izdotie rīkojumi būtu pieejami tās tīmekļa vietnē ([107]).

### 2.4. **Tiesiskā aizsardzība**

(65) Lai nodrošinātu pietiekamu aizsardzību un jo īpaši individuālo tiesību īstenošanu, datu subjektam vajadzētu būt pieejamiem efektīviem administratīvajiem un tiesiskajiem aizsardzības līdzekļiem.

(66) ES un ASV DPR, piemērojot *tiesību aizsardzības, izpildes un atbildības principu*, paredz, ka organizācijām jānodrošina tiesību aizsardzības līdzekļi fiziskām personām, kuras ietekmē neatbilstība, un tādējādi Savienības datu subjektiem ir iespēja iesniegt sūdzības par ES un ASV DPR organizāciju neatbilstību un vajadzības gadījumā panākt šo sūdzību atrisināšanu ar lēmumu, ar kuru nodrošina efektīvu tiesiskās aizsardzības līdzekli ([108]). Sertifikācijas ietvaros organizācijām jāievēro šā principa prasības, paredzot iedarbīgus un viegli pieejamus neatkarīgus tiesību aizsardzības mehānismus, ar kuriem katras fiziskās personas sūdzības un strīdus var izmeklēt un efektīvi atrisināt, neradot izmaksas fiziskajai personai ([109]).

([101]) Sk., piemēram, *FTC* rīkojumu *Drizly, LLC* lietā, kur citustarp uzņēmumam uzlikts pienākums 1) iznīcināt tā savāktos personas datus, kas tam nav nepieciešami, lai patērētājiem nodrošinātu savus produktus vai pakalpojumus, 2) atturēties no personas datu vākšanas vai glabāšanas, ja vien tas nav nepieciešams saglabāšanas grafikā norādītiem konkrētiem nolūkiem.

([102]) Sk., piemēram, *FTC* rīkojumu *CafePress* lietā (2022. gada 24. marts), kurā citastarp pieprasīts minimizēt vākto datu apjomu.

([103]) Sk., piemēram, *FTC* izpildes panākšanas darbības attiecībā uz *Drizly, LLC* un *CafePress*, kur attiecīgajiem uzņēmumiem pieprasīts ieviest īpašu drošības programmu vai konkrētus drošības pasākumus. Turklāt attiecībā uz datu aizsardzības pārkāpumiem skatīt arī *FTC* 2023. gada 27. janvāra rīkojumu *Chegg* lietā, 2019. gadā panākto izlīgumu ar *Equifax* (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Sk., piemēram, *RealPage, Inc* lietu (2018. gada 16. oktobris), kurā *FTC* veica izpildes panākšanas darbību saskaņā ar *FCRA*, vēršoties pret īrnieku skrīninga uzņēmumu, kas izīrētājiem un īpašumu apsaimniekošanas uzņēmumiem sniedza izpētes ziņojumus par fiziskām personām, balstoties uz informāciju, kas iegūta no īres darījumu vēstures, publiski pieejamiem datiem (ieskaitot datus par sodāmību un piespiedu izlikšanu no dzīvesvietas) un kredītvēstures, un šie ziņojumi pēc tam tika ņemti vērā, vērtējot personu atbilstību mājokļu izīrēšanai. *FTC* konstatēja, ka uzņēmums nav veicis saprātīgus pasākumus, lai nodrošinātu, ka uz tā automātiskā lēmumu pieņemšanas rīka pamata sniegtā informācija ir precīza.

([105]) Sk. V pielikuma iedaļu "Izpildes panākšanas prakse".

([106]) Sk. 5 U.S.C. §§ 3105, 7521(a), 554(d) un 556(b)(3).

([107]) V pielikums, sk. iedaļu "Par ES un ASV DPR pārkāpumiem pieņemto izpildes rīkojumu uzraudzība un publiskošana".

([108]) I pielikuma II.7. iedaļa.

([109]) I pielikuma III.11. iedaļa.

(67) Organizācijas var izvēlēties neatkarīgu tiesību aizsardzības mehānismu Savienībā vai Amerikas Savienotajās Valstīs. Kā sīkāk skaidrots 73. apsvērumā, tas ietver iespēju brīvprātīgi apņemties sadarboties ar ES DAI. Ja organizācijas apstrādā cilvēkresursu datus, šāda apņemšanās sadarboties ar ES DAI ir obligāta. Citas alternatīvas ietver neatkarīgas strīdu alternatīvas izšķiršanas mehānismus vai privātajā sektorā izstrādātas privātuma programmas, kuru noteikumos iekļauti DPR principi. Šādās programmās jāietver efektīvi izpildes mehānismi saskaņā ar *tiesību aizsardzības, izpildes un atbildības principa* prasībām.

(68) Attiecīgi ES un ASV DPR paredz datu subjektiem vairākas iespējas īstenot savas tiesības, iesniegt sūdzības par ES un ASV DPR organizāciju neatbilstību un panākt viņu sūdzību izskatīšanu, ja nepieciešams, pieņemot lēmumu par efektīvu tiesisko aizsardzību. Fiziskas personas var iesniegt sūdzību tieši organizācijai, neatkarīgas strīdu izšķiršanas struktūrai, kuru izraudzījusies organizācija, valstu DAI, *DoC* vai *FTC*. Gadījumos, kad viņu sūdzības nav atrisinātas, izmantojot jebkuru no šiem tiesību aizsardzības vai izpildes mehānismiem, personām ir arī tiesības pieprasīt šķīrējtiesu, kuras lēmums ir saistošs (šā lēmuma I pielikumam pievienoto I pielikumu). Izņemot šķīrējtiesas kolēģiju, kuras gadījumā vispirms ir jāizmanto daži tiesiskās aizsardzības līdzekļi, pirms var pieprasīt šķīrējtiesu, fiziskās personas pēc savas izvēles var brīvi izvēlēties jebkuru vai visus tiesiskās aizsardzības mehānismus, un tām nav pienākuma izdarīt izvēli par labu vienam vai otram mehānismam vai ievērojot noteiktu secību.

(69) Pirmkārt, Savienības datu subjekti var sekot ar neatbilstību DPR principiem saistītajām lietām, tieši sazinoties ar ES un ASV DPR organizācijām ([110]). Lai sekmētu strīdu izšķiršanu, organizācijai ir jāievieš efektīvs tiesiskās aizsardzības mehānisms šādu sūdzību izskatīšanai. Tādēļ organizācijas privātuma politikai ir skaidri jāinformē fiziskas personas par kontaktpunktu organizācijā vai ārpus tās, kas izskatīs sūdzības (tajā skaitā jebkuru atbilstīgu iestādi Savienībā, kura var atbildēt uz pieprasījumiem vai sūdzībām), kā arī par izraudzīto neatkarīgas strīdu izšķiršanas struktūru (sk. 70. apsvērumu). Saņemot fiziskas personas sūdzību – gan tieši no pašas fiziskās personas, gan ar *DoC* starpniecību, kad DAI ir nodevusi to izskatīšanai, organizācijai ir jāsniedz atbilde Savienības datu subjektam 45 dienu laikā ([111]). Tāpat organizācijām ir nekavējoties jāatbild uz jautājumiem un citiem informācijas pieprasījumiem no *DoC* vai DAI ([112]) (gadījumos, kad organizācija ir uzņēmusies saistības sadarboties ar DAI) saistībā ar to, kā tās ievēro DPR principus.

(70) Otrkārt, personas var iesniegt sūdzību tieši organizācijas norīkotai neatkarīgai strīdu izšķiršanas struktūrai (Amerikas Savienotajās Valstīs vai Savienībā), kas izmeklē un risina fizisku personu sūdzības (ja vien tās nav acīmredzami nepamatotas vai nenozīmīgas) un nodrošina personai atbilstīgu tiesību aizsardzību bez maksas ([113]). Šādas struktūras piemērotām sankcijām un tiesiskās aizsardzības līdzekļiem ir jābūt pietiekami stingriem, lai nodrošinātu organizāciju atbilstību DPR principiem, un jāparedz organizācijas veikta neatbilstības ietekmes novēršana vai koriģēšana un, atkarībā no apstākļiem, turpmākas attiecīgo datu apstrādes pārtraukšana un/vai to dzēšana, kā arī neatbilstības konstatējumu publicēšana ([114]). Organizācijas norīkotām neatkarīgām strīdu izšķiršanas struktūrām savās publiskajās tīmekļa vietnēs ir jāiekļauj relevantā informācija par ES un ASV DPR un pakalpojumiem, ko tās sniedz saskaņā ar šo regulējumu ([115]). Tām katru gadu ir jāpublicē gada ziņojums, kurā sniegta kopējā statistika par šiem pakalpojumiem ([116]).

([110]) I pielikuma III.11.d iedaļas i) punkts.
([111]) I pielikuma III.11.d iedaļas i) punkts.
([112]) Tā ir izskatītāja iestāde, kuru norīkojusi DAI komisija, kas paredzēta papildprincipā "Datu aizsardzības iestāžu loma" (I pielikuma III.5. iedaļa).
([113]) I pielikuma III.11.d iedaļa.
([114]) I pielikuma II.7. un III.11.e iedaļa.
([115]) I pielikuma III.11.d iedaļas ii) punkts.
([116]) Gada pārskatā jāiekļauj šāda informācija: 1) pārskata gadā saņemto ar ES un ASV DPR saistīto sūdzību kopējais skaits; 2) saņemto sūdzību veidi; 3) strīdu izšķiršanas kvalitātes rādītāji, piemēram, sūdzību izskatīšanas ilgums, un 4) saņemto sūdzību rezultāti, jo īpaši noteikto tiesiskās aizsardzības līdzekļu vai sankciju skaits un veidi.

(71) Veicot atbilstības pārbaudes procedūras, *DoC* var pārbaudīt, vai ES un ASV DPR organizācijas patiešām ir reģistrētas tādos neatkarīgos tiesību aizsardzības mehānismos, kurus tās norādījušas ([117]). Gan organizācijām, gan atbildīgajiem neatkarīgajiem tiesību aizsardzības mehānismiem ir jāspēj nekavējoties atbildēt uz *DoC* jautājumiem un informācijas pieprasījumiem saistībā ar ES un ASV DPR. *DoC* sadarbosies ar neatkarīgiem tiesību aizsardzības mehānismiem, lai pārbaudītu, vai tie savās tīmekļa vietnēs iekļauj informāciju par DPR principiem un par pakalpojumiem, ko tie sniedz saskaņā ar ES un ASV DPR, un vai tie publicē gada pārskatus ([118]).

(72) Gadījumos, kad organizācija neievēro strīdu izšķiršanas vai pašregulējuma struktūras nolēmumu, struktūrai par šādu neievērošanu ir jāinformē *DoC* un *FTC* (vai cita ASV iestāde ar piekritību izmeklēt organizācijas neatbilstību), vai kompetenta tiesa ([119]). Ja organizācija atsakās ievērot jebkuras privātuma pašregulējuma, neatkarīgas strīdu izšķiršanas vai valdības iestādes galīgo lēmumu vai gadījumā, ja šāda iestāde konstatē, ka organizācija bieži neievēro DPR principus, to var uzskatīt par pastāvīgu neizpildi, kā rezultātā *DoC*, vispirms informējot organizāciju, kura nav ievērojusi DPR principus, un dodot tai iespēju 30 dienu laikā atbildēt, svītros šo organizāciju no DPR saraksta ([120]). Ja pēc svītrošanas no saraksta organizācija turpinās apgalvot, ka ir sertificēta ES un ASV DPR, *DoC* vērsīsies pie *FTC* vai citas izpildes iestādes ([121]).

(73) Treškārt, arī fiziskas personas Savienībā var vērsties ar sūdzībām valsts DAI, kuras var izmantot izmeklēšanas un tiesību aizsardzības pilnvaras, kuras tām piešķirtās saskaņā ar Regulu (ES) 2016/679. Organizācijām ir pienākums sadarboties, kad DAI veic izmeklēšanu un risina sūdzību – gan tad, ja tā attiecas uz cilvēkresursu datu apstrādi, kuri savākti saistībā ar darba tiesiskajām attiecībām, gan tad, ja attiecīgā organizācija ir brīvprātīgi piekritusi pārraudzībai, ko veic DAI ([122]). Jo īpaši organizācijām ir jāatbild uz pieprasījumiem, jāievēro DAI sniegtie ieteikumi, tajā skaitā par tiesiskās aizsardzības vai kompensācijas pasākumiem, un jāsniedz DAI rakstveida apstiprinājums par šādu rīcību ([123]). Ja DAI sniegtie ieteikumi netiek ņemti vērā, DAI šādas lietas nodod *DoC* (kas organizācijas var svītrot no ES un ASV DPR saraksta) vai, ja nepieciešama izpildes panākšanas darbība, lietas tiek nodotas *FTC* vai *DoT* (nesadarbošanās ar DAI un principu neievērošana ir aizliegta saskaņā ar ASV likumiem) ([124]).

(74) Lai veicinātu sadarbību efektīvas sūdzību izskatīšanas nolūkā, gan *DoC*, gan *FTC* ir izveidojušas īpašu kontaktpunktu, kas ir atbildīgs par tiešu saziņu ar DAI ([125]). Šie kontaktpunkti sniedz atbalstu saistībā ar DAI pieprasījumiem par organizācijas atbilstību DPR principiem.

(75) DAI sagatavotos ieteikumus ([126]) sniedz pēc tam, kad abām strīdā iesaistītajām pusēm ir bijusi pienācīga iespēja sniegt piezīmes un uzrādīt visus pierādījumus, ko tās vēlas. Attiecīgā komisija var sniegt ieteikumus, cik vien drīz to atļaus prasība par pienācīgu izskatīšanu un parasti 60 dienu laikā pēc sūdzības saņemšanas ([127]). Ja organizācija 25 dienu laikā pēc ieteikuma sniegšanas to neievēro un nesniedz pienācīgu paskaidrojumu par kavēšanos, komisija var paziņot par tās nodomu vai nu iesniegt lietu *FTC* (vai citai kompetentai ASV izpildes iestādei), vai arī secināt, ka

([117]) I pielikuma iedaļa "Pašsertifikācijas prasību izpildes pārbaude".
([118]) Sk. III pielikuma iedaļu "Sadarbības veicināšana ar strīdu alternatīvas izšķiršanas struktūrām, kas sniedz ar DPR principiem saistītus pakalpojumus". Sk. arī I pielikuma III.11.d iedaļas ii)–iii) punktu.
([119]) Sk. I pielikuma III.11.e iedaļu.
([120]) Sk. I pielikuma III.11.g iedaļu, jo īpaši ii) un iii) punktu.
([121]) Sk. III pielikuma iedaļu "Nepatiesu apgalvojumu par dalību meklēšana un reaģēšana uz tiem".
([122]) I pielikuma II.7.b iedaļa.
([123]) I pielikuma III.5. iedaļa.
([124]) I pielikuma III.5.c iedaļas ii) punkts.
([125]) III pielikums (sk. iedaļu "Sadarbības ar DAI veicināšana") un IV pielikums (sk. iedaļas "Pieprasījumu prioritāra izskatīšana un izmeklēšana" un "Sadarbība izpildes jomā ar ES DAI").
([126]) Datu aizsardzības iestādēm, pamatojoties uz savu kompetenci organizēt savu darbu un savstarpēji sadarboties, būtu jāizstrādā neformālas DAI komisijas reglaments.
([127]) I pielikuma III.5.c iedaļas i) punkts.

sadarbošanās saistības ir ievērojami pārkāptas. Pirmajā gadījumā rezultāts var būt izpildes panākšanas darbība saskaņā ar FTC likuma 5. pantu (vai līdzīgu tiesību aktu) ([128]). Otrajā gadījumā komisija informēs *DoC*, kas organizācijas atteikumu ievērot DAI komisijas ieteikumu uzskatīs par pastāvīgu pārkāpumu, kā rezultātā organizācija tiks svītrota no DPR saraksta.

(76) 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 ES dalībvalsts vietējās tiesās.

(77) Personas var arī iesniegt sūdzību DAI pat tad, ja DAI komisija nav norīkota kā organizācijas strīdu izšķiršanas struktūra. Šādos gadījumos DAI var pārsūtīt šādas sūdzības *DoC* vai *FTC*. Lai atvieglotu un pastiprinātu sadarbību jautājumos, kas saistīti ar fizisku personu iesniegtām sūdzībām un ES un ASV DPR organizāciju neatbilstību, *DoC* izveidos īpašu kontaktpunktu, kas darbosies kā sadarbības koordinators un palīdzēs veikt DAI pieprasījumus par organizācijas atbilstību DPR principiem ([129]). Tāpat īpašu kontaktpunktu ir apņēmusies izveidot *FTC* ([130]).

(78) Ceturtkārt, *DoC* ir apņēmusies saņemt, izskatīt un darīt visu iespējamo, lai izskatītu sūdzības par organizācijas neatbilstību DPR principiem ([131]). Šajā nolūkā *DoC* nodrošina īpašas procedūras DAI, lai nodotu sūdzības izskatīšanai speciālam kontaktpunktam, izsekotu tās un turpinātu saziņu ar organizācijām, lai sekmētu sūdzību risināšanu ([132]). Lai paātrinātu fizisku personu iesniegtu sūdzību apstrādi, kontaktpunkts sazinās tieši ar attiecīgo DAI par atbilstības jautājumiem un īpaši informē to par sūdzību statusu periodā, kas nepārsniedz 90 dienas pēc nodošanas izskatīšanai ([133]). Tas ļauj datu subjektiem iesniegt sūdzības par ES un ASV DPR organizāciju neatbilstību tieši savas valsts DAI un nodrošina, ka tās tiek pārsūtītas *DoC* kā ASV iestādei, kas pārvalda ES un ASV DPR.

(79) Ja, pamatojoties uz pārbaudēm, kas veiktas *ex officio*, sūdzībām vai jebkādu citu informāciju, *DoC* secinās, ka organizācija ir pastāvīgi pārkāpusi DPR principus, tā dzēsīs šādu organizāciju no DPR saraksta ([134]). Atteikums ievērot jebkādas privātuma pašregulējuma, neatkarīgas strīdu izšķiršana vai valsts struktūras (tajā skaitā DAI) galīgo lēmumu, tiks uzskatīts par pastāvīgu pārkāpumu ([135]).

(80) Piektkārt, ES un ASV DPR organizācijai ir jābūt pakļautai ASV kompetento iestāžu (jo īpaši *FTC* ([136])) jurisdikcijai, kurām ir nepieciešamās izmeklēšanas un izpildes panākšanas pilnvaras, lai efektīvi nodrošinātu atbilstību DPR principiem. *FTC* prioritārā kārtā izskatīs pieprasījumus par neatbilstību DPR principiem, kuri saņemti no neatkarīgām strīdu izšķiršanas vai pašregulējuma struktūrām, *DoC* un DAI (rīkojoties pēc pašu iniciatīvas vai saskaņā ar sūdzībām) nosakot, vai ir pārkāpts *FTC* likuma 5. pants ([137]). *FTC* ir uzņēmusies saistības izstrādāt standartizētu nodošanas izskatīšanai procedūru, norīkot iestādē kontaktpunktu DAI nodoto lietu izskatīšanai un apmainīties ar informāciju par izskatīšanai nodotajām lietām. Turklāt tā var pieņemt sūdzības tieši no fiziskām personām un pēc savas iniciatīvas veikt ar ES un ASV DPR saistītu izmeklēšanu, jo īpaši kā daļu no plašākas privātuma jautājumu izmeklēšanas.

([128]) I pielikuma III.5.c iedaļas ii) punkts.
([129]) Sk. III pielikuma iedaļu "Sadarbības ar DAI veicināšana".
([130]) Sk. IV pielikuma iedaļas "Pieprasījumu prioritāra izskatīšana un izmeklēšana" un "Sadarbība izpildes jomā ar ES DAI".
([131]) III pielikums, sk., piemēram, iedaļu "Sadarbības ar DAI veicināšana".
([132]) I pielikuma II.7.e iedaļa un III pielikuma iedaļa "Sadarbības ar DAI veicināšana".
([133]) Turpat.
([134]) I pielikuma III.11.g iedaļa.
([135]) I pielikuma III.11.g iedaļa.
([136]) ES un ASV DPR organizācijai ir publiski jāpauž apņemšanās ievērot DPR principus, jāpublisko sava privātuma politika, kas atbilst šiem principiem, un tā pilnībā jāīsteno. To neievērošanas gadījumā piemēro izpildes darbības saskaņā ar *FTC* likuma 5. pantu, kas aizliedz negodīgas un maldinošas darbības, ko veic tirdzniecībā vai kas to ietekmē.
([137]) Sk. arī līdzīgas saistības, ko uzņēmusies *DoT*; V pielikums.

(81) Sestkārt, ja fiziskas personas sūdzība nav apmierinoši atrisināta ne ar vienu citu pieejamo tiesiskās aizsardzības līdzekli, Savienības datu subjekts kā galēju tiesību aizsardzības mehānismu var izmantot iespēju pieprasīt saistošu šķīrējtiesu, ko sprież ES un ASV datu privātuma regulējuma kolēģija (ES un ASV DPR kolēģija) ([138]). Organizācijām ir jāinformē fiziskas personas par iespēju pieprasīt saistošu šķīrējtiesu, un organizācijām ir pienākums reaģēt, ja fiziska persona ir izmantojusi šo iespēju, iesniedzot paziņojumu attiecīgajai organizācijai ([139]).

(82) ES un ASV DPR kolēģijas sastāvā ir vismaz desmit šķīrējtiesnešu, kurus iecēlusi *DoC* un Komisija, pamatojoties uz viņu neatkarību, godīgumu, kā arī pieredzi ASV privātuma un Savienības datu aizsardzības tiesībās. Katram atsevišķam strīdam puses no šī kopuma izvēlas vienu vai trīs ([140]) šķīrējtiesnešus.

(83) *DoC* šķīrējtiesas procesu pārvaldīšanai izvēlējās Starptautisko strīdu izšķiršanas centru (*ICDR*) – Amerikas Šķīrējtiesu asociācijas (*AAA*) starptautisko nodaļu. Lietu izskatīšanu ES un ASV DPR šķīrējtiesas kolēģijā reglamentēs saskaņots šķīrējtiesas reglaments un iecelto šķīrējtiesnešu rīcības kodekss. *ICDR AAA* tīmekļa vietnē ir sniegta skaidra un kodolīga informācija fiziskām personām par šķīrējtiesas mehānismu un šķīrējtiesas pieteikuma iesniegšanas procedūru.

(84) Šķīrējtiesas noteikumi, par kuriem vienojušās *DoC* un Komisija, papildina ES un ASV DPR, kurā ir vairākas iezīmes, kas uzlabo šā mehānisma pieejamību Savienības datu subjektiem: i) sagatavojot prasību kolēģijai, datu subjektam var palīdzēt viņa valsts DAI; ii) lai gan šķīrējtiesa notiks Amerikas Savienotajās Valstīs, Savienības datu subjekti var izvēlēties piedalīties ar videokonferences vai telefonkonferences starpniecību, kas fiziskajai personai tiks nodrošināta bez maksas; iii) kaut arī šķīrējtiesā parasti tiek izmantota angļu valoda, mutiskais tulkojums šķīrējtiesas sēdē un rakstiskais tulkojums principā tiks nodrošināti pēc pamatota pieprasījuma un bez maksas datu subjektam; iv) visbeidzot, lai gan katrai pusei pašai jāsedz sava advokāta honorārs, ja to šķīrējtiesas kolēģijā pārstāv advokāts, *DoC* uzturēs fondu, kurā ES un ASV DPR organizācijas veiks ikgadējas iemaksas, lai segtu šķīrējtiesas procedūras izmaksas, nepārsniedzot maksimālo summu, ko noteiks ASV iestādes, apspriežoties ar Komisiju ([141]).

(85) ES un ASV DPR kolēģijai būs tiesības piemērot fiziskajai personai pielāgotu, taisnīgu nemonetāru koriģējošu pasākumu ([142]), kas nepieciešams, lai novērstu neatbilstību DPR principiem. Kaut arī, pieņemot lēmumu, šķīrējtiesas kolēģija ņem vērā citus tiesību aizsardzības līdzekļus, kas jau iegūti, izmantojot citus ES un ASV DPR mehānismus, fiziskas personas joprojām var vērsties šķīrējtiesā, ja tās uzskata, ka šie citi tiesiskās aizsardzības līdzekļi ir nepietiekami. Tas ļauj Savienības datu subjektiem pieprasīt šķīrējtiesu visos gadījumos, kad ES un ASV DPR organizācijas neatkarīgu tiesību aizsardzības mehānismu vai ASV kompetento iestāžu (piemēram, *FTC*) darbība vai bezdarbība nav apmierinoši atrisinājusi viņu sūdzības. Šķīrējtiesas iespēju izmantot nevar, ja DAI ir juridiskas pilnvaras risināt izskatāmo prasību attiecībā uz ES un ASV DPR organizāciju, proti, gadījumos, kad organizācijai ir vai nu pienākums sadarboties un ievērot DAI ieteikumus attiecībā uz cilvēkresursu datu, kas savākti saistībā ar nodarbinātību, apstrādi, vai arī tā ir brīvprātīgi apņēmusies to darīt. Fiziskas personas var prasīt šķīrējtiesas lēmuma izpildi ASV tiesās saskaņā ar Federālo šķīrējtiesas procesa likumu – šādi tiek nodrošināti tiesiskās aizsardzības līdzekļi gadījumā, ja organizācija neievēro noteikumus.

([138]) Sk. I pielikuma iedaļu "Šķīrējtiesas modelis".
([139]) Sk. I pielikuma II.1.a iedaļas xi) punktu un II.7.c iedaļu.
([140]) Pusēm būs jāvienojas par kolēģijas šķīrējtiesnešu skaitu.
([141]) I pielikuma G.6. iedaļa.
([142]) Fiziskas personas nevar pieprasīt zaudējumu atlīdzināšanu šķīrējtiesā, bet šķīrējtiesas pieprasīšana neierobežo iespēju pieprasīt zaudējumu atlīdzināšanu parastās ASV tiesās.

(86) Septītkārt, ja organizācija neievēro savas saistības ievērot DPR principus un publicēto privātuma politiku, saskaņā ar ASV tiesību aktiem ir pieejami papildu tiesiskās aizsardzības līdzekļi – arī iespēja saņemt kaitējuma kompensāciju. Piemēram, fiziskas personas noteiktos apstākļos var iegūt tiesisko aizsardzību (arī kaitējuma kompensāciju) saskaņā ar štata patērētāju tiesību aktiem krāpnieciski sagrozītas informācijas, negodīgas vai maldinošas rīcības vai prakses gadījumos ([143]), kā arī saskaņā ar tiesību aktiem par atlīdzināmu kaitējumu (jo īpaši saistībā ar atlīdzināmu kaitējumu, kas attiecas uz vienatnības traucēšanu ([144]), vārda vai tēla piesavināšanos ([145]) un privātu faktu publiskošanu ([146])).

(87) Kopā dažādās iepriekš aprakstītas tiesiskās aizsardzības metodes nodrošina, ka jebkura sūdzība par sertificētu organizāciju neatbilstību ES un ASV DPR tiek efektīvi izskatīta un risināta.

## 3. AMERIKAS SAVIENOTO VALSTU PUBLISKO IESTĀŽU PIEKĻUVE PERSONAS DATIEM, KO NOSŪTA NO EIROPAS SAVIENĪBAS, UN ŠĀDU DATU IZMANTOŠANA

(88) Komisija ir arī novērtējusi ierobežojumus un garantijas, tajā skaitā pārraudzības un individuālās tiesiskās aizsardzības mehānismus, kas Amerikas Savienoto Valstu tiesību aktos pieejami saistībā ar tādu personas datu vākšanu un vēlāku izmantošanu, kurus ASV publiskās iestādes nosūta pārziņiem un apstrādātājiem ASV sabiedrības interesēs, jo īpaši krimināltiesību aizsardzības un nacionālās drošības nolūkos ("valdības piekļuve") ([147]). Novērtējot, vai nosacījumi, ar kādiem valdības piekļuve datiem, kas saskaņā ar šo lēmumu nosūtīti uz Amerikas Savienotajām Valstīm, atbilst "līdzvērtības pēc būtības" pārbaudei saskaņā ar Regulas (ES) 2016/679 45. panta 1. punktu, kā to interpretējusi Tiesa, ņemot vērā Pamattiesību hartu, Komisija jo īpaši ņēma vērā vairākus kritērijus.

(89) Jo īpaši, jebkuriem ierobežojumiem, kas skar tiesības uz personas datu aizsardzību, ir jābūt paredzētiem tiesību aktos, un juridiskajam pamatam, kurš pieļauj šādu tiesību ierobežojumu, pašam jānosaka attiecīgo tiesību īstenošanas ierobežojuma darbības joma ([148]). Turklāt, lai nodrošinātu atbilstību samērīguma prasībai, saskaņā ar kuru atkāpes no personas datu aizsardzības un to ierobežojumi piemērojami tikai tiktāl, ciktāl tas ir absolūti nepieciešams (noteikti vajadzīgs) demokrātiskā sabiedrībā, lai sasniegtu konkrētus vispārējas nozīmes mērķus, kas ir līdzvērtīgi Savienībā atzītajiem, šim juridiskajam pamatam jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgo pasākumu darbības jomu un piemērošanu, un jānosaka minimāli aizsardzības pasākumi, lai personām, kuru dati ir nosūtīti, būtu pietiekamas garantijas efektīvai viņu personas datu aizsardzībai pret ļaunprātīgas izmantošanas risku ([149]). Turklāt šiem noteikumiem un aizsardzības pasākumiem jābūt juridiski saistošiem un

([143]) Sk., piemēram, Kalifornijas štata patērētāju aizsardzības likumu (*Cal. Civ. Code §§ 1750 - 1785 (West) Consumers Legal Remedies Act*); Kolumbijas apgabala patērētāju tiesību aizsardzības likumu (*D.C. Code §§ 28–3901*); Floridas štata patērētāju tiesību aizsardzības likumu (*Fla. Stat. §§ 501.201–501.213, Deceptive and Unfair Trade Practices Act*); Ilinoisas štata patērētāju tiesību aizsardzības likumu (*815 Ill. Comp. Stat. 505/1–505/12, Consumer Fraud and Deceptive Business Practices Act*); Pensilvānijas štata patērētāju tiesību aizsardzības likumu (*73 Pa. Stat. Ann. §§ 201-1–201-9.3 (West) Unfair Trade Practices and Consumer Protection Law*).

([144]) T. i., ja notikusi tīša iejaukšanās personas privātajās lietās tādā veidā, kas ļoti aizskartu saprātīgu personu (*Restatement (2nd) of Torts, §652(b)*).

([145]) Šo atlīdzināmo kaitējumu parasti piemēro gadījumos, kad kāds piesavinās un izmanto kādas fiziskas personas vārdu vai tēlu, lai reklamētu uzņēmumu vai produktu vai līdzīgiem komerciāliem mērķiem (sk. *Restatement (2nd) of Torts, § 652C*).

([146]) T. i., ja tiek publiskota informācija par personas privāto dzīvi, ja tā ļoti aizskar saprātīgu personu un ja šī informācija būtiski nerada leģitīmas bažas sabiedrībai (*Restatement (2nd) of Torts, § 652D*).

([147]) Tas ir būtiski arī I pielikuma I.5. iedaļas kontekstā. Saskaņā ar to un līdzīgi, kā noteikts VDAR, atbilstībai datu aizsardzības prasībām un privātuma principos iekļautajām tiesībām var piemērot ierobežojumus. Tomēr šādi ierobežojumi nav absolūti; uz tiem var paļauties tikai noteiktos apstākļos, piemēram, tiktāl, cik tas nepieciešams, lai pakļautos tiesas rīkojumam vai ievērotu sabiedrības intereses, tiesībaizsardzības vai nacionālās drošības prasības. Šajā kontekstā un skaidrības labad šajā iedaļā arī ir dotas atsauces uz 127.–141. apsvērumā novērtētajiem IR Nr. 14086 izklāstītajiem nosacījumiem.

([148]) Sk. spriedumu lietā *Schrems II*, 174. un 175. punktu, un minēto judikatūru. Attiecībā uz dalībvalstu publisko iestāžu piekļuvi sk. spriedumu lietā C-623/17 *Privacy International*, ECLI:EU:C:2020:790, 65. punkts; un apvienotajās lietās C-511/18, C-512/18 un C-520/18, *La Quadrature du Net* un citi, ECLI:EU:C:2020:791, 175. punkts.

([149]) Sk. spriedumu lietā *Schrems II*, 176. un 181. punktu, kā arī minēto judikatūru. Attiecībā uz dalībvalstu publisko iestāžu piekļuvi sk. arī spriedumu lietā *Privacy International*, 68. punkts, un *La Quadrature du Net* un citi, 132. punkts.

fiziskām personām izpildāmiem ([150]). Datu subjektiem jo īpaši jābūt iespējai celt prasību neatkarīgā un objektīvā tiesā, lai gūtu piekļuvi saviem personas datiem vai panāktu šādu datu labošanu vai dzēšanu ([151]).

### 3.1. **ASV publisko iestāžu piekļuve datiem un to izmantošana krimināltiesību aizsardzības nolūkos**

(90) Attiecībā uz iejaukšanos personas datos, kas nosūtīti saskaņā ar ES un ASV DPR krimināltiesību aizsardzības nolūkos, Amerikas Savienoto Valstu tiesību aktos ir noteikti vairāki ierobežojumi attiecībā uz piekļuvi personas datiem un to izmantošanu, kā arī ir paredzēti pārraudzības un tiesiskās aizsardzības mehānismi, kas atbilst šā lēmuma 89. apsvērumā minētajām prasībām. Nosacījumi, saskaņā ar kuriem var notikt šāda piekļuve, un garantijas, kas piemērojamas šo pilnvaru izmantošanai, ir sīki novērtēti turpmākajās iedaļās. Šajā saistībā ASV valdība (ar Tieslietu ministrijas (*DoJ*) starpniecību) ir arī sniegusi apliecinājumus par piemērojamiem ierobežojumiem un aizsardzības pasākumiem (šā lēmuma VI pielikums).

#### 3.1.1. ***Juridiskais pamats, ierobežojumi un garantijas***

##### 3.1.1.1. *Ierobežojumi un aizsardzības pasākumi attiecībā uz personas datu vākšanu krimināltiesību aizsardzības nolūkos*

(91) Personas datiem, ko apstrādā sertificētas ASV organizācijas un kas tiktu nosūtīti no Savienības, pamatojoties uz ES un ASV DPR, ASV federālie prokurori un federālie izmeklētāji krimināltiesību aizsardzības nolūkos var piekļūt saskaņā ar dažādām procedūrām, kā sīkāk paskaidrots 92.–99. apsvērumā. Šīs procedūras piemēro vienādi, ja informācija tiek iegūta no jebkuras ASV organizācijas neatkarīgi no attiecīgo datu subjektu valstspiederības vai dzīvesvietas ([152]).

(92) Pirmkārt, pēc federālā tiesībaizsardzības iestādes darbinieka vai valdības advokāta pieprasījuma tiesnesis var izdot orderi kratīšanai vai konfiskācijai (arī elektroniski glabātas informācijas) ([153]). Šādu orderi var izdot tikai tad, ja pastāv "pamatots iemesls" ([154]), ka orderī norādītajā vietā ir atrodami "konfiscējami priekšmeti" (noziedzīga nodarījuma pierādījumi, nelikumīgi turēti priekšmeti vai manta, kas paredzēta vai plānota izmantošanai vai izmantota noziedzīga nodarījuma izdarīšanā). Orderī jānorāda konfiscējamā manta vai priekšmets un jānorāda tiesnesis, kuram orderis ir jāatgriež. Persona, kas pakļauta kratīšanai vai kuras īpašums ir pakļauts kratīšanai, var

([150]) Sk. spriedumu lietā *Schrems II*, 181. un 182. punktu.

([151]) Sk. spriedumu lietā *Schrems I*, 95. punktu, un spriedumu lietā *Schrems II*, 194. punktu. Šajā sakarā EST ir īpaši uzsvērusi, ka Pamattiesību hartas 47. panta ievērošana, garantējot tiesības uz efektīvu tiesisko aizsardzību neatkarīgā un objektīvā tiesā, "atbilst arī Eiropas Savienībā prasītajam aizsardzības līmenim, kura ievērošana Komisijai ir jākonstatē, pirms tā pieņem lēmumu par atbilstību [aizsardzības līmeņa pietiekamību] saskaņā ar Regulas (ES) 2016/679 45. panta 1. punktu" (spriedums lietā *Schrems II*, 186. punkts).

([152]) Sk. VI pielikumu. Skatīt, piemēram, attiecībā uz Likumu par telefona sarunu noklausīšanos (*Wiretap Act*), Glabāta saziņas satura likumu (*Stored Communications Act*) un Likumu par zvanīto numuru reģistrētājiem (*Pen Register Act*) (sīkāk minēti 95.–98. apsvērumā), *Suzlon Energy Ltd v. Microsoft Corp., 671 F.3d 726, 729* (9th Cir. 2011).

([153]) Federālie kriminālprocesa noteikumi (*Federal Rules of Criminal Procedure*), 41. not. 2018. gada spriedumā Augstākā tiesa apstiprināja, ka kratīšanas orderis vai ordera izņēmums ir nepieciešams arī tiesībaizsardzības iestādēm, lai piekļūtu vēsturiskiem mobilo sakaru staciju atrašanās vietu ierakstiem, kas sniedz visaptverošu pārskatu par lietotāja pārvietošanos, un ka lietotājam var būt pamatotas cerības uz privātumu attiecībā uz šādu informāciju*(Timothy Ivory Carpenter* / Amerikas Savienotās Valstis, Nr. 16-402, 585 U.S. (2018)). Tāpēc šādus datus no mobilo sakaru uzņēmuma parasti nevar iegūt, pamatojoties uz tiesas rīkojumu, ja ir pamatots iemesls uzskatīt, ka informācija ir relevanta un būtiska notiekošai krimināllizmeklēšanai, bet, ja tiek izmantots orderis, ir jāpierāda pamatota iemesla pastāvēšana.

([154]) Augstākā tiesa uzskata, ka "pamatots iemesls" ir "praktisks, netehnisks" standarts, kas balstās uz "ikdienas dzīves faktu un praktiskiem apsvērumiem, saskaņā ar kuriem rīkojas saprātīgi un apdomīgi cilvēki (..)"*(Illinois/Gates*, 462 U.S. 213, 232 (1983)). Attiecībā uz kratīšanas orderiem pamatots iemesls pastāv tad, ja pastāv pamatota varbūtība, ka kratīšanā tiks atrasti noziedzīga nodarījuma pierādījumi (turpat).

pieprasīt neatklāt pierādījumus, kas iegūti nelikumīgas kratīšanas rezultātā vai izriet no šādas kratīšanas, ja šie pierādījumi tiek iesniegti pret šo personu kriminālprocesā ([155]). Ja datu turētājam (piemēram, uzņēmumam) tiek pieprasīts izpaust datus saskaņā ar orderi, tas var jo īpaši apstrīdēt šādu izpaušanas prasību kā pārmērīgi apgrūtinošu ([156]).

(93) Otrkārt, tiesas pavēsti var izdot zvērinātie (tiesas izmeklēšanas daļa, ko sasauc tiesnesis vai miertiesnesis) saistībā ar konkrētu smagu noziegumu ([157]) izmeklēšanu, parasti pēc federālā prokurora pieprasījuma, lai prasītu kādam iesniegt vai darīt pieejamus komercdarbības dokumentus, elektroniski glabātu informāciju vai citus materiālus vienumus. Papildus tam vairākos federālajos likumos ir atļauts izmantot administratīvās pavēstes, lai panāktu, ka tiek sagatavoti vai darīti pieejami komercdarbības dokumenti, 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 ([158]). Abos gadījumos informācijai ir jābūt relevantai izmeklēšanai, un tiesas pavēste nedrīkst būt nepamatota, t. i., pārāk vispārīga, patvaļīga vai apgrūtinoša (un tiesas pavēstes saņēmējs to var apstrīdēt, pamatojoties uz šiem iemesliem) ([159]).

(94) Ļoti līdzīgi nosacījumi attiecas uz administratīvām pavēstēm, kas izdotas, lai pieprasītu piekļuvi datiem, kuri ir ASV uzņēmumu rīcībā civiliem vai regulatīviem ("sabiedrības interešu") nolūkiem. Aģentūru, kuras pilda civilas vai regulatīvas funkcijas, pilnvaras izdot šādas administratīvās pavēstes ir jāparedz tiesību aktā. Administratīvās pavēstes izmantošanai tiek piemērota "pamatotības pārbaude", kas paredz, ka izmeklēšana tiek veikta saskaņā ar likumīgu nolūku, ar pavēsti pieprasītā informācija attiecas uz šo nolūku, ar pavēsti pieprasītā informācija aģentūrai jau nav pieejama un ir izpildīti pavēstes izdošanai nepieciešamie administratīvie soļi ([160]). Augstākās tiesas judikatūrā arī ir precizēta nepieciešamība līdzsvarot sabiedrības interešu nozīmīgumu pieprasītajā informācijā ar personas un organizācijas privātuma interešu nozīmīgumu ([161]). Lai arī administratīvās pavēstes izmantošanai nav nepieciešama iepriekšēja tiesas atļauja, to var izvērtēt tiesā, ja uz iepriekšminētā pamata to apstrīd saņēmējs vai ja izdevējaģentūra vēršas tiesā, lai pavēsti izpildītu ([162]). Papildus šiem vispārīgajiem ierobežojumiem, atsevišķos tiesību aktos var būt paredzētas konkrētas (stingrākas) prasības ([163]).

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

([156]) Sk. *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (kurā uzskatīts, ka "pienācīgā procesā nepieciešama uzklausīšana jautājumā par apgrūtinājumu, pirms liek tālruņa sakaru uzņēmumu sniegt" palīdzību saistībā ar kratīšanas orderi) un *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

([157]) ASV Konstitūcijas piektais grozījums paredz, ka zvērinātajiem ir jāceļ apsūdzība par ikvienu "ar nāvi sodāmu vai citādu smagu noziedzīgu nodarījumu". Iepriekšējas izmeklēšanas zvērināto tiesā ir no 16 līdz 23 zvērināto, un tie nosaka, vai pastāv pamatots iemesls uzskatīt, ka ir izdarīts noziegums. Lai nonāktu pie šāda secinājuma, iepriekšējas izmeklēšanas zvērināto tiesām ir piešķirtas izmeklēšanas pilnvaras, kas ļauj tām izdot pavēstes.

([158]) Sk. VI pielikumu.

([159]) Federālie kriminālprocesa noteikumi, 17. not.

([160]) *United States v. Powell*, 379 U.S. 48 (1964)

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

([162]) Augstākā tiesa ir precizējusi, ka administratīvas pavēstes apstrīdēšanas gadījumā tiesai ir jāvērtē, vai 1) izmeklēšana tiek veikta likumā pamatotā nolūkā, 2) Kongresam ir atļauts pieprasīt konkrētās pavēstes izmantošanas pilnvaras un 3) "pieprasītie dokumenti ir izmeklēšanai relevanti". Tiesa arī ir norādījusi, ka administratīvas pavēstes pieprasījumam ir jābūt "saprātīgam", t. i. "jānorāda iesniedzamie dokumenti, kas atbilst, bet nepārsniedz attiecīgās izmeklēšanas nolūku", ieskaitot "precizitāti aprakstot pārmeklējamo vietu un personas vai priekšmetus, kas konfiscējami".

([163]) Piemēram, Likums par tiesībām uz finanšu datu aizsardzību (*Right to Financial Privacy Act*) valsts iestādei paredz tiesības izmantot administratīvu pavēsti, lai iegūtu finanšu iestādes glabātus finanšu datus, tikai, ja 1) ir pamats uzskatīt, ka pieprasītie dati ir saistīti ar leģitīmu tiesībaizsardzības iestāžu izmeklēšanu un 2) klientam ir izsniegta pavēstes kopija kopā ar paziņojumu, kurā ar saprātīgu precizitāti ir norādīts izmeklēšanas raksturs (12 U.S.C. §3405). Vēl viens piemērs ir Likums par godīgu kredītinformāciju (*Fair Credit Reporting Act*), kas patērētāju kredītu uzraudzības iestādēm, atbildot uz administratīvas pavēstes pieprasījumiem, aizliedz atklāt patērētāja kredītinformāciju (tām ir atļauts atbildēt tikai uz zvērināto pavēstēm vai tiesas rīkojumiem, 15 U.S.C. §1681 et seq.). Uz piekļuvi saziņas datiem attiecas Glabātās saziņas satura likuma konkrētās prasības, ieskaitot attiecībā uz iespēju izmantot administratīvas pavēstes (detalizētu pārskatu skatīt 96. un 97. apsvērumā).

(95) Treškārt, iegūt piekļuvi sakaru datiem krimināltiesību aizsardzības iestādēm ļauj vairāki juridiskie pamati. Tiesa var izdot rīkojumu, ar ko atļauj saistībā ar noteiktu tālruņa numuru vai e-pastu vākt reāllaika informāciju par zvanīšanu, maršrutēšanu, adresēšanu un signalizēšanu, kas nav saistīta ar saturu (izmantojot zvanīto numuru reģistrētāju vai uztveršanas un izsekošanas ierīci), ja tā konstatē, ka iestāde ir apliecinājusi, ka informācija, ko varētu iegūt, ir būtiska notiekošai krimināLizmeklēšanai ([164]). Rīkojumā cita starpā jānorāda aizdomās turētā identitāte, ja tāda zināma, tos sakaru raksturlielumus, uz kuriem tas attiecas, un paziņojums par nodarījumu, uz kuru attiecas vācamā informācija. Zvanīto numuru reģistrētāju vai uztveršanas un izsekošanas ierīču izmantošanu var atļaut ne ilgāk kā uz sešdesmit dienām, un šo termiņu var pagarināt tikai ar jaunu tiesas rīkojumu.

(96) Turklāt piekļuvi abonentu informācijai, datplūsmas datiem un saglabātajam saziņas saturam, ko glabā interneta pakalpojumu sniedzēji, tālruņu sakaru uzņēmumi un citi trešo personu pakalpojumu sniedzēji, krimināltiesību aizsardzības nolūkos var iegūt, pamatojoties uz Glabāta saziņas satura likumu ([165]). Lai iegūtu glabātās elektroniskās saziņas saturu, krimināltiesību aizsardzības iestādēm principā ir jāsaņem no tiesneša attiecīgs orderis, pamatojoties uz pamatotu iemeslu uzskatīt, ka konkrētajā kontā ir noziedzīga nodarījuma pierādījumi ([166]). Lai iegūtu abonentu reģistrācijas informāciju, IP adreses un saistītos laika zīmolus, kā arī norēķinu informāciju, krimināltiesību aizsardzības iestādes var izmantot pavēsti. Attiecībā uz vairumu pārējās glabātās nesatura informācijas, piemēram, e-vēstuļu galvenēm bez tēmas rindiņas, krimināltiesību aizsardzības iestādei ir jāiegūst tiesas rīkojums, kas tiks izdots, ja tiesnesis būs pārliecināts, ka ir pamatots iemesls uzskatīt, ka pieprasītā informācija ir relevanta un būtiska notiekošai krimināLizmeklēšanai.

(97) Pakalpojumu sniedzēji, kas saņem pieprasījumus saskaņā ar Glabāta saziņas satura likumu, var brīvprātīgi par to paziņot klientam vai abonentam, kura informācija tiek pieprasīta, izņemot gadījumus, kad attiecīgā krimināltiesību aizsardzības iestāde saņem aizsardzības rīkojumu, kas aizliedz šādu paziņošanu ([167]). Šāds aizsardzības rīkojums ir tiesas rīkojums, ar kuru elektronisko sakaru pakalpojumu sniedzējam vai attālās datošanas pakalpojumu sniedzējam, kuram adresēts orderis, pavēste vai tiesas rīkojums, pieprasa tik ilgi, cik tiesa uzskata par vajadzīgu, nepaziņot nevienai citai personai par ordera, pavēstes vai tiesas rīkojuma esību. Aizsardzības rīkojumus izdod gadījumos, kad tiesa konstatē, ka ir pamats uzskatīt, ka paziņošana nopietni kaitētu izmeklēšanai vai nepamatoti aizkavētu tiesas procesu, piemēram, tāpēc, ka tiktu apdraudēta personas dzīvība vai fiziskā drošība, notiktu bēgšana no krimināLvajāšanas, potenciālo liecinieku iebiedēšana utt. Ģenerālprokurora vietnieka memorandā (kas ir saistošs visiem *DoJ* advokātiem un amatpersonām) noteikts, ka prokuroriem ir sīki jāizvērtē aizsardzības rīkojuma izdošanas nepieciešamība un jāiesniedz tiesai pamatojums par to, kā konkrētajā lietā ir izpildīti likumā noteiktie kritēriji aizsardzības rīkojuma iegūšanai ([168]). Memorandā arī noteikts, ka aizsardzības rīkojumu pieteikumos parasti nedrīkst prasīt, lai paziņošana tiktu atlikta uz laiku, kas ilgāks par vienu gadu. Ja izņēmuma gadījumos varētu būt nepieciešami rīkojumi, kuros norādīts ilgāks laikposms, šādus rīkojumus var pieprasīt tikai ar ASV ģenerālprokurora vai attiecīgā ģenerālprokurora palīga norīkota uzrauga rakstisku piekrišanu. Turklāt prokuroram, izbeidzot izmeklēšanu, ir nekavējoties jāizvērtē, vai ir pamats saglabāt jebkādus spēkā esošos aizsardzības rīkojumus, un, ja tas tā nav, aizsardzības rīkojuma spēkā esība ir jāizbeidz un jānodrošina, ka par to tiek paziņots pakalpojumu sniedzējam ([169]).

([164]) 18 U.S.C. §3123.

([165]) 18 U.S.C. §§ 2701-2713.

([166]) 18 U.S.C. §§ 2701(a)-(b)(1)(A). Ja attiecīgajam abonentam vai klientam tas ir attiecīgi paziņots (iepriekš vai noteiktos apstākļos – ar aizkavētu paziņojumu), satura informāciju, kas tiek glabāta ilgāk nekā 180 dienas, var iegūt arī, pamatojoties uz administratīvu pavēsti vai zvērināto pavēsti (18 U.S.C. §§ 2701(b)(1)(B)), vai tiesas rīkojumu (ja ir pamatots iemesls uzskatīt, ka informācija ir relevanta un būtiska notiekošai krimināLizmeklēšanai (18 U.S.C. §§ 2701(d)). Tomēr saskaņā ar federālās apelācijas tiesas nolēmumu valdības izmeklētāji kratīšanas orderus parasti saņem no tiesnešiem, lai no komerciāla sakaru pakalpojumu sniedzēja iegūtu privātās saziņas saturu vai saglabātos datus. Amerikas Savienotās Valstis / *Warshak*, 631 F.3d 266 (*6th Cir.*, 2010).

([167]) 18 U.S.C. § 2705(b).

([168]) Sk. ģenerālprokurora vietnieka *Rod Rosenstein* 2017. gada 19. oktobrī izdoto memorandu par stingrāku politiku attiecībā uz aizsardzības (vai neizpaušanas) rīkojumu pieteikumiem, kas pieejams https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Ģenerālprokurora vietnieces *Lisa Monaco* 2022. gada 27. maijā izdotais memorands par papildu politiku attiecībā uz aizsardzības rīkojumu pieteikumiem saskaņā ar 18 U.S.C. §2705(b).

(98) Krimināltiesību aizsardzības iestādes var arī reāllaikā pārtvert fiksēto tālruņa līniju, mutisko vai elektronisko saziņu, pamatojoties uz tiesas rīkojumu, kurā tiesnesis cita starpā konstatē, ka pastāv pamatots iemesls uzskatīt, ka sarunu noklausīšanās vai elektroniskās saziņas pārtveršana nodrošinās federāla noziedzīga nodarījuma pierādījumus vai informāciju par tādas personas atrašanās vietu, kura izvairās no kriminālvajāšanas ([170]).

(99) Papildu aizsardzību nodrošina dažādi Tieslietu ministrijas politikas dokumenti un vadlīnijas, tajā skaitā Ģenerālprokurora vadlīnijas FIB iekšzemes operācijām (*AGG DOM*), kas cita starpā paredz, ka Federālais izmeklēšanas birojs (FIB) izmanto iespējami mazāk invazīvas izmeklēšanas metodes, ņemot vērā ietekmi uz privātumu un pilsoniskajām brīvībām ([171]).

(100) Saskaņā ar ASV valdības apgalvojumiem tāda pati vai lielāka aizsardzība, kāda aprakstīta iepriekš, ir piemērojama tiesībaizsardzības iestāžu veiktai izmeklēšanai štata līmenī (attiecībā uz izmeklēšanu, ko veic saskaņā ar štata likumiem) ([172]). Jo īpaši, konstitucionāli noteikumi, kā arī štata līmeņa tiesību akti un judikatūra atkārtoti apstiprina iepriekšminētos aizsardzības pasākumus pret nepamatotu kratīšanu un konfiskāciju, paredzot, ka ir jāizdod kratīšanas orderis ([173]). Līdzīgi federālā līmenī paredzētajai aizsardzībai kratīšanas orderi var izdot, tikai ja tiek apliecināts pamatotas iemesls, un tajā ir jābūt norādītai kratīšanas vietai un personām vai priekšmetiem, kas konfiscējami ([174]).

([170]) 18 U.S.C. §§ 2510-2522.

([171]) *Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (September 2008)*, skatīt http://www.justice.gov/archive/opa/docs/guidelines.pdf. Papildu noteikumi un politika, no kā izriet federālo prokuroru izmeklēšanas darbību ierobežojumi, ir izklāstīti Amerikas Savienoto Valstu Prokuroru rokasgrāmatā; pieejama šeit: http://www.justice.gov/usam/united-states-attorneys-manual. Lai atkāptos no šīm vadlīnijām, ir jāsaņem iepriekšējs apstiprinājums no FIB direktora, direktora vietnieka vai direktora norīkota izpilddirektora palīga, izņemot gadījumus, kad šādu apstiprinājumu nav iespējams saņemt, jo pastāv tūlītējs vai nopietns apdraudējums personu vai īpašuma drošībai vai nacionālajai drošībai (šādā gadījumā direktoram vai citai pilnvarotajai personai par to ir jāpaziņo, cik drīz vien praktiski iespējams). Ja vadlīnijas netiek ievērotas, FIB par to jāinformē *DoJ*, kas savukārt informē ģenerālprokuroru un ģenerālprokurora vietnieku.

([172]) VI pielikuma 2. zemsvītras piezīme. Sk. arī, piemēram, *Arnold v. City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) ("Personu tiesību un pilsonisko brīvību jomā ASV Konstitūcija, ciktāl tā attiecas uz štatiem, nodrošina minimumu, kas visos štata tiesas lēmumiem noteikti jānodrošina"); *Cooper v. California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) ("Mūsu viedoklis, protams, neietekmē štata pilnvaras noteikt augstākus standartus kratīšanai un konfiskācijai, nekā paredzēts federālajā konstitūcijā, ja tas izvēlas šādi rīkoties"); *Petersen / City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) ("Lai arī Arizonas štata konstitūcija var paredzēt stingrākus standartus attiecībā uz kratīšanu un konfiskāciju, nekā paredzēts federālajā konstitūcijā, Arizonas tiesas nedrīkst sniegt mazāku aizsardzību, kā paredzēts Ceturtajā grozījumā").

([173]) Vairums štatu savās konstitūcijās ir atkārtojuši Ceturtajā grozījumā paredzētos aizsardzības pasākumus. Sk. *Alabama Const. art. I, § 5)*; *Alaska Const. art. I, § 14*; *1*; *Arkansas Const. art. II, § 15*; *California Const. art. I, § 13*; *Colorado Const. art. II, § 7*; *Conneticut Const. art. I, § 7*; *Delaware Const. art. I, § 6*; *Florida Const. art. I, § 12*; *Georgia Const. art. I, § I, para. XIII*; *Hawai Const. art. I, § 7*; *Idaho Const. art. I, § 17*; *Illinois Const. art. I, § 6*; *Indiana Const. art. I, § 11*; *Iowa Const. art. I, § 8*; *Kansas Const. Bill of Rights, § 15*; *Kentucky Const. § 10*; *Louisiana Const. art. I, § 5*; *Maine Const. art. I, § 5*; *Massachusets Const. Decl. of Rights art. 14*; *Michigan Const. art. I, § 11*; *Minnesota Const. art. I, § 10*; *Mississippi Const. art. III, § 23*; *Missouri Const. art. I, § 15*; *Montana Const. art. II, § 11*; *Nebraska Const. art. I, § 7*; *Nevad Const. art. I, § 18*; *New Hampshire Const. pt. 1, art. 19*; *N.J. Const. art. II, § 7*; *New Mexico Const. art. II, § 10*; *New York Const. art. I, § 12*; *North Dakota Const. art. I, § 8*; *Ohio Const. art. I, § 14*; *Oklahoma Const. art. II, § 30*; *Oregon Const. art. I, § 9*; *Pennsylvania Const. art. I, § 8*; *Rhode Island Const. art. I, § 6*; *South Carolina Const. art. I, § 10*; *South Dakota Const. art. VI, § 11*; *Tennessee Const. art. I, § 7*; *Texas Const. art. I, § 9*; *Utah Const. art. I, § 14*; *Vermont Const. ch. I, art. 11*; *West Virginia Const. art. III, § 6*; *Wisconsin Const. art. I, § 11*; *Wyoming Const. art. I, § 4*. Citi štati (piemēram, Merilenda, Ziemeļkarolīna un Virdžīnija) savās konstitūcijās ir iekļāvuši konkrētus formulējumus attiecībā uz orderiem, ko tiesa ir interpretējusi kā tādus, kas nodrošina līdzīgu vai augstāku aizsardzības līmeni, kāds paredzēts Ceturtajā grozījumā (sk. *Maryland. Decl. of Rts. art. 26*; *North Carolina Const. art. I, § 20*; *Virginia Const. art. I, § 10*, un attiecīgo judikatūru, piemēram, *Hamel v. State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; *State v. Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) un *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). Visbeidzot, Arizonas un Vašingtonas štatā ir konstitucionālas normas, kas nodrošina vispārīgāku privātuma aizsardzību (*Arizona Const. art. 2, § 8*; *Washington Const. art. I, § 7*), ko tiesas ir interpretējušas kā tādas, kas nodrošina augstāku aizsardzības līmeni nekā paredzēts Ceturtajā grozījumā (skatīt, piemēram, lietas *State v. Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State v. Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984) , *State v. Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994) ).

([174]) Skatīt, piemēram, *California Penal Code § 1524,3(b)*; *Rule 3.6-3.13 Alabama Rules of Criminal Procedure*; *Section 10.79.035*; *Revised Code of Washington*; *Section 19.2-59 of Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia*.

3.1.1.2. *Savāktās informācijas turpmāka izmantošana*

(101) Attiecībā uz federālo krimināltiesību aizsardzības iestāžu savākto datu turpmāku izmantošanu dažādos likumos, pamatnostādnēs un standartos ir paredzētas īpašas garantijas. Izņemot specifiskos instrumentus, kas attiecināmi uz FIB veiktām darbībām (*AGG DOM* un FIB iekšzemes izmeklēšanas un operāciju vadlīnijas), šajā iedaļā aprakstītās prasības kopumā attiecas uz datu, ieskaitot datus, kam piekļūts civilos vai regulatīvos nolūkos, turpmāku izmantošanu jebkurā federālajā iestādē. Tas ietver prasības, kas izriet no Pārvaldības un budžeta biroja norādījumiem/noteikumiem, Federālā informācijas drošības pārvaldības modernizācijas likuma (*Federal Information Security Management Modernization Act*), E-pārvaldes likuma (*E-Government Act*) un Federālā reģistru likuma (*Federal Records Act*).

(102) Pamatojoties uz Klingera–Koena likumā (*Clinger–Cohen Act*) (P.L. 104-106, Division E) un 1987. gada Datordrošības likumā (*Computer Security Act*) (P.L. 100-235) tam piešķirtajām pilnvarām Pārvaldības un budžeta birojs (*OMB*) izdeva *Circular No. A-130*, nosakot vispārēji saistošus norādījumus, kas attiecas uz visām federālajām aģentūrām (ieskaitot tiesībaizsardzības iestādes) identitātes informācijas apstrādes ietvaros ([175]). Jo īpaši apkārtrakstā ir noteikts, ka visām federālajām aģentūrām ir "jāierobežo identitātes informācijas radīšana, vākšana, izmantošana, apstrāde, glabāšana, uzturēšana, izplatīšana un izpaušana tikai tādā apjomā, kas ir likumīgi atļauts, relevants un pamatoti uzskatāms par nepieciešamu pilnvarotu aģentūras funkciju pienācīgai izpildei" ([176]). Turklāt, ciktāl praktiski iespējams, federālajām aģentūrām ir jānodrošina, lai identitātes informācija būtu precīza, relevanta, savlaicīga un pilnīga, un jāsamazina tās apjoms līdz minimumam, kas nepieciešams aģentūras funkciju pienācīgai izpildei. Raugoties vispārīgāk, federālajām aģentūrām jāizveido visaptveroša privātuma programma, lai nodrošinātu atbilstību piemērojamām privātuma prasībām, jāizstrādā un jāizvērtē privātuma politika un jāpārvalda privātuma riski; jāuztur procedūras, kas izmantojamas, lai atklātu un dokumentētu privātuma atbilstības incidentus, un ziņotu par tiem; jāizstrādā privātuma izpratnes uzlabošanas un apmācības programmas darbiniekiem un darbuzņēmējiem; kā arī jāievieš politika un procedūras, kas nodrošinātu, ka darbinieki ir atbildīgi par privātuma prasību un politikas ievērošanu ([177]).

(103) Turklāt E-pārvaldes likums ([178]) paredz, ka visām federālajām aģentūrām (arī krimināltiesību aizsardzības iestādēm) jāievieš informācijas drošības aizsardzības pasākumi, kas ir samērīgi ar risku un kaitējuma apmēru, ko varētu radīt neatļauta piekļuve datiem, to izmantošana, izpaušana, bojāšana, pārveidošana vai iznīcināšana; ir vajadzīgs direktors informācijas jautājumos, kas nodrošina atbilstību informācijas drošības prasībām un veic ikgadēju neatkarīgu aģentūras informācijas drošības programmu un prakses izvērtēšanu (to ieceļ, piemēram, ģenerālinspektors; sk. 109. apsvērumu) ([179]). Tāpat Federālo reģistru likums (*FRA*) ([180]) un papildu noteikumi ([181]) paredz, ka federālo aģentūru rīcībā esošajai informācijai ir jāpiemēro garantijas, ar ko nodrošina informācijas fizisko integritāti un aizsargā to pret neatļautu piekļuvi.

(104) Saskaņā ar tiesību aktos (tajā skaitā 2014. gada Likumā par federālās informācijas drošības modernizāciju (*Federal Information Security Modernisation Act*)) noteiktajām federālās varas pilnvarām, *OMB* un Nacionālais standartu un tehnoloģiju institūts (*NIST*) ir izstrādājuši standartus, kas ir saistoši federālajām aģentūrām (arī krimināltiesību aizsardzības iestādēm) un kas sīkāk nosaka obligātās informācijas drošības prasības, kuras jāievieš, tajā skaitā piekļuves kontroles, informētības un apmācības nodrošināšana, ārkārtas rīcības plānošana, reaģēšana uz incidentiem, revīzijas un pārskatatbildības rīki, sistēmu un informācijas integritātes nodrošināšana, privātuma un drošības riska novērtējumu veikšana utt ([182]). Turklāt visām federālajām aģentūrām (arī krimināltiesību aizsardzības

([175]) T. i., "informācija, ko var izmantot, lai atšķirtu vai izsekotu personas identitāti atsevišķi vai kopā ar citu informāciju, kas ir saistīta vai sasaistāma ar konkrētu personu", sk. *OMB Circular* Nr. A-130, 33. lpp. (termina "identitātes informācija" definīcija).

([176]) *OMB Circular* Nr. A-130, *Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information*, 81 Fed. Reg. 49,689 (2016. gada 28. jūlijs), 17. lpp.

([177]) *Appendix II, §5(a)-(h).*

([178]) 44 U.S.C. *Chapter 36*.

([179]) 44 U.S.C. §§ 3544-3545.

([180]) *FAC*, 44 U.S.C. § 3105.

([181]) 36 C.F.R. §§ 1228,150, et seq., 1228,228, un *Appendix A*.

([182]) Sk., piemēram, *OMB Circular* Nr. A-130; *NIST SP 800–53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations* (2020. gada 10. decembris), kā arī *NIST* federālos informācijas apstrādes standartus Nr. 200 *Minimum Security Requirements for Federal Information and Information Systems*.

iestādēm) saskaņā ar *OMB* vadlīnijām ir jāuztur un jāīsteno plāns, kurā noteikts, kā rīkoties datu aizsardzības pārkāpumu gadījumos – arī gadījumos, kad jāreaģē uz šādiem pārkāpumiem un jānovērtē kaitējuma risks ([183]).

(105) Attiecībā uz datu saglabāšanu *FRA* ([184]) ir noteikts, ka ASV federālajām aģentūrām (arī krimināltiesību aizsardzības iestādēm) ir jānosaka savu ierakstu saglabāšanas termiņi (pēc kuriem šādi ieraksti ir jāiznīcina), un Nacionālajai arhīvu un ierakstu administrācijai tas jāapstiprina ([185]). Šo saglabāšanas termiņu nosaka, ņemot vērā dažādus faktorus, piemēram, izmeklēšanas veidu, to, vai pierādījumi joprojām ir relevanti izmeklēšanai utt. Attiecībā uz FIB *AGG DOM* ir noteikts, ka FIB ir jāievieš šāds ierakstu saglabāšanas plāns un jāuztur sistēma, kas ļauj ātri iegūt informāciju par izmeklēšanas statusu un pamatojumu.

(106) Visbeidzot, *OMB Circular* Nr. A-130 ir arī noteiktas prasības saistībā ar identitātes informācijas izplatīšanu. Principā identitātes informācijas izplatīšana un atklāšana ir jāierobežo līdz tādam apmēram, kas ir likumīgi atļauts, attiecināms un saprātīgi uzskatāms par nepieciešamu, lai pilnvērtīgi izpildītu aģentūras darba uzdevumus ([186]). Koplietojot identitātes informāciju ar citām valdības iestādēm, ASV federālajām aģentūrām attiecīgā gadījumā ir jāparedz nosacījumi (tajā skaitā īpašu drošības un privātuma kontroles pasākumu īstenošana), kas reglamentē informācijas apstrādi, izmantojot rakstiskas vienošanās (tajā skaitā līgumus, datu izmantošanas nolīgumus, informācijas apmaiņas nolīgumus un saprašanās memorandus) ([187]). Attiecībā uz informācijas izplatīšanas pamatu *AGG DOM* un FIB iekšzemes izmeklēšanas un operāciju vadlīnijas ([188]), piemēram, paredz, ka FIB var būt juridisks pienākums tā rīkoties (piem., saskaņā ar starptautisku līgumu) vai arī informāciju var būt atļauts izplatīt noteiktos apstākļos, piemēram, citām ASV aģentūrām, ja informācijas atklāšana ir saderīga ar nolūku, kādā informācija tika savākta, un šāda rīcība ir saistīta ar pienākumu izpildi; kongresa komitejām; ārvalstu aģentūrām, ja informācija ir saistīta ar to pienākumiem un tās izplatīšana atbilst ASV interesēm; informācijas izplatīšana ir jo īpaši nepieciešama, lai aizsargātu personu vai īpašuma drošumu vai drošību vai lai aizsargātos pret noziedzīgu nodarījumu vai nacionālās drošības apdraudējumu vai tos novērstu, un informācijas atklāšana ir saderīga ar nolūku, kuram informācija ir savākta ([189]).

3.1.2. ***Pārraudzība***

(107) Federālo krimināltiesību aizsardzības iestāžu darbību pārrauga dažādas struktūras ([190]). Kā paskaidrots 92.–99. apsvērumā, vairumā gadījumu tas ietver sākotnēju tiesas veiktu pārraudzību, kam ir jāatļauj atsevišķi vākšanas pasākumi, pirms tos ir iespējams izmantot. Turklāt citas struktūras pārrauga dažādus krimināltiesību aizsardzības iestāžu darbības posmus, ieskaitot personas datu vākšanu un apstrādi. Kopā šīs tiesas un ārpustiesas struktūras nodrošina, ka tiesībaizsardzības iestādes tiek neatkarīgi pārraudzītas.

([183]) *Memorandum 17-12, 'Preparing for and Responding to a Breach of Personally Identifiable Information'*, pieejams https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, un *OMB Circular* Nr. A-130. Piemēram, Tieslietu ministrijas procedūras reaģēšanai uz datu aizsardzības pārkāpumiem; sk. https://www.justice.gov/file/4336/download.

([184]) *FRA*, 44 U.S.C. §§3101 et seq.

([185]) Nacionālā arhīvu un ierakstu administrācija ir pilnvarota novērtēt aģentūru ierakstu pārvaldības praksi un var noteikt, vai ir pamatoti turpināt atsevišķu ierakstu saglabāšanu (44 U.S.C. §§ 2904(c), 2906).

([186]) *OMB Circular* Nr. A-130, *Section 5.f.1.(d)*

([187]) *OMB Circular* Nr. A-130, *Appendix I §3(d)*.

([188]) Skatīt arī FIB iekšzemes izmeklēšanas un operāciju vadlīniju (*FBI Domestic Investigation and Operations Guide – DIOG*) 14. iedaļu.

([189]) *AGG-DOM*, *Section VI, B* un *C*; FIB iekšzemes izmeklēšanas un operāciju vadlīniju (*DIOG*) 14. iedaļu.

([190]) Šajā iedaļā minētie mehānismi arī attiecas uz federālu iestāžu veiktu datu vākšanu un izmantošanu civilos un regulatīvos nolūkos. Federālās civilās un regulatīvās iestādes pārrauga attiecīgie ģenerālinspektori un Kongress, ieskaitot Valdības pārskatatbildības biroju, kas ir Kongresa revīzijas un izmeklēšanas aģentūra. Ja vien aģentūrā nav privātuma un civilo brīvību speciālists (šāds amats parasti ir tādās aģentūrās kā Tieslietu ministrijā un Iekšzemes drošības ministrijā (*DHS*) to tiesībaizsardzības un nacionālās drošības uzdevumu dēļ), šos pienākumus pilda aģentūras vecākā amatpersona privātuma jautājumos (*SAOP*). Visām federālajām aģentūrām ir tiesisks pienākums nozīmēt *SAOP*, kurā ir atbildīga par aģentūras atbilstības privātuma likumiem nodrošināšanu un ar to saistīto jautājumu pārraudzīšanu. Skatīt, piemēram, *OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016)*.

(108) Pirmkārt, dažādās iestādēs, kas atbild par krimināltiesību aizsardzību, ir privātuma un pilsonisko brīvību amatpersonas ([191]). Lai arī šo amatpersonu 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 fiziskām personām, kas uzskata, ka ir aizskarts viņu privātums un pilsoniskās brīvības. Katras ministrijas vai aģentūras vadītājiem ir jānodrošina, lai privātuma un pilsonisko brīvību amatpersonu rīcībā būtu materiāli un resursi viņu pilnvaru īstenošanai, lai viņiem būtu pieejami visi viņu funkciju veikšanai nepieciešamie materiāli un personāls, lai viņi tiktu informēti par ierosinātajām politikas izmaiņām un ar viņiem apspriestos par tām ([192]). Privātuma un pilsonisko brīvību amatpersonas periodiski ziņo Kongresam, tajā skaitā par ministrijā/aģentūrā saņemto sūdzību skaitu un raksturu, un sniedz kopsavilkumu par šādu sūdzību izskatīšanu, veiktajām pārbaudēm un izmeklēšanām un amatpersonas veikto darbību ietekmi ([193]).

(109) Otrkārt, neatkarīgs ģenerālinspektors pārrauga Tieslietu ministrijas (un arī FIB) darbību ([194]). Likumā noteikts, ka ģenerālinspektori ir neatkarīgi ([195]) un atbild par neatkarīgu izmeklēšanu, revīziju un pārbaužu veikšanu attiecībā uz ministrijas programmām un darbībām. Tiem ir piekļuve visiem ierakstiem, atskaitēm, revīziju materiāliem, pārskatiem, dokumentiem, materiāliem, ieteikumiem un citiem relevantiem materiāliem, vajadzības gadījumā ar tiesas pavēsti, un tie var iegūt liecības nopratināšanā ([196]). Lai arī ģenerālinspektori izdod tikai nesaistošus ieteikumus par korektīvām darbībām, to ziņojumi, arī par turpmāku rīcību (vai tās neveikšanu) ([197]), parasti tiek publiskoti un nosūtīti Kongresam, kas, pamatojoties uz to, var izmantot savu pārraudzības funkciju (sk. 111. apsvērumu) ([198]).

([191]) Sk. 42 U.S.C. § 2000ee-1. Tas attiecas, piemēram, uz Tieslietu ministriju, Iekšzemes drošības ministriju (*DHS*) un FIB. Turklāt *DHS* ir izveidots galvenās privātuma amatpersonas amats, un šī amatpersona atbild par privātuma aizsardzības saglabāšanu un uzlabošanu un pārredzamības veicināšanu ministrijā (*6 U.S.C. 142, Section 222*). Visas *DHS* sistēmas, tehnoloģijas, veidlapas un programmas, ar kuru palīdzību tiek vākti personas dati vai kuras ietekmē privātumu, pārrauga galvenā privātuma amatpersona, kurai ir piekļuve visiem ierakstiem, ziņojumiem, revīzijām, pārskatiem, dokumentiem, materiāliem, ieteikumiem un citiem materiāliem, kas pieejami ministrijā un ko vajadzības gadījumā var iegūt arī ar tiesas pavēsti. Privātuma amatpersonai katru gadu jāziņo Kongresam par ministrijas darbībām, kas ietekmē privātumu, tajā skaitā par sūdzībām par privātuma pārkāpumiem.

([192]) 42 U.S.C. § 2000ee-1(d).

([193]) Sk. 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). Piemēram, *DoJ* galvenās privātuma un pilsonisko brīvību amatpersonas un Privātuma un pilsonisko brīvību biroja ziņojumā par laikposmu no 2020. gada oktobra līdz 2021. gada martam norādīts, ka ir veiktas 389 privātuma pārbaudes, tajā skaitā informācijas sistēmu un citu programmu pārbaudes (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) Līdzīgi ar 2002. gada Iekšzemes drošības likumu (*Homeland Security Act*) Iekšzemes drošības ministrijā tika izveidots Ģenerālinspektora birojs.

([195]) Ģenerālinspektoram ir noteikts laiks amatā, un to var atstādināt tikai prezidents, kuram rakstveidā jāpaziņo Kongresam šādas atstādināšanas iemesli.

([196]) Sk. 1978. gada Ģenerālinspektoru likumu (*Inspector General Act of 1978*), § 6.

([197]) Šajā sakarā skatīt, piemēram, *DoJ* Ģenerālinspektora biroja sagatavoto pārskatu par *DoJ* ģenerālinspektora ieteikumiem un to, cik lielā mērā tie īstenoti, veicot turpmākus pasākumus ministrijā un aģentūrā, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

([198]) Sk. 1978. gada Ģenerālinspektoru likumu, §§ 4(5), 5. Piemēram, Tieslietu ministrijas Ģenerālinspektora birojs nesen publicēja savu pusgada ziņojumu Kongresam (par laikposmu no 2021. gada 1. oktobra līdz 2022. gada 31. martam, https://oig.justice.gov/node/23596), kurā sniegts pārskats par Tieslietu ministrijas programmu un darbību revīzijām, izvērtējumiem, pārbaudēm, īpašiem pārskatiem un izmeklēšanām. Šīs darbības ietvēra izmeklēšanu par kādu bijušo darbuzņēmēju saistībā ar elektroniskās novērošanas (fiziskas personas noklausīšanās) datu nelikumīgu izpaušanu notiekošā izmeklēšanā, kā rezultātā būvuzņēmējs tika notiesāts. Ģenerālinspektora birojs veica arī izmeklēšanu par *DoJ* aģentūru informācijas drošības programmām un praksi, kas ietvēra reprezentatīvas aģentūru sistēmu apakškopas informācijas drošības politikas, procedūru un prakses rezultativitātes pārbaudi.

(110) Treškārt, tiktāl, cik tie veic pretterorisma darbības, ministrijas ar krimināltiesību aizsardzības pienākumiem ir pakļautas Privātuma un pilsonisko brīvību pārraudzības padomes (*PCLOB*) pārraudzībai, kas ir neatkarīga izpildaģentūra, ko veido pieci locekļi no abām partijām, kurus uz fiksētu sešu gadu termiņu amatā ieceļ prezidents ar Senāta apstiprinājumu ([199]). Saskaņā ar *PCLOB* dibināšanas statūtiem tai ir uzticēti pienākumi pretterorisma politikas un tās īstenošanas jomā ar mērķi aizsargātu privātumu un pilsoniskās brīvības. Savās pārbaudēs tā var piekļūt visiem attiecīgo aģentūru ierakstiem, atskaitēm, revīziju materiāliem, pārskatiem, dokumentiem, materiāliem un ieteikumiem, veikt nopratināšanu un uzklausīt liecības ([200]). Tā saņem ziņojumus no dažādu federālo ministriju/aģentūru pilsonisko brīvību un privātuma amatpersonām ([201]), var izdot tiem ieteikumus valdībai un tiesībaizsardzības iestādēm un regulāri sniedz atskaites Kongresa komitejām un prezidentam ([202]). Padomes ziņojumi – arī Kongresam adresētajiem – jādara maksimāli pieejami publiski ([203]).

(111) Visbeidzot, krimināltiesību aizsardzības darbības pārrauga īpašas ASV Kongresa komitejas (Pārstāvju palātas un Senāta tieslietu komitejas). Tieslietu komitejas regulāri veic dažādas pārraudzības darbības, jo īpaši uzklausīšanas, izmeklēšanas, pārskatu un ziņojumu veidā ([204]).

### 3.1.3. ***Tiesiskā aizsardzība***

(112) Kā jau norādīts, krimināltiesību aizsardzības iestādēm lielākajā daļā gadījumu ir jāsaņem iepriekšēja tiesas atļauja vākt personas datus. Tas gan nav nepieciešams attiecībā uz administratīvām tiesas pavēstēm, jo tās attiecas tikai uz īpašām situācijām, un saistībā ar tām tiks veikta neatkarīga izskatīšana tiesā – vismaz tad, ja valdība vēlas panākt izpildi tiesā. Jo īpaši, administratīvo pavēstu saņēmēji var apstrīdēt tās tiesā kā nepamatotas, t. i., pārāk vispārīgas, patvaļīgas vai apgrūtinošas ([205]).

(113) Fiziskas personas, pirmkārt, var vērsties krimināltiesību aizsardzības iestādēs ar pieprasījumiem vai sūdzībām saistībā ar savu personas datu apstrādi. Tas ietver arī pieprasījumus piekļūt saviem personas datiem vai labot tos ([206]). Attiecībā uz pretterorisma darbībām fiziskas personas var iesniegt sūdzību tiesībaizsardzības iestāžu privātuma un pilsonisko brīvību amatpersonām (vai citām privātuma aizsardzības amatpersonām) ([207]).

(114) Turklāt ASV tiesību aktos personām ir paredzētas vairākas tiesiskās aizsardzības iespējas, lai vērstos pret publisku iestādi vai kādu no tās ierēdņiem, ja šīs iestādes apstrādā personas datus ([208]). Šie risinājumi, jo īpaši *APA*, Informācijas brīvības likums (*FOIA*) un Elektroniskās saziņas privātuma likums (*ECPA*), ir pieejami visām fiziskām personām neatkarīgi no viņu valstspiederības un ievērojot visus piemērojamos nosacījumus.

---

([199]) Padomes locekļi jāatlasa, pamatojoties tikai uz viņu profesionālo kvalifikāciju, sasniegumiem, publisko reputāciju, zināšanām pilsonisko brīvību un privātuma jomā un relevanto pieredzi, neņemot vērā viņu politisko piederību. Padomē nekādā gadījumā nedrīkst būt vairāk nekā trīs locekļi, kas pieder vienai un tai pašai politiskajai partijai. Padomē ieceltā persona, kamēr tā pilda savus amata pienākumus, nedrīkst būt vēlēta amatpersona, ierēdnis vai federālās valdības darbinieks, kam ir cits amats nekā tikai padomes loceklis. Sk.42 U.S.C. § 2000ee (h).

([200]) 42 U.S.C. § 2000ee (g).

([201]) Sk. 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). To vidū ir vismaz Tieslietu ministrija, Aizsardzības ministrija, Iekšzemes drošības ministrija, kā arī jebkura cita ministrija, aģentūra vai struktūra, kuru *PCLOB* atzinusi par piemērotu.

([202]) 42 U.S.C. §2000ee, (e).

([203]) 42 U.S.C. § 2000ee (f).

([204]) Piemēram, komitejas organizē tematiskas uzklausīšanas (sk., piemēram, nesen notikušo Pārstāvju palātas Tieslietu komitejas uzklausīšanu par digitālajiem sistemātiskas meklēšanas tīkliem https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), kā arī regulāras pārraudzības uzklausīšanas, piemēram, par FIB un *DoJ*, sk. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 un https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

([205]) Sk. VI pielikumu.

([206]) *OMB Circular* Nr. A-130, *Appendix II, Section 3(a)* un *(f)* paredz, ka federālajām aģentūrām ir jānodrošina atbilstoša piekļuve datiem un to labošana, ja no fiziskas personas tiek saņemts attiecīgs pieprasījums, un tām ir jāizveido procedūras ar privātumu saistītu sūdzību un pieprasījumu saņemšanai un risināšanai.

([207]) Sk. 42 U.S.C. § 2000ee-1, piemēram, attiecībā uz Tieslietu ministriju un Iekšzemes drošības ministriju. Skatīt arī *OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy.*

([208]) Šajā iedaļā minētie tiesiskās aizsardzības mehānismi arī attiecas uz federālu iestāžu veiktu datu vākšanu un izmantošanu civilos un regulatīvos nolūkos.

(115) Parasti saskaņā ar *APA* noteikumiem par izskatīšanu tiesā ([209]) "ikvienai personai, kam nodarīta juridiska netaisnība aģentūras darbības rezultātā vai ko nelabvēlīgi ietekmē vai neapmierina aģentūras darbība", ir tiesības vērsties tiesā ([210]). 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 tiesību aktiem" ([211]).

(116) Konkrēti, Elektroniskās saziņas privātuma likuma (*ECPA*) ([212]) 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, kas ir trešās personas ([213]). Tajā paredzēta krimināltatbildība 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.

(117) Turklāt vairākos tiesību aktos personām ir piešķirtas tiesības celt tiesā prasību pret ASV publisko iestādi vai amatpersonu attiecībā uz personas datu apstrādi, piemēram, Likumā par telefona sarunu noklausīšanos (*Wiretap Act*) ([214]), Likumā par datorkrāpšanu un ļaunprātīgu izmantošanu (*Computer Fraud and Abuse Act*) ([215]), Federālajā likumā par noteiktiem atlīdzināmiem kaitējumiem (*Federal Torts Claim Act*) ([216]), Likumā par tiesībām uz finanšu datu aizsardzību (*Right to Financial Privacy Act*) ([217]), un Likumā par godīgu kredītinformāciju (*Fair Credit Reporting Act*) ([218]).

([209]) 5 U.S.C. § 702.

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

([211]) 5 U.S.C. § 706(2)(A).

([212]) 18 U.S.C. §§ 2701-2712.

([213]) *ECPA* aizsargā saziņas saturu, kas ir divu noteiktu kategoriju tīkla pakalpojumu sniedzēju rīcībā, proti, šādu pakalpojumu sniedzēju rīcībā: i) elektronisko sakaru pakalpojumi, piemēram, telefonija vai e-pasts; ii) attālinātās datošanas pakalpojumi, piemēram, datoru krātuvju nodrošināšanas vai apstrādes pakalpojumi.

([214]) 18 U.S.C. §§ 2510 et seq. 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 civilprasību par Likuma par telefona sarunu noklausīšanos pārkāpšanu, tajā skaitā konkrētos apstākļos pret atsevišķu valsts amatpersonu vai Amerikas Savienotajām Valstīm. Ar saturu nesaistītas informācijas (piem., IP adrese, saņēmēja/sūtītāja e-pasta adrese) vākšanai – sk. arī 18. sadaļas nodaļu "Zvanīto numuru reģistrētāji un uztveršanas un izsekošanas ierīces" (*Pen Registers and Trap and Trace Devices*) (18 U. S.C. §§ 3121-3127 un civilprasībām – § 2707).

([215]) 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, tajā skaitā konkrētos apstākļos prasību var celt pret atsevišķu valsts amatpersonu.

([216]) 28 U.S.C. §§ 2671 et seq. Saskaņā ar Federālo likumu par noteiktiem atlīdzināmiem kaitējumiem (*Federal Tort Claims Act*), persona konkrētos apstākļos var celt prasību pret Amerikas Savienotajām Valstīm attiecībā uz "jebkura valsts iestādes darbinieka nolaidīgu vai nelikumīgu darbību vai bezdarbību amata vai darba pienākumu izpildē."

([217]) 12 U.S.C. §§ 3401 et seq. 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.

([218]) 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.

(118) Vienlaikus saskaņā ar *FOIA* ([219]), 5 U.S.C. § 552, ikvienai personai ir tiesības iegūt piekļuvi federālo aģentūru datiem, arī tādiem, kas satur attiecīgās personas datus. Pēc administratīvo tiesiskās aizsardzības līdzekļu izsmelšanas fiziska persona var vērsties tiesā, lai izmantotu šīs tiesības, ja vien šo datu publiskošanu neaizliedz izņēmums vai īpaša izslēgšana tiesībaizsardzības nolūkos ([220]). Tādā gadījumā tiesa izvērtē, vai ir piemērojams kāds izņēmums vai uz tādu likumīgi atsaucas attiecīgā publiskā iestāde.

### 3.2. **ASV publisko iestāžu veikta piekļuve datiem un to izmantošana nacionālās drošības nolūkos**

(119) Amerikas Savienoto Valstu tiesību aktos ir noteikti vairāki ierobežojumi un garantijas attiecībā uz piekļuvi personas datiem un to izmantošanu nacionālās drošības nolūkos, kā arī ir paredzēti pārraudzības un tiesiskās aizsardzības mehānismi, kas atbilst šā lēmuma 89. apsvērumā minētajām prasībām. Nosacījumi, saskaņā ar kuriem var notikt šāda piekļuve, un garantijas, kas piemērojamas šo pilnvaru izmantošanai, ir sīki novērtēti turpmākajās iedaļās.

#### 3.2.1. ***Juridiskais pamats, ierobežojumi un garantijas***

##### 3.2.1.1. *Piemērojamais tiesiskais regulējums*

(120) Personas datus, kas no Savienības nosūtīti ES un ASV DPR organizācijām, ASV iestādes var vākt nacionālās drošības nolūkos, pamatojoties uz dažādiem juridiskiem instrumentiem, piemērojot īpašus nosacījumus un garantijas.

(121) Kad organizācija ASV ir saņēmusi personas datus, ASV izlūkošanas aģentūras nacionālās drošības vajadzībām var pieprasīt piekļuvi šiem datiem tikai saskaņā ar likumu, jo īpaši saskaņā ar Ārējās izlūkošanas uzraudzības likumu (*FISA*) vai tiesību aktu noteikumiem, kas atļauj piekļuvi ar nacionālās drošības vēstulēm (*NSL*) ([221]). *FISA* ir vairāki juridiskie pamati, kurus var izmantot, lai vāktu (un pēc tam apstrādātu) Savienības datu subjektu personas datus, kas nosūtīti saskaņā ar ES un ASV DPR (*FISA* ([222]) 105. pants, *FISA* 302. pants ([223]), *FISA* 402. pants ([224]), *FISA* 501. pants ([225]) un *FISA* 702. pants ([226])), kā sīkāk aprakstīts 142.–152. apsvērumā.

([219]) 5 U.S.C. § 552.

([220]) Šāda izslēgšana tomēr ir regulēta. Piemēram, saskaņā ar 5 U.S.C. § 552 (b)(7) *FOIA* noteiktās 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 privātumā, D) varētu būt pamatoti uzskatāma par konfidenciāla avota (tajā skaitā 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 nacionālās 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, kad 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 kriminālatiesību pārkāpumu; un B) ir iemesls uzskatīt, ka i) izmeklēšanas vai procesa subjekts nav informēts par to norisi, un ii) dokumentācijas esības 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 iedaļas prasības". (5 U.S.C. § 552 (c)(1)).

([221]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v un 18 U.S.C. § 2709. Sk. 153. apsvērumu.

([222]) 50 U.S.C. § 1804, kas attiecas uz tradicionālo individualizēto elektronisko novērošanu.

([223]) 50 U.S.C. §1822, kas attiecas uz fizisku kratīšanu ārējās izlūkošanas nolūkos.

([224]) 50 U.S.C. § 1842 kopā ar § 1841(2) un *Section 3127 of Title 18*, kas attiecas uz zvanīto numuru reģistrētāju vai uztveršanas un izsekošanas ierīču uzstādīšanu.

([225]) 50 U.S.C. § 1861, kas ļauj FIB iesniegt "pieteikumu rīkojuma saņemšanai, kas atļauj pārvadātājam, publiskas izmitināšanas iestādei, fiziskai noliktavai vai transportlīdzekļu nomas iestādei nodot tās rīcībā esošos ierakstus izmeklēšanas vajadzībām, lai iegūtu ārējās izlūkošanas informāciju vai veiktu izmeklēšanu saistībā ar starptautisko terorismu".

([226]) *50 U.S. Code § 1881a*, kas ļauj ASV izlūkošanas kopienas struktūrām, izmantojot elektronisko sakaru pakalpojumu sniedzēju palīdzību, kura ir sniedzama obligāti, mēģināt no ASV uzņēmumiem iegūt tādu informāciju par konkrētām personām, kas nav ASV personas un atrodas ārpus Amerikas Savienotajām Valstīm (arī interneta saziņas saturu).

(122) ASV izlūkošanas aģentūrām ir arī iespējas vākt personas datus ārpus Amerikas Savienotajām Valstīm, un tie var būt personas dati, kuri tiek nosūtīti starp Savienību un Amerikas Savienotajām Valstīm. Datu vākšana ārpus Amerikas Savienotajām Valstīm ir balstīta uz Izpildrīkojumu Nr. 12333 (IR Nr. 12333) ([227]), ko izdevis prezidents ([228]).

(123) Sakaru izlūkdatu vākšana ir izlūkdatu vākšanas veids, kas ir vissvarīgākais saistībā ar šo aizsardzības līmeņa pietiekamības konstatējumu, jo tas attiecas uz elektronisko sakaru un datu vākšanu no informācijas sistēmām. Šādu datu vākšanu ASV izlūkošanas aģentūras var veikt gan Amerikas Savienoto Valstu teritorijā (pamatojoties uz *FISA*), gan datu nosūtīšanas laikā uz Amerikas Savienotajām Valstīm (pamatojoties uz IR Nr. 12333).

(124) 2022. gada 7. oktobrī ASV prezidents izdeva IR Nr. 14086 par drošības pasākumu uzlabošana Amerikas Savienoto Valstu sakaru izlūkošanas darbībām, nosakot ierobežojumus un garantijas visām ASV sakaru izlūkošanas darbībām. Minētais IR lielā mērā aizstāj Prezidenta politikas direktīvu (PPD 28) ([229]), stiprina nosacījumus, ierobežojumus un garantijas, kas attiecas uz visām sakaru izlūkošanas darbībām (t. i., uz *FISA*un IR Nr. 12333 pamata) neatkarīgi no to vietas ([230]), un ar to izveido jaunu tiesiskās aizsardzības mehānismu, ar kura palīdzību fiziskas personas var atsaukties uz šīm garantijām un tās īstenot ([231]) (sīkāk skatīt 176.–194. apsvērumu). Tādējādi ar to ASV tiesību aktos tiek ieviesti to sarunu rezultāti, kas notika starp ES un ASV pēc tam, kad Tiesa atzina par spēkā neesošu Komisijas lēmumu par aizsardzības līmeņa pietiekamību, ko nodrošina ES un ASV privātuma vairogs (sk. 6. apsvērumu). Tāpēc tas ir īpaši svarīgs šajā lēmumā novērtētā tiesiskā regulējuma elements.

(125) IR Nr. 14086 ieviestie ierobežojumi un aizsardzības pasākumi papildina *FISA* 702. iedaļā un IR Nr. 12333 paredzētos. Izlūkošanas aģentūrām ir jāievēro zemāk (3.2.1.2. un 3.2.1.3. iedaļā) aprakstītās prasības, veicot sakaru izlūkošanas darbības saskaņā ar *FISA* 702. iedaļu un IR Nr. 12333, proti, atlasot/identificējot ārējās izlūkošanas informācijas kategorijas, kas iegūstamas saskaņā ar *FISA* 702. iedaļu; vācot ārējās izlūkošanas vai pretizlūkošanas informāciju saskaņā ar IR Nr. 12333; un pieņemot individuālus lēmumus par mērķiem saskaņā ar *FISA* 702. iedaļu un IR Nr. 12333.

(126) Prasības, kas noteiktas šajā prezidenta izdotajā izpildrīkojumā, ir saistošas visām izlūkošanas kopienas struktūrām. Tās ir jāīsteno ar aģentūras politiku un procedūrām, ar kurām tās transponē konkrētos ikdienas darbību virzienos. Šajā sakarā IR Nr. 14086 ASV izlūkošanas aģentūrām ir dots ne vairāk kā viens gads laika, lai atjauninātu to esošos politikas dokumentus un procedūras (t. i., līdz 2023. gada 7. oktobrim) un saskaņotu tās ar IR noteiktajām prasībām. Šāda atjaunināta politika un procedūras ir jāizstrādā, apspriežoties ar ģenerālprokuroru, Nacionālās izlūkošanas direktora biroja pilsonisko brīvību aizsardzības amatpersonu (*ODNI CLPO*) un *PCLOB*– neatkarīgu pārraudzības struktūru, kas ir pilnvarota pārskatīt izpildvaras politiku un tās īstenošanu, lai aizsargātu privātumu un pilsoniskās brīvības (sk. 110. apsvērumu par *PCLOB* lomu un statusu) –, un tās ir jādara pieejamas publiski ([232]). Turklāt, tiklīdz atjauninātā politika un procedūras būs ieviestas, *PCLOB* veiks pārbaudi, lai nodrošinātu to atbilstību

([227]) IR Nr. 12333 *United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 December 1981 as amended 30 July 2008)*. IR Nr. 12333 vispārīgāk noteic ASV izlūkošanas centienu mērķus, virzienus, pienākumus un atbildību (tajā skaitā dažādu izlūkošanas kopienas struktūru lomu) un nosaka vispārējos parametrus izlūkošanas darbību veikšanai.

([228]) Saskaņā ar ASV Konstitūcijas II pantu par nacionālo drošību, jo īpaši par ārējās izlūkošanas datu vākšanu, ir atbildīgs prezidents kā bruņoto spēku virspavēlnieks.

([229]) IR Nr. 14086 atceļ iepriekšējo prezidenta direktīvu PPD 28, izņemot tās 3. iedaļu un papildinošo pielikumu (kurā noteikts, ka izlūkošanas aģentūrām katru gadu jāpārskata to sakaru izlūkošanas prioritātes un prasības, ņemot vērā sakaru izlūkošanas darbību sniegtos ieguvumus ASV nacionālajām interesēm, kā arī šo darbību radīto risku) un 6. iedaļu (kurā ietverti vispārīgi noteikumi), sk. Nacionālās drošības memorandu par Prezidenta politikas direktīvas Nr. 28 daļēju atcelšanu, kas pieejams https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Sk. *Section 5(f)*, IR Nr. 14086, kur paskaidrots, ka IR ir tāda pati piemērošanas joma kā PPD 28, kas saskaņā ar tā 3. zemsvītras piezīmi attiecas uz sakaru izlūkošanas darbībām, kuras veic, lai vāktu saziņas saturu vai informāciju par saziņu, izņemot sakaru izlūkošanas darbības, ko veic, lai pārbaudītu vai attīstītu sakaru izlūkošanas spējas.

([231]) Šajā sakarā skatīt, piemēram, IR Nr. 14086 5. iedaļas h) punktu, kurā paskaidrots, ka IR noteiktie aizsardzības pasākumi rada juridiskas tiesības, un fiziskas personas tās var īstenot, izmantojot tiesiskās aizsardzības mehānismu.

([232]) Sk. *Section 2(c)(iv)(C)*, IR Nr. 14086.

IR. Katrai izlūkošanas aģentūrai 180 dienu laikā pēc tam, kad *PCLOB* ir pabeigusi šādu pārbaudi, ir rūpīgi jāizvērtē un jāīsteno vai kā citādi jāņem vērā visi *PCLOB* ieteikumi. ASV valdība 2023. gada 3. jūlijā publicēja šādu atjauninātu politiku un procedūras ([233]).

3.2.1.2. *Ierobežojumi un aizsardzības pasākumi attiecībā uz personas datu vākšanu nacionālās drošības nolūkos*

(127) IR Nr. 14086 nosaka vairākas visaptverošas prasības, kas attiecas uz visām sakaru izlūkošanas darbībām (personas datu vākšana, izmantošana, izplatīšana utt.).

(128) Pirmkārt, šādām darbībām jābūt pamatotām ar likumu vai prezidenta atļauju un veiktām saskaņā ar ASV tiesību aktiem, ieskaitot Konstitūciju ([234]).

(129) Otrkārt, ir jāievieš atbilstošas garantijas, lai nodrošinātu, ka privātums un pilsoniskās brīvības ir neatņemama šādu pasākumu plānošanas daļa ([235]).

(130) Konkrēti, jebkuras sakaru izlūkošanas darbības var veikt tikai "pēc tam, kad, pamatojoties uz visu attiecīgo faktoru saprātīgu novērtējumu, ir konstatēts, ka darbības ir nepieciešamas, lai sasniegtu apstiprinātu izlūkošanas prioritāti" (attiecībā uz jēdzienu "apstiprināta izlūkošanas prioritāte" skatīt 135. apsvērumu) ([236]).

(131) Turklāt šādas darbības drīkst veikt tikai "tādā apjomā un veidā, kas ir samērīgs ar apstiprināto izlūkošanas prioritāti, kuras dēļ tās ir atļautas" ([237]). Citiem vārdiem sakot, ir jāpanāk pienācīgs līdzsvars "starp izvirzītās izlūkošanas prioritātes svarīgumu un ietekmi uz skarto fizisko personu privātumu un pilsoniskajām brīvībām neatkarīgi no to valstspiederības vai dzīvesvietas" ([238]).

(132) Visbeidzot, lai nodrošinātu atbilstību šīm vispārīgajām prasībām, kas atspoguļo likumības, nepieciešamības un samērīguma principu, sakaru izlūkošanas darbības ir pakļautas pārraudzībai (sīkāk skatīt 3.2.2. iedaļā) ([239]).

(133) Šīs visaptverošās prasības attiecībā uz sakaru izlūkdatu vākšanu tiek papildus pamatotas ar vairākiem nosacījumiem un ierobežojumiem, kas nodrošina, ka iejaukšanās fizisku personu tiesībās ir minimāli nepieciešamā līmenī un ir samērīga, lai sasniegtu likumīgu mērķi.

(134) Pirmkārt, IR divējādi ierobežo pamatojumu, saskaņā ar kuru var vākt datus kā daļu no sakaru izlūkošanas darbībām. No vienas puses, IR ir noteikti likumīgi mērķi, kurus var mēģināt sasniegt, vācot sakaru izlūkdatus, piemēram, lai saprastu vai novērtētu tādu ārvalstu organizāciju (arī starptautisku teroristu organizāciju) spējas, nodomus vai darbības, kas rada pašreizējus vai iespējamus draudus ASV nacionālajai drošībai; lai aizsargātu pret ārvalstu militārajām spējām un darbībām; lai izprastu vai novērtētu starptautiskus draudus, kas ietekmē globālo drošību, piemēram, klimata un citas ekoloģiskās pārmaiņas, riskus sabiedrības veselībai un draudus humanitārajai situācijai ([240]). No otras puses, IR ir uzskaitīti konkrēti mērķi, kurus nekad nedrīkst mēģināt sasniegt ar sakaru izlūkošanas darbībām, piemēram, lai apgrūtinātu fizisku personu vai preses kritiku, nepiekrišanu vai ideju vai

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

([234]) *Section 2(a)(i)*, IR Nr. 14086.

([235]) *Section 2(a)(ii)*, IR Nr. 14086.

([236]) *Section 2(a)(ii)(A)*, IR Nr. 14086. Tas ne vienmēr nozīmē, ka sakaru izlūkošana ir vienīgais veids, kā sasniegt apstiprinātas izlūkošanas prioritātes aspektus. Piemēram, sakaru izlūkdatu vākšanu var izmantot, lai nodrošinātu alternatīvus apstiprināšanas ceļus (piemēram, lai apstiprinātu informāciju, kas saņemta no citiem izlūkošanas avotiem) vai lai saglabātu uzticamu piekļuvi tai pašai informācijai (IR Nr. 14086 2. iedaļas c) punkta i) apakšpunkta A daļa).

([237]) *Section 2(a)(ii)(B)*, IR Nr. 14086.

([238]) *Section 2(a)(ii)(B)*, IR Nr. 14086.

([239]) *Section 2(a)(iii)* saistībā ar *Section 2(d)*, IR Nr. 14086.

([240]) *Section 2(b)(i)*, IR Nr. 14086. Tā kā IR norādītajā likumīgo mērķu sarakstā nav iekļauti iespējami apdraudējumi nākotnē, IR paredz iespēju prezidentam atjaunināt sarakstu, ja rodas jaunas nacionālās drošības prasības, piemēram, jauni nacionālās drošības apdraudējumi. Šādi atjauninājumi principā ir jāpublisko, ja vien prezidents nenolemj, ka tas apdraudētu ASV nacionālo drošību (IR Nr. 14086 2. iedaļas b) punkta i) apakšpunkta B daļa).

politisko uzskatu brīvu paušanu, lai nelabvēlīgi ietekmētu personas, pamatojoties uz viņu etnisko izcelsmi, rasi, dzimti, dzimtisko identitāti, seksuālo orientāciju vai reliģisko pārliecību, vai lai sniegtu konkurences priekšrocības ASV uzņēmumiem ([241]).

(135) Turklāt izlūkošanas aģentūras nevar paļauties uz IR Nr. 14086 noteiktajiem likumīgajiem mērķiem kā tādiem, lai attaisnotu sakaru izlūkdatu vākšanu, bet operatīvos nolūkos tie ir jāpamato ar konkrētākām prioritātēm, kuru īstenošanai var vākt sakaru izlūkdatus. Citiem vārdiem sakot, faktiskā vākšana var notikt tikai tādēļ, lai veicinātu konkrētākas prioritātes īstenošanu. Šādas prioritātes tiek noteiktas, izmantojot īpašu procesu, kura mērķis ir nodrošināt atbilstību piemērojamajām juridiskajām prasībām, tajā skaitā tām, kas attiecas uz privātumu un pilsoniskajām brīvībām. Konkrētāk, izlūkošanas prioritātes vispirms izstrādā nacionālās izlūkošanas direktors (izmantojot tā dēvēto Nacionālo izlūkošanas prioritāšu satvaru) un iesniedz tās prezidentam apstiprināšanai ([242]). Pirms izlūkošanas prioritātes tiek ierosinātas prezidentam, direktoram saskaņā ar IR Nr. 14086 ir jāsaņem *ODNI CLPO* sagatavots novērtējums par katru prioritāti attiecībā uz to, vai tā 1) sekmē vienu vai vairākus IR uzskaitītos likumīgos mērķus, 2) tā nav paredzēta sakaru izlūkdatu vākšanai, un nav paredzams, ka tās dēļ šādi dati tiks vākti, lai sasniegtu IR uzskaitītos aizliegtos mērķus, un 3) tā tika izveidota, pienācīgi ņemot vērā visu personu privātumu un pilsoniskās brīvības, neatkarīgi no to valstspiederības vai dzīvesvietas ([243]). Ja direktors nepiekrīt *CLPO* novērtējumam, abi viedokļi ir jāiesniedz prezidentam ([244]).

(136) Tāpēc šis process jo īpaši nodrošina, ka privātuma apsvērumi tiek ņemti vērā jau sākotnējā posmā, kad tiek izstrādātas izlūkošanas prioritātes.

(137) Otrkārt, kad izlūkošanas prioritāte ir noteikta, lēmumu par to, vai un kādā apjomā var vākt sakaru izlūkdatus, lai veicinātu šādas prioritātes īstenošanu, nosaka vairākas prasības. Ar šīm prasībām tiek praksē ieviesti IR Nr. 2. iedaļas a) punktā noteiktie visaptverošie nepieciešamības un samērīguma standarti.

(138) Jo īpaši sakaru izlūkdatus drīkst vākt tikai "pēc tam, kad, pamatojoties uz visu attiecīgo faktoru saprātīgu novērtējumu, ir konstatēts, ka vākšana ir nepieciešama, lai veicinātu konkrētas izlūkošanas prioritātes īstenošanu" ([245]). Nosakot, vai konkrēta sakaru izlūkošanas datu vākšanas darbība ir nepieciešama, lai veicinātu apstiprinātas izlūkošanas prioritātes īstenošanu, ASV izlūkošanas aģentūrām ir jāapsver citu mazāk invazīvu avotu un metožu pieejamība, iespējamība un piemērotība, arī no diplomātiskiem un publiskiem avotiem ([246]). Prioritāte jāpiešķir šādiem alternatīviem, mazāk invazīviem avotiem un metodēm, ja tādi ir pieejami ([247]).

(139) Ja, piemērojot šādus kritērijus, sakaru izlūkdatu vākšana tiek uzskatīta par nepieciešamu, tai jābūt "pēc iespējas pielāgotai" un tā "nedrīkst nesamērīgi ietekmēt privātumu un pilsoniskās brīvības" ([248]). Lai novērstu nesamērīgu ietekmi uz privātumu un pilsoniskajām brīvībām, t. i., lai panāktu pienācīgu līdzsvaru starp nacionālās drošības vajadzībām un privātuma un pilsonisko brīvību aizsardzību, pienācīgi jāņem vērā visi attiecīgie faktori, piemēram, sasniedzamā mērķa raksturs, vākšanas darbības intensitāte, tajā skaitā tās ilgums, iespējamais vākšanas ieguldījums izvirzītā mērķa sasniegšanā, pamatoti paredzamās sekas fiziskām personām un vācamo datu raksturs un sensitivitāte ([249]).

([241]) *Section 2(b)(ii)*, IR Nr. 14086.
([242]) *Section 102A*, Nacionālās drošības likums (*National Security Act*) un *Section 2(b)(iii)*, IR Nr. 14086.
([243]) Izņēmuma gadījumos (jo īpaši, ja šādu procesu nevar veikt, jo ir nepieciešams risināt jaunu vai pieaugošu izlūkošanas vajadzību), šādas prioritātes var noteikt tieši prezidents vai izlūkošanas kopienas struktūras vadītājs, kuram principā jāpiemēro tie paši kritēriji, kas aprakstīti *section 2(b)(iii)(A)(1)-(3)*, sk. *Section 4(n)*, IR Nr. 14086.
([244]) *Section 2(b)(iii)(C)*, IR Nr. 14086.
([245]) *Section 2(b)* un *(c)(i)(A)*, IR Nr. 14086.
([246]) *Section 2(c)(i)(A)*, IR Nr. 14086.
([247]) *Section 2(c)(i)(A)*, IR Nr. 14086.
([248]) *Section 2(c)(i)(B)*, IR Nr. 14086.
([249]) *Section 2(c)(i)(B)*, IR Nr. 14086.

(140) Attiecībā uz sakaru izlūkošanas datu vākšanas veidu – datu vākšanai Amerikas Savienotajās Valstīs, kas ir visrelevantākā attiecībā uz šo aizsardzības līmeņa pietiekamības konstatējumu, jo tā attiecas uz datiem, kuri ir nosūtīti organizācijām ASV, vienmēr jābūt mērķorientētai, kā sīkāk paskaidrots 142.–153. apsvērumā.

(141) Pamatojoties uz IR Nr. 12333, "lielapjoma datu vākšana" ([250]) ir veicama tikai ārpus Amerikas Savienotajām Valstīm. Arī šajā gadījumā saskaņā ar IR Nr. 14086 par prioritāru ir jānosaka mērķorientēta vākšana ([251]). Turpretī lielapjoma datu vākšana ir atļauta tikai tad, ja informāciju, kas nepieciešama, lai veicinātu apstiprinātas izlūkošanas prioritātes īstenošanu, nevar pamatoti iegūt ar mērķorientētu vākšanu ([252]). Ja ir nepieciešams veikt lielapjoma datu vākšanu ārpus Amerikas Savienotajām Valstīm, saskaņā ar IR Nr. 14086 ([253]) piemēro īpašas garantijas. Pirmkārt, ir jāpiemēro metodes un tehniskie pasākumi, lai vāktu tikai tādus datus, kas nepieciešami apstiprinātās izlūkošanas prioritātes īstenošanai, vienlaikus līdz minimumam samazinot nerelevantas informācijas vākšanu ([254]). Otrkārt, IR ierobežo savāktās lielapjoma informācijas izmantošanu (arī vaicājumu procedūras) līdz sešiem konkrētiem mērķiem, tajā skaitā šādiem: aizsardzība pret terorismu, ķīlnieku sagrābšanu un personu turēšanu gūstā, ko veic ārvalstu valdība, organizācija vai persona vai kas tiek veikta to vārdā; aizsardzība pret ārvalstu spiegošanu, sabotāžu vai slepkavībām; aizsardzība pret apdraudējumiem, ko rada masu iznīcināšanas ieroču vai ar tiem saistītu tehnoloģiju izplatīšana un draudi utt. ([255]) Visbeidzot, ar lielapjoma vākšanas metodēm iegūtas sakaru izlūkdatu informācijas vaicājumu procedūras var veikt tikai tad, ja tas ir nepieciešams, lai sasniegtu apstiprinātu izlūkošanas prioritāti, īstenojot šos sešus mērķus un saskaņā ar politiku un procedūrām, kurās pienācīgi ņemta vērā vaicājumu ietekme uz visu personu privātumu un pilsoniskajām brīvībām neatkarīgi no to valstspiederības vai dzīvesvietas ([256]).

(142) Papildus IR Nr. 14086 prasībām uz Amerikas Savienotajās Valstīs esošai organizācijai nosūtītiem datiem, kas savākti sakaru izlūkošanas nolūkos, attiecas īpaši ierobežojumi un garantijas, ko reglamentē *FISA* 702. pants ([257]). *FISA* 702. pants ļauj ar ASV elektronisko sakaru pakalpojumu sniedzēju palīdzību, kas sniedzama obligāti, iegūt ārējo izlūkošanas informāciju, novērojot personas, kuras nav ASV personas un par kurām ir pamats uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām Valstīm ([258]). Lai vāktu ārējās izlūkošanas informāciju saskaņā ar *FISA* 702. pantu, ģenerālprokurors un nacionālās izlūkošanas direktors katru gadu iesniedz Ārējās izlūkošanas

([250]) T. i., liela daudzuma sakaru izlūkdatu vākšana, kas tehnisku vai operatīvu apsvērumu dēļ tiek iegūta, neizmantojot diskriminantus (piemēram, neizmantojot īpašus identifikatorus vai atlases nosacījumus), sk. *Section 4(b)*, IR Nr. 14086. Saskaņā ar IR Nr. 14086 un kā sīkāk paskaidrots 141. apsvērumā, lielapjoma datu vākšana saskaņā ar IR Nr. 12333 tiek veikta tikai tad, ja tas ir nepieciešams, lai veicinātu konkrētas apstiprinātas izlūkošanas prioritātes, un tai piemēroti vairāki ierobežojumi un garantijas, kas paredzēti, lai nodrošinātu, ka piekļuve datiem nav neselektīva. Tāpēc lielapjoma datu vākšana ir pretstatāma vispārējai un neselektīvai datu vākšanai ("masu novērošana") bez ierobežojumiem un garantijām.

([251]) *Section 2(c)(ii)(A)*, IR Nr. 14086.

([252]) *Section 2(c)(ii)(A) EO*, IR Nr. 14086.

([253]) IR Nr. 14086 konkrētie noteikumi par lielapjoma datu vākšanu arī attiecas uz mērķorientētu sakaru izlūkdatu vākšanu, kuras ietvaros īslaicīgi tiek izmantoti dati, kas iegūti, neizmantojot diskriminantus (piemēram, konkrētus atlases terminus vai identifikatorus), t. i., lielā apjomā (kas ir iespējams tikai ārpus Amerikas Savienoto Valstu teritorijas). Tas neattiecas uz gadījumiem, kad šādi dati tiek izmantoti, tikai mērķtiecīgas sakaru izlūkdatu vākšanas sākotnējā tehniskajā posmā, tiek glabāti tikai īsu laika periodu, cik nepieciešams šī posma īstenošanai, un pēc tam tiek nekavējoties dzēsti (IR Nr. 14086 2. iedaļas c) punkta ii) apakšpunkta D daļa). Šādā gadījumā sākotnējās vākšanas, neizmantojot diskriminantus, vienīgais nolūks ir nodrošināt mērķtiecīgu datu vākšanu, izmantojot konkrētu identifikatoru vai atlases terminu. Šādā scenārijā valdības datubāzēs tiek ievietoti tikai tie dati, kas atbilst noteiktam diskriminantam, bet pārējie dati tiek dzēsti. Tāpēc šādu mērķtiecīgu vākšanu reglamentē vispārīgie noteikumi, kas attiecas uz sakaru izlūkdatu vākšanu, ieskaitot IR Nr. 14086 2. iedaļas a)–b) punkts un 2. iedaļas c) punkta i) apakšpunkts.

([254]) *Section 2(c)(ii)(A)*, IR Nr. 14086.

([255]) *Section 2(c)(ii)(B)*, IR Nr. 14086. Ja rodas jaunas nacionālās drošības prasības, ko izvirza, piemēram, jauni draudi nacionālajai drošībai, prezidents šo sarakstu var atjaunināt. Šādi atjauninājumi principā ir jāpublisko, ja vien prezidents nenolemj, ka tas apdraudētu ASV nacionālo drošību (IR Nr. 14086 2. iedaļas c) punkta ii) apakšpunkta C daļa). Attiecībā uz vaicājumu izmantošanu datiem, kas savākti ar lielapjoma vākšanas metodēm, skatīt IR Nr. 14086 2. iedaļas c) punkta iii) apakšpunkta D daļu.

([256]) *Section 2(a)(ii)(A)* saistībā ar *Section 2(c)(iii)(D)*, IR Nr. 14086. Sk. arī VII pielikumu.

([257]) 50 U.S.C. § 1881.

([258]) 50 U.S.C. § 1881a (a). Jo īpaši, kā norādīja *PCLOB*, 702. pantā paredzēto novērošanu "pilnībā veido mērķtiecīga pievēršanās konkrētām personām [kas nav ASV pilsoņi], par kurām ir pieņemts individualizēts lēmums" (Privātuma un pilsonisko brīvību pārraudzības padome, ziņojums "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", 2014. gada 2. jūlijs, 702. panta ziņojums, 111. lpp.). Sk. arī *NSA CLPO* ziņojumu "NSA's Implementation of Foreign Intelligence Act Section 702", 2014. gada 16. aprīlis. Termins "elektronisko sakaru pakalpojumu sniedzējs" ir definēts 50 U.S.C. § 1881 (a)(4).

uzraudzības tiesai (*FISC*) apliecinājumus, kuros noteiktas iegūstamās ārējās izlūkošanas informācijas kategorijas ([259]). Apliecinājumiem jāpievieno mērķorientēšanas, minimizācijas un vaicājumu procedūras, kuras arī ir apstiprinājusi Tiesa un kuras ir juridiski saistošas ASV izlūkošanas aģentūrām.

(143) *FISC* ir neatkarīga tiesa ([260]), kura izveidota ar federālo likumu un kuras lēmumus var pārsūdzēt Ārējās izlūkošanas uzraudzības pārskatīšanas tiesā (*FISCR*) ([261]) un, visbeidzot, Amerikas Savienoto Valstu Augstākajā tiesā ([262]). *FISC* (un *FISCR*) palīdz pastāvīga kolēģija, kuras sastāvā ir pieci juristi un pieci tehniskie speciālisti, kas ir kompetenti gan nacionālās drošības jautājumos, gan pilsonisko brīvību jomā ([263]). No šīs grupas tiesa ieceļ personu, kas darbojas kā *amicus curiae*, lai palīdzētu izskatīt jebkuru rīkojuma vai pārskatīšanas pieteikumu, kas, pēc tiesas ieskatiem, sniedz jaunu vai būtisku likuma interpretāciju, ja vien tiesa nesecina, ka šāda iecelšana ir neatbilstīga ([264]). Tas jo īpaši nodrošina, ka tiesas novērtējumā ir pienācīgi atspoguļoti privātuma apsvērumi. Tiesa var iecelt arī personu vai organizāciju, kas darbojas kā *amicus curiae*, arī lai sniegtu tehnisko ekspertīzi, kad vien uzskata to par nepieciešamu, vai arī, pamatojoties uz pieprasījumu, ļaut personai vai organizācijai pagarināt *amicus curiae* darbības termiņu ([265]).

(144) *FISC* izskata sertifikātu un saistīto procedūru (jo īpaši mērķorientēšanas un minimizēšanas procedūru) atbilstību *FISA* prasībām. Ja tā uzskata, ka prasības nav izpildītas, tā var pilnībā vai daļēji atteikt sertifikāciju un pieprasīt grozīt procedūras ([266]). Šajā sakarā *FISC* ir vairākkārt apstiprinājusi, ka, izskatot 702. panta mērķorientēšanas un minimizēšanas procedūras, tā neaprobežojas tikai ar rakstiskām procedūrām, bet izskata arī to, kā šīs procedūras īsteno valdība ([267]).

(145) Individualizētus lēmumus par mērķorientēšanu pieņem Nacionālā drošības aģentūra (*National Security Agency* (*NSA*) – izlūkošanas aģentūra, kas atbilstīgi *FISA* 702. pantam ir atbildīga par mērķorientēšanu) saskaņā ar *FISC* apstiprinātām mērķorientēšanas procedūrām, kuras paredz, ka *NSA*, pamatojoties uz visu apstākļu kopumu, jānovērtē, vai, veicot mērķtiecīgu izlūkošanu pret konkrētu personu, būs iespējams iegūt sertifikācijas apliecinājumā norādītu ārējās izlūkošanas informācijas kategorija ([268]). Šim novērtējumam jābūt konkrētam un balstītam uz faktiem, pamatotam ar analītisku vērtējumu, specializētām analītiķa zināšanām un pieredzi, kā arī iegūstamās ārējās

([259]) 50 U.S.C. § 1881a (g).

([260]) *FISC* sastāvā ir 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 *FISA* mainās rotācijas kārtībā ir pēc septiņiem gadiem. *FISA* nosaka, ka tiesnešiem jābūt no vismaz septiņiem dažādiem ASV tiesu apgabaliem. Sk. 50 U.S.C. § 1803 (a). Tiesnešiem palīdz pieredzējuši tiesas ierēdņi, kas ir tiesas juridiskie darbinieki un kas sagatavo vākšanas pieprasījumu juridisko analīzi. Sk. ASV Ārējās izlūkošanas uzraudzības tiesas galvenā tiesneša god. *Reggie B. Walton* vēstuli ASV Senāta Tieslietu komitejas priekšsēdētājam god. *Patrick J. Leahy* (2013. gada 29. jūlijs) ("Valtona vēstule"), 2. lpp.; pieejama šeit: https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

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

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

([263]) 50 U.S.C. § 1803 (i)(1),(3)(A).

([264]) 50 U.S.C. § 1803 (i)(2)(A).

([265]) 50 U.S.C. § 1803 (i)(2)(B).

([266]) Sk., piemēram, *FISC* 2018. gada 18. oktobra atzinumu, kas pieejams https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf un ko apstiprinājusi Ārējās izlūkošanas uzraudzības pārskatīšanas tiesa savā 2019. gada 12. jūlija atzinumā, kurš pieejams https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) Sk., piemēram, *FISC* memorandatzinumu un rīkojumu 35. lpp. (2020. gada 18. novembris) (publiskot atļauts 2021. gada 26. aprīlī), (D pielikumu).

([268]) 50 U.S.C. § 1881a(a), *Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, of March 2018* (*NSA* mērķorientēšanas procedūras), pieejams https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf , 1.–4. lpp., sīkāki skaidrojumi *PCLOB* ziņojumā, 41. un 42. lpp.

izlūkošanas informācijas raksturu ([269]). Mērķorientēšana tiek veikta, identificējot tā dēvētos selektorus, ar ko identificē konkrētus saziņas līdzekļus, piemēram, izlūkošanas subjekta e-pasta adresi vai tālruņa numuru, bet nekad atslēgvārdus vai fizisku personu vārdus ([270]).

(146) *NSA* analītiķi vispirms identificēs ārvalstīs esošas personas, kuras nav ASV personas un kuru novērošana, pamatojoties uz analītiķu novērtējumu, ļaus iegūt attiecīgos ārējās izlūkošanas datus, kas norādīti apliecinājumā ([271]). Kā izklāstīts *NSA* mērķorientēšanas procedūrās, *NSA* var vērst novērošanu pret kādu izlūkošanas subjektu tikai tad, ja tā par šo subjektu jau ir ieguvusi kādu informāciju ([272]). Tā var izrietēt no informācijas, kas iegūta no dažādiem avotiem, piemēram, cilvēku veiktas izlūkošanas. Izmantojot šos citus avotus, analītiķim ir jāuzzina arī par konkrētu selektoru (t. i., saziņas kontu), ko izmanto potenciālais izlūkošanas subjekts. Kad ir identificētas atsevišķas personas un to izsekošana ir apstiprināta ar plašu pārskatīšanas mehānismu *NSA* ([273]) ietvaros, tiks piešķirti (t. i. izstrādāti un piemēroti) selektori, kas identificē izlūkošanas subjektu sakaru līdzekļus (piemēram, e-pasta adreses) ([274]).

(147) *NSA* ir jādokumentē faktiskais pamats izlūkošanas subjekta izvēlei ([275]) un regulāri pēc sākotnējās mērķorientēšanas jāapstiprina, ka mērķorientēšanas standarts joprojām tiek ievērots ([276]). Kad mērķorientēšanas standarts vairs netiek ievērots, informācijas vākšana ir jāpārtrauc ([277]). *NSA* veikto katra izlūkošanas subjekta izvēli, kā arī katra reģistrētā mērķorientēšanas novērtējuma un pamatojuma uzskaiti reizi divos mēnešos pārbauda Tieslietu ministrijas izlūkošanas pārraudzības biroju amatpersonas, kurām ir pienākums ziņot *FISC* un Kongresam par jebkādiem pārkāpumiem ([278]). *NSA* rakstiskā dokumentācija atvieglo *FISC* veikto pārraudzību attiecībā uz to, vai mērķtiecīga vēršanās pret konkrētām fiziskajām personām ir veikta pareizi saskaņā ar *FISA* 702. pantu un atbilstīgi tās uzraudzības pilnvarām, kas aprakstītas 173. un 174. apsvērumā ([279]). Visbeidzot, nacionālās izlūkošanas direktoram (*DNI*) katru gadu publiskos ikgadējos statistikas pārredzamības ziņojumos ir jāziņo arī par kopējo saskaņā ar *FISA* 702. pantu noteikto izlūkošanas subjektu skaitu. Uzņēmumi, kas saņem *FISA* 702. panta direktīvas, datus par saņemtajiem pieprasījumiem var publicēt apkopotā veidā (pārredzamības ziņojumos) ([280]).

([269]) *NSA* mērķorientēšanas procedūras, 4. lpp.

([270]) Sk. *PCLOB* ziņojumu par 702. pantu, 32.–33., 45. lpp. ar turpmākām atsaucēm. Sk. arī ģenerālprokurora un nacionālā izlūkošanas direktora iesniegto Pusgada novērtējumu par atbilstību procedūrām un vadlīnijām, kas izdotas saskaņā ar Ārējās izlūkošanas uzraudzības likuma 702. iedaļu par pārskata periodu no 2016. gada 1. decembra līdz 2017. gada 31. maijam, 41. lpp (2018. gada oktobris), pieejams vietnē https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

([271]) *PCLOB* ziņojums par 702. pantu, 42. un 43. lpp.

([272]) *NSA* mērķorientēšanas procedūras, 2. lpp.

([273]) *PCLOB* ziņojums par 702. pantu, 46. lpp. Piemēram, *NSA* ir jāapstiprina, ka starp izlūkošanas subjektu un selektoru pastāv saikne, jādokumentē ārējās izlūkošanas informācija, kuru paredzēts iegūt, šī informācija ir jāizskata un jāapstiprina diviem *NSA* vecākajiem analītiķiem, un vispārējā procesā tiks sekots turpmākām atbilstības pārbaudēm, ko veiks *ODNI* un Tieslietu ministrija. Sk. *NSA CLPO* ziņojumu "NSA veiktā Ārējās izlūkošanas likuma 702. iedaļas īstenošana", 2014. gada 16. aprīlis.

([274]) 50 U.S.C. § 1881a (h).

([275]) *NSA* mērķorientēšanas procedūras, 8. lpp. Sk. arī *PCLOB* ziņojumu par 702. pantu, 46. lpp. Rakstiska pamatojuma nesniegšana ir dokumentācijas atbilstības incidents, par kuru ir jāziņo *FISC* un Kongresam. Sk. *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017*, p. 41 (2018. gada oktobris), *DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017 at p. A-6*, pieejams https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Sk. ASV valdības Ārējās izlūkošanas uzraudzības tiesai iesniegto dokumentu *2015 Summary of Notable Section 702 Requirements*, 2. un 3. lpp. (2015. gada 15. jūlijs), un VII pielikumā sniegto informāciju.

([277]) Sk. ASV valdības Ārējās izlūkošanas uzraudzības tiesai iesniegto dokumentu *2015 Summary of Notable Section 702 Requirements*, 2. un 3. lpp. (2015. gada 15. jūlijs), kurā noteikts: "Ja valdība vēlāk novērtē, ka izlūkošanas subjekta selektora turpmāka piešķiršana, visticamāk, nepalīdzēs iegūt ārējās izlūkošanas informāciju, ir nepieciešama tūlītēja piešķiršanas pārtraukšana, un kavēšanās var izraisīt atbilstības incidentu, par ko jāziņo." Sk. arī VII pielikumā sniegto informāciju.

([278]) *PCLOB* ziņojums par 702. pantu, 70.–72. lpp. Amerikas Savienoto Valstu Ārējās izlūkošanas uzraudzības tiesas reglamenta 13. panta b) punkts, pieejams https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) Sk. arī *DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017 at p. A-6*.

([280]) 50 U.S.C. § 1874.

(148) Attiecībā uz citiem juridiskajiem pamatiem personas datu vākšanai, kas nosūtīti organizācijām ASV, piemēro dažādus ierobežojumus un garantijas. Kopumā datu lielapjoma vākšana ir konkrēti aizliegta saskaņā ar *FISA* 402. pantu (par zvanīto numuru reģistrētāju un uztveršanas un izsekošanas ierīču izmantošanu), tāpat ir aizliegta šāda vākšana ar nacionālās drošības vēstuļu palīdzību, un tā vietā tiek prasīts izmantot īpašus "atlases noteikumus" ([281]).

(149) Lai veiktu tradicionālo individualizēto elektronisko novērošanu (saskaņā ar *FISA* 105. pantu), izlūkošanas aģentūrām jāiesniedz pieteikums *FISC*, kuram pievienots faktu un apstākļu izklāsts, kas pamato pārliecību, ka pastāv pamatots iemesls uzskatīt, ka attiecīgo saziņas līdzekli izmanto vai gatavojas izmantot sveša vara vai svešas varas aģents ([282]). *FISC* citustarp novērtēs, vai, pamatojoties uz iesniegtajiem faktiem, ir pamatots iemesls uzskatīt, ka tas patiešām ir šāds gadījums ([283]).

(150) Lai, pamatojoties uz *FISA* 301. pantu, veiktu kratīšanu telpās vai īpašumā, kuras rezultātā paredzēts pārbaudīt, konfiscēt utt. informāciju, materiālus vai īpašumu (piemēram, datorierīci), ir jāiesniedz *FISC* rīkojuma saņemšanas ([284]) pieteikums. Šādā pieteikumā citustarp ir jānorāda, ka ir pamatots iemesls uzskatīt, ka kratīšanas mērķis ir kāda sveša vara vai svešas varas aģents; ka telpā vai īpašumā, kurās veicama kratīšana, ir ārējās izlūkošanas informācija un ka telpas, kurās veicama kratīšana, to izmanto kāda sveša vara (vai tās aģents), tā ir kādas svešas varas (aģenta) īpašumā, valdījumā, turējumā vai tiek pārvesta uz svešu varu (aģentam) vai no tās (no aģenta) ([285]).

(151) Tāpat, lai uzstādītu zvanīto numuru reģistrētājus vai uztveršanas un izsekošanas ierīces (saskaņā ar *FISA* 402. pantu), ir jāiesniedz *FISC* (vai ASV miertiesneša) rīkojuma saņemšanas pieteikums un jāizmanto īpašs atlases nosacījums, t. i., nosacījums, kas konkrēti identificē personu, kontu utt. un tiek izmantots, lai maksimāli ierobežotu pieprasītās informācijas apmēru ([286]). Šī pilnvara nav saistīta ar paziņojumu saturu, bet drīzāk ir ar mērķi informēt par klientu vai abonentu, kas izmanto pakalpojumu (piemēram, vārds un uzvārds, adrese, abonenta numurs, saņemtā pakalpojuma ilgums/veids, maksājuma avots/līdzeklis).

(152) *FISA* 501. pantā ([287]), kas ļauj vākt pārvadātāja (t. i., jebkuras personas vai organizācijas, kas par atlīdzību pārvadā cilvēkus vai īpašumu pa sauszemi, dzelzceļu, ūdeni vai gaisu), publiskas izmitināšanas iestādes (piemēram, viesnīcas, moteļa vai kroga), transportlīdzekļu nomas iestādes vai fiziskas noliktavas (t. i., iestādes, kas nodrošina vietu preču un materiālu uzglabāšanai vai sniedz ar to saistītus pakalpojumus) ([288]) komercdarbības dokumentus, arī noteikts, ka nepieciešams iesniegt pieteikumu *FISC* vai miertiesnesim. Šajā pieteikumā ir jānorāda pieprasītie dokumenti un konkrēti un skaidri formulēti fakti, kas dod pamatu uzskatīt, ka persona, uz kuru dokumenti attiecas, ir kāda sveša vara vai svešas varas aģents ([289]).

(153) Visbeidzot, *NSL* ir atļautas ar dažādiem likumiem un ļauj izmeklēšanas iestādēm no konkrētām struktūrām (piemēram, finanšu iestādēm, kredītinformācijas aģentūrām, elektronisko sakaru pakalpojumu sniedzējiem) iegūt konkrētu informāciju (kas neietver saziņas saturu), kura iekļauta kredītinformācijā, finanšu pārskatos un elektroniskajos abonentu un darījumu reģistros ([290]). Likumu par *NSL*, kas atļauj piekļuvi elektroniskās saziņas saturam, var izmantot tikai FIB, un tajos ir noteikts, ka pieprasījumos ir jāizmanto nosacījums, kas konkrēti identificē personu, struktūru, tālruņa numuru vai kontu, un jāapliecina, ka informācija ir relevanta atļautai nacionālās drošības izmeklēšanai, lai nodrošinātu aizsardzību pret starptautisko terorismu vai slepenām izlūkošanas darbībām ([291]). *NSL* saņēmējiem ir tiesības to apstrīdēt tiesā ([292]).

([281]) 50 U.S. Code § 1842(c)(3) un attiecībā uz *NSL* – 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a) un 18 U.S.C. § 2709(a).

([282]) "Svešas varas aģents" var ietvert personas, kas nav ASV personas un kas iesaistījušies starptautiskā terorismā vai starptautiskā masu iznīcināšanas ieroču izplatīšanā (šāda iesaistīšanās ietver arī sagatavošanās darbības) (50 U.S.C. § 1801 (b)(1)).

([283]) 50 U.S.C. § 1804. Sk. arī § 1841(4) attiecībā uz atlases noteikumu izvēli.

([284]) 50 U.S.C. § 1821(5).

([285]) 50 U.S.C. § 1823(a).

([286]) 50 U.S.C. § 1842 kopā ar § 1841(2) un *Section 3127 of Title 18*.

([287]) 50 U.S.C. § 1862.

([288]) 50 U.S.C. §§ 1861-1862.

([289]) 50 U.S.C. § 1862(b).

([290]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v un 18 U.S.C. § 2709.

([291]) 18 U.S.C. § 2709(b).

([292]) Piemēram, 18 U.S.C. § 2709(d).

3.2.1.3. *Savāktās informācijas turpmāka izmantošana*

(154) Uz to personas datu apstrādi, ko ASV izlūkošanas aģentūras savākušas, izmantojot sakaru izlūkošanu, attiecas vairākas garantijas.

(155) Pirmkārt, katrai izlūkošanas aģentūrai ir jānodrošina pienācīga datu drošība un jānovērš nepilnvarotu personu piekļuve personas datiem, kas iegūti, izmantojot sakaru izlūkošanu. Šajā sakarā dažādos instrumentos, to skaitā likumos, pamatnostādnēs un standartos, ir sīkāk precizētas obligāti ieviešamas informācijas drošības prasības (piemēram, daudzfaktoru autentifikācija, šifrēšana u. c.) ([293]). Piekļūt savāktajiem datiem drīkst tikai pilnvaroti, apmācīti darbinieki, kuriem šī informācija ir nepieciešama savu darba pienākumu veikšanai ([294]). Raugoties vispārīgāk, izlūkošanas aģentūrām ir jānodrošina saviem darbiniekiem atbilstoša apmācība, arī par procedūrām, kuras ievēro, ziņojot par tiesību aktu pārkāpumiem un tos novērš (arī IR Nr. 14086) ([295]).

(156) Otrkārt, izlūkošanas aģentūrām ir jāievēro izlūkošanas kopienas precizitātes un objektivitātes standarti, jo īpaši attiecībā uz datu kvalitātes un uzticamības nodrošināšanu, alternatīvu informācijas avotu apsvēršanu un objektivitāti analīžu veikšanā ([296]).

(157) Treškārt, attiecībā uz datu saglabāšanu IR Nr. 14086 ir precizēts, ka uz tādu personu personas datiem, kas nav ASV personas, attiecas tie paši saglabāšanas termiņi, kuri attiecas uz ASV personu personas datiem ([297]). Izlūkošanas aģentūrām ir jānosaka konkrēti saglabāšanas termiņi un/vai faktori, kas jāņem vērā, lai noteiktu atbilstošo saglabāšanas termiņu (piemēram, vai informācija ir noziedzīga nodarījuma pierādījums; vai informācija ir uzskatāma par ārējas izlūkošanas informāciju; vai informācija ir nepieciešama, lai aizsargātu personu vai organizāciju drošību, ieskaitot starptautiskā terorisma upurus vai mērķus), kas ir definēts citos tiesību instrumentos ([298]).

(158) Ceturtkārt, īpašus noteikumus piemēro tādu personas datu izplatīšanai, kas iegūti, izmantojot sakaru izlūkošanu. Vispārīga prasība paredz, ka personas datus par personām, kas nav ASV personas, drīkst izplatīt tikai tad, ja tā ir tāda paša veida informācija, kādu var izplatīt par ASV personām, piemēram, informācija, kas vajadzīga, lai aizsargātu kādas personas vai organizācijas drošību (piemēram, starptautisko teroristu organizāciju mērķus, upurus vai ķīlniekus) ([299]). Turklāt personas datus nedrīkst izplatīt tikai personas valstspiederības vai dzīvesvietas valsts dēļ vai lai apietu IR Nr. 14086 prasības ([300]). Izplatīšana ASV valdības ietvaros var notikt tikai tad, ja pilnvarotai un

([293]) *Section 2(c)(iii)(B)(1)*, IR Nr. 14086. Sk. arī Nacionālās drošības likuma VIII sadaļu (kurā sīki izklāstītas prasības attiecībā uz piekļuvi klasificētai informācijai), IR Nr. 12333, *section 1.5*, (kurā noteikts, ka izlūkošanas kopienas aģentūru vadītājiem jāievēro informācijas apmaiņas un drošības pamatnostādnes, informācijas privātuma un citas juridiskās prasības), Nacionālās drošības direktīva Nr. 42 *National Policy for the Security of National Security Telecommunications and Information Systems* (kurā Nacionālās drošības sistēmu komitejai uzdots nodrošināt sistēmas drošības vadlīnijas izpildministrijām un izpildaģentūrām attiecībā uz nacionālās drošības sistēmām) un Nacionālās drošības memorandu Nr. 8 *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* (ar kuru nosaka termiņus un norādījumus par to, kā tiks īstenotas kiberdrošības prasības attiecībā uz nacionālās drošības sistēmām, to skaitā saistībā ar daudzfaktoru autentifikāciju, šifrēšanu, mākoņtehnoloģijām un galapunktu noteikšanas pakalpojumiem).

([294]) *Section 2(c)(iii)(B)(2)*, IR Nr. 14086. Turklāt personas datiem, attiecībā uz kuriem nav pieņemts galīgais lēmums par saglabāšanu, var piekļūt, tikai lai pieņemtu vai atbalstītu šādu lēmumu vai veiktu atļautas administratīvas, testēšanas, izstrādes, drošības vai pārraudzības funkcijas (*Section 2(c)(iii)(B)(3)*, IR Nr. 14086).

([295]) *Section 2(d)(ii)*, IR Nr. 14086.

([296]) *Section 2(c)(iii)(C)*, IR Nr. 14086.

([297]) *Section 2(c)(iii)(A)(2)(a)-(c)*, IR Nr. 14086. Raugoties vispārīgāk, katrai aģentūrai ir jāievieš politika un procedūras, kas izstrādātas, lai līdz minimumam samazinātu ar sakaru izlūkošanas palīdzību savākto personas datu izplatīšanu un saglabāšanas ilgumu (*Section 2(c)(iii)(A)*, IR Nr. 14086)).

([298]) Sk., piemēram, *Section 309 of the Intelligence Authorization Act for Fiscal Year 2015*; atsevišķu izlūkošanas aģentūru apstiprinātās minimizācijas procedūras saskaņā ar *FISA* 702. pantu un ar *FISC* atļauju; ģenerālprokurora un *FRA* apstiprinātas procedūras (kas paredz, ka ASV federālajām aģentūrām, ieskaitot nacionālās drošības aģentūras, ir jānosaka datu saglabāšanas termiņi, ko apstiprina Nacionālais arhīvs un Datu administrācija).

([299]) *Section 2(c)(iii)(A)(1)(a)* un *5(d)*, IR Nr. 14086, saistībā ar *Section 2.3* IR Nr. 12333.

([300]) *Section 2(c)(iii)(A)(1)(b)* un (e), IR Nr. 14086.

apmācītai personai ir pamatota pārliecība, ka saņēmējam šī informācija ([301]) ir nepieciešama un ka saņēmējs to pienācīgi aizsargās ([302]). Lai noteiktu, vai personas datus var izplatīt saņēmējiem ārpus ASV valdības (tajā skaitā ārvalstu valdībai vai starptautiskai organizācijai), ir jāņem vērā izplatīšanas nolūks, izplatāmo datu veids un apjoms, kā arī iespējamā negatīvā ietekme uz attiecīgo(-ajām) personu(-ām) ([303]).

(159) Visbeidzot, arī lai atvieglotu piemērojamo juridisko prasību ievērošanas pārraudzību, kā arī efektīvu tiesiskās aizsardzības līdzekļu izmantošanu, saskaņā ar IR Nr. 14086 katrai izlūkošanas aģentūrai ir jāglabā atbilstoša dokumentācija par sakaru izlūkdatu vākšanu. Dokumentācijas prasības attiecas uz tādiem elementiem kā faktu bāze novērtējumam, vai konkrēta vākšanas darbība ir nepieciešama, lai veicinātu apstiprinātas izlūkošanas prioritātes īstenošanu ([304]).

(160) Papildus minētajiem IR Nr. 14086 paredzētajiem drošības pasākumiem attiecībā uz sakaru izlūkošanas ietvaros savāktajiem datiem uz visām ASV izlūkošanas aģentūrās attiecas arī vispārīgākas prasības par nolūka ierobežošanu, datu minimizēšanu, precizitāti, drošību, saglabāšanu un izplatīšanu, kas izriet jo īpaši no *OMB Circular* Nr. A-130, E-pārvaldes likuma, Federālā reģistru likuma (sk. 101.–106. apsvērumu) un Nacionālās drošības sistēmu komitejas (*CNSS*) norādījumiem ([305]).

3.2.2. ***Pārraudzība***

(161) ASV izlūkošanas aģentūru darbību uzrauga dažādas iestādes.

(162) Pirmkārt, IR Nr. 14086 prasīts, lai katrā izlūkošanas aģentūrā būtu augsta līmeņa juridiskās, pārraudzības un atbilstības amatpersonas, kas nodrošinātu atbilstību piemērojamajiem ASV tiesību aktiem ([306]). Jo īpaši tām ir periodiski jāpārrauga sakaru izlūkošanas darbības un jānodrošina, ka tiek novērstas jebkādas neatbilstības. Izlūkošanas aģentūrām jānodrošina šādām amatpersonām piekļuve visai relevantajai informācijai, lai tās varētu veikt pārraudzības funkcijas, un aģentūras nedrīkst veikt nekādas darbības, lai kavētu vai neatbilstoši ietekmētu to pārraudzības darbības ([307]). Turklāt par jebkuru būtisku neatbilstības incidentu ([308]), ko konstatē pārraudzības amatpersona vai jebkurš cits darbinieks, nekavējoties jāziņo izlūkošanas aģentūras vadītājam un nacionālās izlūkošanas direktoram, kam jānodrošina, ka tiek veikti visi nepieciešamie pasākumi, lai novērstu un nepieļautu būtiska neatbilstības incidenta atkārtošanos ([309]).

(163) Šo pārraudzības funkciju veic amatpersonas, kas ir atbildīgas par atbilstības nodrošināšanu, kā arī privātuma un pilsonisko brīvību amatpersonas un ģenerālinspektori ([310]).

([301]) Piemēram, *AGG-DOM* paredz, ka FIB var izplatīt informāciju, tikai ja saņēmējam to ir nepieciešams zināt, lai izpildītu savu saņēmēja uzdevumu vai aizsargātu sabiedrības intereses.

([302]) *Section 2(c)(iii)(A)(1)(c)*, IR Nr. 14086. Izlūkošanas aģentūras var, piemēram, izplatīt informāciju situācijās, kas saistītas ar kriminālizmeklēšanu vai noziedzīgu nodarījumu, arī, piemēram, izplatot brīdinājumus par nonāvēšanas, smagu miesas bojājumu vai nolaupīšanas draudiem; izplatot informāciju par kiberdraudiem, incidentiem vai ielaušanos un apziņojot cietušos vai brīnot potenciālus noziedzīgā nodarījumā cietušos.

([303]) *Section 2(c)(iii)(A)(1)(d)*, IR Nr. 14086.

([304]) *Section 2(c)(iii)(E)*, IR Nr. 14086.

([305]) Sk. *CNSS* politiku Nr. 22 "Kiberdrošības risku pārvaldības politika" un *CNSS* instrukcijas Nr. 1253, kuras doti detalizēti norādījumi par drošības pasākumiem, kas ieviešami nacionālās drošības sistēmās.

([306]) *Section 2(d)(i)(A)-(B)*, IR Nr. 14086.

([307]) *Sections 2(d)(i)(B)-(C)*, IR Nr. 14086.

([308]) T. i., sistēmiska vai tīša piemērojamo ASV tiesību aktu neievērošana, kas varētu kaitēt kādas izlūkošanas kopienas reputācijai vai integritātei vai kā citādi apšaubīt izlūkošanas kopienas darbības pareizību, arī ņemot vērā jebkādu būtisku ietekmi uz attiecīgās personas vai personu privātuma un pilsonisko brīvību interesēm, sk. *Section 5(l)*, IR Nr. 14086.

([309]) *Section 2(d)(iii)*, IR Nr. 14086.

([310]) *Section 2(d)(i)(B)*, IR Nr. 14086.

(164) Tāpat kā krimināltiesību aizsardzības iestāžu gadījumā, privātuma un pilsonisko brīvību amatpersonas ir visās izlūkošanas aģentūrās ([311]). Šo amatpersonu pilnvaras parasti ietver tādu procedūru uzraudzību, kuras nodrošina, ka attiecīgā ministrija/aģentūra adekvāti izskata ar privātumu un pilsoniskajām brīvībām saistītus jautājumus un ir ieviesusi atbilstošas procedūras, ar kurām risināt sūdzības no fiziskām personām, kas uzskata, ka ir aizskarts viņu privātums un pilsoniskās brīvības (un atsevišķos gadījumos, piemēram Nacionālās izlūkošanas direktora biroja (*ODNI*) gadījumā, šīm amatpersonām pašām ir tiesības izmeklēt sūdzības ([312])). Izlūkošanas aģentūru vadītājiem ir jānodrošina, lai privātuma un pilsonisko brīvību amatpersonām būtu resursi viņu pilnvaru īstenošanai, lai tām būtu pieejami visi viņu funkciju veikšanai nepieciešamie materiāli un personāls, lai viņas tiktu informētas par ierosinātajām politikas izmaiņām un ar viņām apspriestos par tām ([313]). Privātuma un pilsonisko brīvību amatpersonas periodiski ziņo Kongresam un *PCLOB*, arī par ministrijā/aģentūrā saņemto sūdzību skaitu un raksturu, un sniedz kopsavilkumu par šādu sūdzību izskatīšanu, veiktajām pārbaudēm un izmeklēšanām un amatpersonas veikto darbību ietekmi ([314]).

(165) Otrkārt, katrai izlūkošanas aģentūrai ir neatkarīgs ģenerālinspektors, kura pienākums, cita starpā, ir pārraudzīt ārējās izlūkošanas darbības. *ODNI* ietvaros tas ir Izlūkošanas kopienas ģenerālinspektora birojs, kam ir visaptveroša kompetence attiecībā uz visu izlūkošanas kopienu un pilnvaras izmeklēt sūdzības vai informāciju saistībā ar apgalvojumiem par nelikumīgu rīcību vai ļaunprātīgu varas izmantošanu saistībā ar *ODNI* un/vai izlūkošanas kopienas programmām un darbībām ([315]). Tāpat kā krimināltiesību aizsardzības iestāžu gadījumā (sk. 109. apsvērumu), šādi ģenerālinspektori saskaņā ar likumu ir neatkarīgi ([316]) un ir atbildīgi par revīziju un izmeklēšanu veikšanu saistībā ar programmām un darbībām, ko attiecīgā aģentūra veic valsts izlūkošanas nolūkos, arī attiecībā uz ļaunprātīgu izmantošanu vai likuma pārkāpšanu ([317]). Tiem ir piekļuve visiem ierakstiem, atskaitēm, revīziju materiāliem, pārskatiem, dokumentiem, materiāliem, ieteikumiem un citiem relevantiem materiāliem,

([311]) Sk. 42 U.S.C. § 2000ee-1. To vidū ir, piemēram, Valsts ministrija, Tieslietu ministrija, Iekšzemes drošības ministrija, Aizsardzības ministrija, *NSA*, Centrālā izlūkošanas pārvalde (CIP), FIB un *ODNI*.

([312]) Sk. *Section 3(c)*, IR Nr. 14086.

([313]) 42 U.S.C. § 2000ee-1(d).

([314]) Sk. 42 U.S.C. § 2000ee-1 (f)(1),(2). Piemēram, *NSA* Pilsonisko brīvību, privātuma un pārredzamības biroja ziņojums par laikposmu no 2021. gada janvāra līdz 2021. gada jūnijam liecina, ka tas ir veicis 591 pārbaudi par ietekmi uz pilsoniskajām brīvībām un privātumu dažādos kontekstos, piemēram, attiecībā uz datu vākšanas darbībām, informācijas apmaiņas mehānismiem un lēmumiem, lēmumiem par datu saglabāšanu u. c., ņemot vērā dažādus faktorus, piemēram, ar konkrēto darbību saistītās informācijas apjomu un veidu, iesaistītās fiziskās personas, datu vākšanas nolūku un paredzamo izmantošanu, garantijas, kas ieviestas, lai mazinātu iespējamos privātuma riskus u. c.(https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Līdzīgi arī CIP Privātuma un pilsonisko brīvību biroja ziņojumos par 2019. gada janvāri–jūniju, ir sniegta informācija par biroja pārraudzības darbībām, piemēram, sniegts pārskats par atbilstību ģenerālprokurora pamatnostādnēm saskaņā ar IR Nr. 12333 attiecībā uz informācijas saglabāšanu un izplatīšanu, sniegtajiem norādījumiem par PPD 28 īstenošanu un prasībām identificēt un novērst datu aizsardzības pārkāpumus, kā arī sniegti pārskati par personas datu izmantošanu un apstrādi (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Šo ģenerālinspektoru ieceļ prezidents ar Senāta apstiprinājumu, un viņu var atstādināt tikai prezidents.

([316]) Ģenerālinspektoram ir noteikts laiks amatā, un to var atstādināt tikai prezidents, kuram rakstveidā jāpaziņo Kongresam šādas atstādināšanas iemesli. Tas nebūt nenozīmē, ka uz tiem pilnībā neattiecas norādījumi. Dažos gadījumos ministrijas vadītājs var aizliegt ģenerālinspektoram sākt, 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. Sk. 1978. gada Ģenerālinspektoru likumu, § 8 (par Aizsardzības ministriju); § 8E (par *DoJ*), § 8G (d)(2)(A),(B) (par *NSA*); 50. U.S.C. § 403q (b) (par CIP); *Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f)* (par izlūkošanas kopienu).

([317]) Sk. 1978. gada Ģenerālinspektoru likumu ar grozījumiem, *Pub. L. 117-108 of 8 April 2022*. Piemēram, kā paskaidrots *NSA* ģenerālinspektora pusgada ziņojumos Kongresam par laikposmu no 2021. gada 1. aprīļa līdz 2022. gada 31. martam, *NSA* ģenerālinspektors veica izvērtējumus par darbībām ar informāciju par ASV personām, kas savākta saskaņā ar IR Nr. 12333, par sakaru izlūkošanas datu neatgriezeniskas dzēšanas procesu, par *NSA* izmantoto automatizēto mērķorientēšanas rīku, kā arī par dokumentācijas un vaicājumu noteikumu ievērošanu attiecībā uz datu vākšanu atbilstīgi *FISA* 702. pantam, un šajā sakarā izdeva vairākus ieteikumus (sk. https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, 5.–8. lpp. un https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907 10.–13. lpp.). Sk. arī nesen veiktās izlūkošanas kopienas ģenerālinspektora revīzijas un izmeklēšanas par informācijas drošību un neatļautu klasificētas nacionālās drošības informācijas izpaušanu (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, 8., 11. lpp. un https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, 19.–20. lpp.).

vajadzības gadījumā ar tiesas pavēsti, un tie var iegūt liecības nopratināšanā ([318]). Ģenerālinspektori nodod lietas, kurās ir aizdomas par noziedzīgiem nodarījumiem, kriminālvajāšanai un sniedz ieteikumus aģentūru vadītājiem par korektīvām darbībām ([319]). Kaut arī to ieteikumi nav saistoši, to ziņojumi – arī par turpmāku rīcību (vai tās neveikšanu) ([320]) – parasti tiek publiskoti un nosūtīti Kongresam, kas, pamatojoties uz tiem, var izmantot savu pārraudzības funkciju (sk. 168. un 169. apsvērumu) ([321]).

(166) Treškārt, Izlūkošanas pārraudzības padome (*IOB*), kas ir izveidota Prezidenta izlūkošanas konsultatīvajā padomē (*PIAB*) pārrauga to, kā ASV izlūkošanas iestādes ievēro Konstitūciju un visus piemērojamos noteikumus ([322]). *PIAB* ir konsultatīva struktūra, kas darbojas Prezidenta izpildbirojā – tās sastāvā ir 16 locekļi, kuri nav saistīti ar ASV valdību un kurus ieceļ prezidents. *IOB* sastāvā ir ne vairāk kā pieci locekļi, kurus no *PIAB* locekļu vidus ieceļ priekšsēdētājs. Saskaņā ar IR Nr. 12333 ([323]) visu izlūkošanas aģentūru vadītājiem ir pienākums ziņot *IOB* par ikvienu izlūkošanas darbību, par kuru ir pamats uzskatīt, ka tā varētu būt nelikumīga vai pretrunā izpildrīkojumam vai prezidenta direktīvai. Lai nodrošinātu, ka *IOB* ir piekļuve informācijai, kas nepieciešama tās funkciju veikšanai, izpildrīkojumā Nr. 13462 ir uzdots nacionālās izlūkošanas direktoram un izlūkošanas aģentūru vadītājiem sniegt visu informāciju un palīdzību, ko *IOB* uzskata par nepieciešamu tās funkciju veikšanai, ciktāl to atļauj likums ([324]). Savukārt *IOB* ir pienākums informēt prezidentu par izlūkošanas darbībām, kas, pēc tās domām, varētu būt pretrunā ASV tiesību aktiem (arī izpildrīkojumiem) un ko pienācīgi nenovērš ģenerālprokurors, nacionālās izlūkošanas direktors vai izlūkošanas aģentūras vadītājs ([325]). Turklāt *IOB* ir pienākums informēt ģenerālprokuroru par iespējamiem krimināltiesību pārkāpumiem.

(167) Ceturtkārt, izlūkošanas aģentūrās ir pakļautas *PCLOB* pārraudzībai. Saskaņā ar *PCLOB* dibināšanas statūtiem tai ir uzticēti pienākumi pretterorisma politikas un tās īstenošanas jomā ar mērķi aizsargātu privātumu un pilsoniskās brīvības. Pārbaudot izlūkošanas aģentūru darbības, tā var piekļūt visiem attiecīgo aģentūru ierakstiem, atskaitēm, revīziju materiāliem, pārskatiem, dokumentiem, materiāliem un ieteikumiem (arī klasificētai informācijai), veikt nopratināšanu un uzklausīt liecības ([326]). Tā saņem ziņojumus no dažādu federālo ministriju/aģentūru pilsonisko brīvību un privātuma amatpersonām ([327]), var izdot ieteikumus valdībai un izlūkošanas aģentūrām un regulāri sniedz atskaites Kongresa komitejām un prezidentam ([328]). Padomes ziņojumi – arī Kongresam adresētie – jādara maksimāli publiski pieejami ([329]). *PCLOB* ir publicējusi vairākus ziņojumus par pārraudzību un turpmākiem pasākumiem, tajā skaitā analīzi par programmām, kas tiek īstenotas, pamatojoties uz *FISA* 702. pantu, un privātuma aizsardzību šajā kontekstā, kā arī PPD 28 un IR Nr. 12333 īstenošanu ([330]). *PCLOB* ir uzdots arī veikt

([318]) Sk. 1978. gada Ģenerālinspektoru likumu, § 6.

([319]) Sk. turpat §§ 4, 6-5.

([320]) Attiecībā uz turpmākiem pasākumiem, kas tiek veikti saistībā ar ģenerālinspektoru ziņojumiem un ieteikumiem, skatīt, piemēram, reakciju uz *DoJ* ģenerālinspektora ziņojumu, kurā konstatēts, ka FIB nav pietiekami pārredzami sadarbojies ar *FISC* saistībā ar pieteikumiem laikposmā no 2014. līdz 2019. gadam, kā rezultātā tika veiktas reformas, lai uzlabotu atbilstību, pārraudzību un pārskatatbildību FIB (piemēram, FIB direktors uzdeva veikt vairāk nekā 40 korektīvu darbību, to skaitā 12 konkrēti ar *FISA* procesu saistītu darbību, kas attiecas uz dokumentāciju, uzraudzību, lietu uzturēšanu, apmācību un revīzijām) (sk. https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance un https://oig.justice.gov/reports/2019/o20012.pdf). Sk., piemēram, arī *DoJ* ģenerālinspektora veikto revīziju par FIB Galvenā juriskonsulta biroja funkcijām un pienākumiem, pārraugot atbilstību piemērojamajiem tiesību aktiem, politikai un procedūrām saistībā ar FIB darbībām nacionālās drošības jomā, un 2. papildinājumu, kurā iekļauta FIB vēstule, kurā pieņemti visi sniegtie ieteikumi. Šajā saistībā 3. papildinājumā ir sniegts pārskats par turpmākajiem pasākumiem un informāciju, ko ģenerālinspektors pieprasīja no FIB, lai varētu slēgt savus ieteikumus (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Sk. 1978. gada Ģenerālinspektoru likumu, §§ 4(5), 5.

([322]) Sk. IR Nr. 13462.

([323]) *Section 1.6(c)*, IR Nr. 12333.

([324]) *Section 8(a)*, IR Nr. 13462.

([325]) *Section 6(b)*, IR Nr. 13462.

([326]) 42 U.S.C. § 2000ee (g).

([327]) Sk. 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). To vidū ir vismaz Tieslietu ministrija, Aizsardzības ministrija, Iekšzemes drošības ministrija, nacionālās izlūkošanas direktors un Centrālā izlūkošanas pārvalde, kā arī jebkurš cita ministrija, aģentūra vai struktūra, kuru *PCLOB* atzinusi par piemērotu.

([328]) 42 U.S.C. §2000ee (e).

([329]) 42 U.S.C. § 2000ee (f).

([330]) Pieejams tīmekļa vietnē https://www.pclob.gov/Oversight.

īpašas pārraudzības funkcijas saistībā ar IR Nr. 14086 īstenošanu, jo īpaši pārbaudot, vai aģentūras procedūras atbilst IR (sk. 126. apsvērumu), un izvērtējot tiesiskās aizsardzības mehānisma darbību (sk. 194. apsvērumu).

(168) Piektkārt, papildus pārraudzības mehānismiem izpildvarā par visu ASV ārējās izlūkošanas darbību pārraudzību atbildīgas ir arī īpašas ASV Kongresa komitejas (Pārstāvju palātas un Senāta Izlūkošanas komiteja un Tieslietu komiteja). Šo komiteju locekļiem ir piekļuve klasificētai informācijai, kā arī izlūkošanas metodēm un programmām ([331]). Šīs komitejas savas pārraudzības funkcijas īsteno dažādos veidos, jo īpaši uzklausīšanas, izmeklēšanas, pārskatu un ziņojumu veidā ([332]).

(169) Kongresa komitejas regulāri saņem ziņojumus par izlūkošanas darbībām, tajā skaitā no ģenerālprokurora, nacionālās izlūkošanas direktora, izlūkošanas aģentūrām un citām pārraudzības struktūrām (piemēram, ģenerālinspektoriem), sk. 164. un 165. apsvērumu. Jo īpaši saskaņā ar Nacionālās drošības likumu "prezidents nodrošina, ka Kongresa izlūkošanas komitejas tiek pilnībā un vienmēr informētas par Amerikas Savienoto Valstu izlūkošanas darbībām, tajā skaitā par jebkādu nozīmīgu gaidāmu izlūkošanas darbību, kas vajadzīga saskaņā ar šo apakšnodaļu" ([333]). Turklāt "prezidents nodrošina, ka Kongresa izlūkošanas komitejām nekavējoties tiek ziņots par ikvienu izlūkošanas darbību, kā arī ikvienu korektīvu darbību, kas ir veikta vai tiek plānota saistībā ar šādu nelikumīgu rīcību" ([334]).

(170) Turklāt no īpašiem likumiem izriet papildu ziņošanas prasības. Piemēram, *FISA* paredz, ka ģenerālprokuroram ir "pilnībā jāinformē" Senāta un Pārstāvju palātas Izlūkošanas un Tieslietu komitejas par valdības darbībām saskaņā ar atsevišķiem *FISA* pantiem ([335]). Tajā arī noteikts, ka valdībai ir jāiesniedz Kongresa komitejām "kopijas visiem lēmumiem, rīkojumiem vai atzinumiem, ko izdevusi *FISC* vai *FISCR* un kas ietver" *FISA* noteikumu "būtisku izskaidrojumu vai interpretāciju". Attiecībā uz novērošanu saskaņā ar *FISA* 702. pantu Kongresa palātu īstenotu pārraudzību veic ar likumā noteiktiem ziņojumiem Izlūkošanas un Tieslietu komitejām, kā arī regulārām instruktāžām un uzklausīšanām. Tajā skaitā ir ģenerālprokurora pusgada ziņojums, kurā aprakstīta *FISA* 702. panta izmantošana, ar pievienotiem apliecinošiem dokumentiem, tajā skaitā Tieslietu ministrijas un *ODNI* atbilstības ziņojumi un jebkādu neatbilstības gadījumu apraksts ([336]), kā arī atsevišķs ģenerālprokurora un *NID* pusgada novērtējums, kurā dokumentēta atbilstība mērķorientēšanas un minimizācijas procedūrām ([337]).

([331]) 50 U.S.C. § 3091.

([332]) Piemēram, komitejas organizē tematiskas uzklausīšanas (sk., piemēram, nesen notikušo Pārstāvju palātas Tieslietu komitejas uzklausīšanu par digitālajiem sistemātiskas meklēšanas tīkliem https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983 un Pārstāvju palātas Izlūkošanas komitejas uzklausīšanu par mākslīgā intelekta izmantošanu izlūkošanas struktūrās, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), regulāras pārraudzības uzklausīšanas, piemēram, attiecībā uz FIB un *DoJ* nacionālās drošības nodaļu, sk. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 un https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Kā izmeklēšanas piemēru skatīt Senāta Izlūkošanas komitejas izmeklēšanu par Krievijas iejaukšanos 2016. gada ASV vēlēšanās – https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. Attiecībā uz ziņojumiem skatīt, piemēram, pārskatu par komitejas (pārraudzības) darbību Senāta Izlūkošanas komitejas ziņojumā Senātam par laikposmu no 2019. gada 4. janvāra līdz 2021. gada 3. janvārim – https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Sk. 50 U.S.C. § 3091(a)(1). Šajā noteikumā ir iekļautas vispārīgas prasības attiecībā uz Kongresa pārraudzību nacionālās drošības jomā.

([334]) Sk. 50 U.S.C. §3091(b).

([335]) Sk. 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

([336]) Sk. 50 U.S.C. § 1881f.

([337]) Sk.50 U.S.C. § 1881a(l)(1).

(171) Turklāt *FISA* ir noteikts, ka ASV valdībai katru gadu ir jāatklāj Kongresam (un sabiedrībai) *FISA* pieprasīto un saņemto rīkojumu skaits, kā arī cita starpā ASV personu un to personu, kas nav ASV personas, skaita aplēses, pret kurām vērsta novērošana ([338]). Ar likumu ir noteikta papildu publiska ziņošana par izdoto nacionālās drošības vēstuļu skaitu, atkal attiecībā gan uz ASV personām, gan personām, kas nav ASV personas (vienlaikus atļaujot *FISA* rīkojumu un apliecinājumu, kā arī nacionālās drošības vēstuļu pieprasījumu saņēmējiem noteiktos apstākļos izdot pārredzamības ziņojumus) ([339]).

(172) Raugoties vispārīgāk, ASV izlūkošanas kopiena veic dažādus pasākumus, lai nodrošinātu pārredzamību saistībā ar to īstenotajām (ārējās) izlūkošanas darbībām. Piemēram, 2015. gadā *ODNI* pieņēma izlūkošanas pārredzamības principus un pārredzamības īstenošanas plānu, kā arī uzdeva katrai izlūkošanas aģentūrai iecelt izlūkošanas pārredzamības amatpersonu, lai veicinātu pārredzamību un vadītu pārredzamības iniciatīvas ([340]). Šo centienu ietvaros izlūkošanas kopienas struktūras ir publiskojušas un turpina publiskot deklasificētas daļas no politikas, procedūrām, pārraudzības ziņojumiem, ziņojumiem par darbībām, kas veiktas saskaņā ar *FISA* 702. pantu un IR Nr. 12333, *FISC* lēmumiem un citiem materiāliem, arī tam īpaši paredzētā tīmekļa lapā "*IC on the Record*", ko pārvalda *ODNI* ([341]).

(173) Visbeidzot, personas datu vākšanu saskaņā ar *FISA* 702. pantu papildus 162.–168. apsvērumā minētajai pārraudzības iestāžu veiktajai uzraudzībai pārrauga arī *FISC* ([342]). Saskaņā ar *FISC* reglamenta 13. noteikumu ASV izlūkošanas aģentūru atbilstības amatpersonām par jebkādiem *FISA* 702. panta mērķorientēšanas, minimizēšanas un vaicājumu procedūru pārkāpumiem ir jāziņo *DoJ* un *ODNI*, kas savukārt par tiem ziņo *FISC*. Turklāt *DoJ* un *ODNI* reizi pusgadā iesniedz *FISC* kopīgus pārraudzības novērtējuma ziņojumus, kuros ir norādītas mērķorientēšanas atbilstības tendences; sniegti statistikas dati; aprakstītas atbilstības incidentu kategorijas; detalizēti aprakstīti iemesli, kādēļ ir notikuši konkrēti mērķorientēšanas atbilstības incidenti, un izklāstīti pasākumi, ko izlūkošanas aģentūras ir veikušas, lai izvairītos no šādu incidentu atkārtošanās ([343]).

(174) Vajadzības gadījumā (piemēram, ja tiek konstatēti mērķorientēšanas procedūru pārkāpumi) Tiesa var uzdot attiecīgajai izlūkošanas aģentūrai veikt koriģējošus pasākumus ([344]). Attiecīgie koriģējošie pasākumi var būt gan individuāli, gan strukturāli, piemēram, no datu iegūšanas pārtraukšanas un nelikumīgi iegūto datu dzēšanas līdz datu vākšanas prakses maiņai, arī attiecībā uz vadlīnijām un darbinieku apmācību ([345]). Turklāt, katru gadu pārskatot 702. panta sertifikācijas apliecinājumus, *FISC* izskata neatbilstības incidentus, lai noteiktu, vai iesniegtie

([338]) 50 U.S.C. § 1873(b). Papildus tam saskaņā ar 402. pantu "nacionālās izlūkošanas direktors, konsultējoties ar ģenerālprokuroru, veic katra Ārējās izlūkošanas uzraudzības tiesas vai Ārējās izlūkošanas uzraudzības pārskatīšanas tiesas izdota lēmuma, rīkojuma vai atzinuma deklasificēšanas pārskatu (kā noteikts 601. panta e) punktā), kurā iekļauta jebkura likuma noteikuma būtiska interpretācija, tajā skaitā jebkāda jauna vai būtiska termina "specifisks atlases nosacījums" interpretācija, un atbilstīgi šim pārskatam katru lēmumu, rīkojumu vai atzinumu publisko pēc iespējas plašā mērogā".

([339]) 50 U.S.C. §§ 1873(b)(7) un1874.

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

([341]) Sk. "*IC on the Record*", kas pieejama https://icontherecord.tumblr.com/.

([342]) Iepriekš *FISC* secināja, ka "tiesai ir skaidrs, ka aģentūras, kas īsteno attiecīgos pasākumus, kā arī [*ODNI*] un [*DoJ* Nacionālās drošības daļa] velta ievērojamus resursus, lai pildītu tām 702. pantā noteiktos atbilstības nodrošināšanas un pārraudzības pienākumus. Parasti neatbilstības gadījumi tiek nekavējoties identificēti un tiek veikti attiecīgi koriģējoši pasākumi, kas cita starpā ietver informācijas, kas iegūta neatbilstoši vai uz kuru attiecas citas iznīcināšanas prasības saskaņā ar piemērojamām procedūrām, neatgriezenisku dzēšanu." *FISA* tiesas memorandatzinums un rīkojums [virsraksts rediģēts] (2014), pieejams https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) Sk., piemēram, *DOJ/ODNI FISA 702 Compliance Report to FISC for June 2018 – Nov. 2018* 21.–65. lpp.

([344]) 50 U.S.C. § 1803(h). Sk. arī PCLOB ziņojumu par 702. pantu, 76. lpp. Turklāt kā nepilnību novēršanas rīkojuma piemēru, kurā valdībai tika uzdots novērst konstatētās nepilnības 30 dienu laikā, sk. *FISC* 2011. gada 3. oktobra memorandatzinumu un rīkojumu. Pieejams šajā tīmekļa vietnē: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Sk. Valtona vēstules 4. iedaļu, 10. un 11. lpp. Sk. arī *FISC* 2018. gada 18. oktobra atzinumu (pieejams vietnē https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf), ko apstiprinājusi Ārējās izlūkošanas uzraudzības pārskatīšanas tiesa savā 2019. gada 12. jūlija atzinumā (pieejams vietnē https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf), kurā *FISC* cita starpā uzdeva valdībai ievērot konkrētas prasības attiecībā uz paziņošanu, dokumentāciju un ziņošanu *FISC*.

([345]) Sk., piemēram, *FISC* memorandatzinumu un rīkojumu, 76. lpp. (2019. gada 6. decembris) (publiskot atļauts 2020. gada 4. septembrī), kurā *FISC* uzdeva valdībai līdz 2020. gada 28. februārim iesniegt rakstisku ziņojumu par pasākumiem, ko valdība veikusi, lai uzlabotu procesus saistībā ar to ziņojumu identificēšanu un dzēšanu, kas izriet no *FISA* 702. pantā noteiktās informācijas un kas tika atsaukti atbilstības apsvērumu dēļ, kā arī par citiem jautājumiem. Sk. arī VII pielikumu.

apliecinājumi atbilst *FISA* prasībām. Tāpat, ja *FISC* konstatē, ka valdības apliecinājumi nav bijuši pietiekami, tajā skaitā konkrētu atbilstības incidentu dēļ, tā var izdot tā dēvēto rīkojumu par nepilnībām, kurā prasīts valdībai 30 dienu laikā novērst pārkāpumu vai kurā prasīts valdībai pārtraukt vai neuzsākt 702. panta apliecinājuma īstenošanu. Visbeidzot, *FISC* izvērtē konstatēto atbilstības problēmu tendences un var pieprasīt procedūru izmaiņas vai papildu pārraudzības un ziņošanas pasākumus, lai uzlabotu atbilstības tendences ([346]).

3.2.3. ***Tiesiskā aizsardzība***

(175) Kā sīkāk paskaidrots šajā iedaļā, Amerikas Savienotajās Valstīs ir vairāki veidi, kā nodrošināt datu subjektiem Savienībā iespēju celt prasību neatkarīgā un objektīvā tiesā, kas var pieņemt tiesiski saistošus lēmumus. Kopā tie dod iespēju fiziskām personām piekļūt saviem personas datiem, pieprasīt, lai tiktu pārbaudīts, vai valdība to datiem piekļūst likumīgi, un, ja tiek konstatēts pārkāpums, pieprasīt, lai šāds pārkāpums tiktu novērsts – tajā skaitā, lai personas dati tiktu izlaboti vai dzēsti.

(176) Pirmkārt, saskaņā ar IR Nr. 14086 ir izveidots īpašs tiesiskās aizsardzības mehānisms, ko papildina ĢP noteikumi, ar ko izveido Datu aizsardzības pārskatīšanas tiesu, lai tā izskatītu un risinātu fizisku personu sūdzības par ASV sakaru izlūkošanas darbībām. Ikvienai fiziskai personai no ES ir tiesības iesniegt sūdzību tiesiskās aizsardzības mehānismam par ASV tiesību aktu, ar ko reglamentē sakaru izlūkošanas darbības (piemēram, IR Nr. 14086, *FISA* 702. pants, IR Nr. 12333) iespējamu pārkāpumu, kas negatīvi ietekmē šīs personas privātuma un pilsonisko brīvību intereses ([347]). Šis tiesiskās aizsardzības mehānisms ir pieejams fiziskām personām no valstīm vai reģionālām ekonomiskās integrācijas organizācijām, kuras ASV ģenerālprokurors ir atzinis par "kvalificētām valstīm" ([348]). Eiropas Savienību un trīs Eiropas Brīvās tirdzniecības asociācijas valstis, kas kopā veido Eiropas Ekonomikas zonu, 2023. gada 30. jūnijā ģenerālprokurors saskaņā ar IR Nr. 14086, *Section 3(f) EO*, atzina par "kvalificētu valsti" ([349]). Šis apzīmējums neskar Līguma par Eiropas Savienību 4. panta 2. punktu.

(177) Savienības datu subjektam, kas vēlas iesniegt šādu sūdzību, tā jāiesniedz uzraudzības iestādei ES dalībvalstī, kuras kompetencē ir publisku iestāžu (DAI) veikta personas datu apstrāde ([350]). Tas nodrošina vieglu piekļuvi tiesiskās aizsardzības mehānismam, ļaujot fiziskām personām vērsties iestādē, kas atrodas "tuvu dzīvesvietai" un ar kuru tās var sazināties savā valodā. Pēc tam kad pārbaudītas 178. apsvērumā minētās prasības attiecībā uz sūdzības iesniegšanu, kompetentā DAI ar Eiropas Datu aizsardzības kolēģijas sekretariāta starpniecību virzīs sūdzību uz tiesiskās aizsardzības mehānismu.

(178) Sūdzības iesniegšanai tiesiskās aizsardzības mehānismā ir noteiktas zemas pieņemamības prasības, jo fiziskām personām nav jāpierāda, ka ar viņu datiem patiešām veiktas ASV sakaru izlūkošanas darbības ([351]). Tajā pašā laikā, lai nodrošinātu izejas punktu tiesiskās aizsardzības mehānismam pārbaudes veikšanai, ir jāsniedz noteikta pamatinformācija, piemēram, par personas datiem, par kuriem ir pamats uzskatīt, ka tie ir nosūtīti uz ASV, un līdzekļiem, ar kādiem tie, iespējams, tikuši nosūtīti; to ASV valdības iestāžu identitāte, kuras, domājams, ir iesaistītas iespējamajā pārkāpumā (ja tādas zināmas); pamats apgalvojumam, ka ir noticis ASV tiesību aktu pārkāpums (lai gan arī šajā gadījumā nav nepieciešams pierādīt, ka personas datus patiešām ir vākušas ASV izlūkošanas aģentūras), kā arī pieprasītā koriģējošā pasākuma veids.

([346]) Sk. VII pielikumu.

([347]) Sk. *Section 4(k)(iv)*, IR Nr. 14086, kurā noteikts, ka sūdzība tiesiskās aizsardzības mehānismam jāiesniedz pašam sūdzības iesniedzējam savā vārdā (t. i., nevis kā valdības, nevalstiskas vai starpvaldību organizācijas pārstāvim). Jēdziens "nelabvēlīgi ietekmēts" neparedz, ka sūdzības iesniedzējam būtu jāsasniedz noteikts slieksnis, lai tas varētu piekļūt tiesiskās aizsardzības mehānismam (šajā sakarā skatīt 178. apsvērumu). Tā vietā tas precizē, ka *ODNI CLPO* un *DPRC* ir pilnvaroti vērsties pret pārkāpumiem, kas skar ASV tiesību aktus par sakaru izlūkošanas darbībām, kuras negatīvi ietekmē sūdzības iesniedzēja privātumu un pilsoniskās brīvības. Savukārt tādu ASV tiesību aktu prasību, kas nav vērstas uz fizisku personu aizsardzību (piemēram, budžeta prasības), pārkāpumi neietilpst *ODNI CLPO* un *DPRC* jurisdikcijā.

([348]) *Section 3(f)*, IR Nr. 14086.

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

([350]) *Section 4(d)(v)*, IR Nr. 14086.

([351]) Sk. *Section 4(k)(i)-(iv)*, IR Nr. 14086.

(179) Sākotnējo izmeklēšanu par sūdzībām, kas iesniegtas šim tiesiskās aizsardzības mehānismam, veic *ODNI CLPO*, kuras pašreizējā likumā noteiktā loma un pilnvaras ir paplašinātas attiecībā uz tām konkrētajām darbībām, kas veiktas saskaņā ar IR Nr. 14086 ([352]). Izlūkošanas kopienā *CLPO* cita starpā ir atbildīga par to, lai *ODNI* un izlūkošanas aģentūru politikā un procedūrās tiktu pienācīgi iekļauta pilsonisko brīvību un privātuma aizsardzība; tā pārrauga, kā *ODNI* ievēro piemērojamās pilsonisko brīvību un privātuma prasības; un veic ietekmes uz privātumu novērtējumus ([353]). *ODNI CLPO* var atbrīvot no amata tikai nacionālās izlūkošanas direktors pamatota iemesla dēļ, proti, pārkāpuma, ļaunprātīgas rīcības, drošības pārkāpuma, nolaidības vai nespējas pildīt amata pienākumus gadījumā ([354]).

(180) Veicot pārbaudi, *ODNI CLPO* ir piekļuve informācijai, kas vajadzīga novērtējuma veikšanai, un šī amatpersona var paļauties uz dažādu izlūkošanas aģentūru privātuma un pilsonisko brīvību amatpersonu palīdzību, kas sniedzama obligāti ([355]). Izlūkošanas aģentūrām ir aizliegts kavēt vai neatbilstoši ietekmēt *ODNI CLPO* veiktās pārbaudes. Tas attiecas arī uz nacionālās izlūkošanas direktoru, kurš nedrīkst iejaukties pārbaudē ([356]). Izskatot sūdzību, *ODNI CLPO* "tiesību akti jāpiemēro objektīvi", ņemot vērā gan nacionālās drošības intereses saistībā ar sakaru izlūkošanas darbībām, gan privātuma aizsardzību ([357]).

(181) Pārbaudes gaitā *ODNI CLPO* nosaka, vai ir noticis piemērojamo ASV tiesību aktu pārkāpums, un tādā gadījumā pieņem lēmumu par atbilstošiem korektīviem pasākumiem ([358]). Ar šādiem korektīviem pasākumiem apzīmē pasākumus, ar kuriem pilnībā novērš konstatēto pārkāpumu, piemēram, pārtrauc nelikumīgu datu iegūšanu, dzēš nelikumīgi iegūtos datus, dzēš neatbilstoši veiktu vaicājumu rezultātus attiecībā uz citādi likumīgi iegūtiem datiem, ierobežo piekļuvi likumīgi iegūtajiem datiem tikai attiecīgi apmācītiem darbiniekiem vai atsauc izlūkošanas ziņojumus, kuros iekļauti dati, kas iegūti bez likumīgas atļaujas vai kas tikuši izplatīti nelikumīgi ([359]). *ODNI CLPO* lēmumi par fizisku personu sūdzībām (arī par korektīviem pasākumiem) ir saistoši attiecīgajām izlūkošanas aģentūrām ([360]).

(182) *ODNI CLPO* ir jāsaglabā pārbaudes dokumentācija un jāsagatavo klasificēts lēmums, kurā paskaidrots faktisko konstatējumu pamatojums, sniegts atzinums par to, vai attiecīgais pārkāpums ir noticis, un norādīts atbilstošs korektīvs pasākums ([361]). Ja *ODNI CLPO* pārbaudē atklāj kādas *FISC* pārraudzībā esošas iestādes pārkāpumu, *CLPO* jāiesniedz arī klasificēts ziņojums nacionālās drošības ģenerālprokurora vietniekam, kura pienākums savukārt ir ziņot par neatbilstību *FISC*, kas var veikt turpmākas izpildes panākšanas darbības (saskaņā ar 173. un 174. apsvērumā aprakstīto procedūru) ([362]).

(183) Kad pārbaude ir pabeigta, *ODNI CLPO* ar valsts iestādes starpniecību informē sūdzības iesniedzēju, ka "pārbaudē vai nu nav konstatēti nekādi pārkāpumi, vai arī *ODNI CLPO* ir pieņēmusi lēmumu, kurā pieprasa veikt atbilstošus korektīvus pasākumus" ([363]). Tas ļauj aizsargāt tādu darbību konfidencialitāti, kas veiktas nolūkā aizsargāt nacionālo drošību, un vienlaikus fiziskajām personām ir sniegts lēmums, kas apliecina, ka viņu sūdzība ir pienācīgi izmeklēta un izskatīta. Turklāt fiziskā persona šo lēmumu var apstrīdēt. Šajā nolūkā fiziskā persona tiks informēta par iespēju pārsūdzēt *CLPO* lēmumus *DPRC* (skatīt 184. un nākamos apsvērumus) un par to, ka gadījumā, ja tiks celta prasība Tiesā, tiks izvēlēts īpašs aizstāvis, kas aizstāvēs sūdzības iesniedzēja intereses ([364]).

([352]) *Section 3(c)(iv)*, IR Nr. 14086. Skatīt arī 1947. gada Nacionālās drošības likuma (50 U.S.C. §403-3d, *Section* 103D) par *CLPO* lomu *ODNI*.
([353]) 50 U.S.C § 3029 (b).
([354]) *Section 3(c)(iv)*, IR Nr. 14086.
([355]) *Section 3(c)(iii)*, IR 14086.
([356]) *Section 3(c)(iv)*, IR Nr. 14086.
([357]) *Section 3(c)(i)(B)(i)* un *(iii)*, IR Nr. 14086.
([358]) *Section 3(c)(i)*, IR Nr. 14086.
([359]) *Section 4(a)*, IR Nr. 14086.
([360]) *Section 3(c)(d)*, IR Nr. 14086.
([361]) *Section 3(c)(i)(F)-(G)*, IR Nr. 14086.
([362]) Sk. arī *Section 3(c)(i)(D)*, IR Nr. 14086.
([363]) *Section 3(c)(i)(E)(1)*, IR Nr. 14086.
([364]) *Sections 3(c)(i)(E)(2)-(3)*, IR Nr. 14086.

(184) Jebkurš sūdzības iesniedzējs, kā arī katra izlūkošanas kopienas struktūra var lūgt *ODNI CLPO* lēmuma pārskatīšanu Datu aizsardzības pārskatīšanas tiesā (*DPRC*). Šādi pārskatīšanas pieteikumi jāiesniedz 60 dienu laikā pēc tam, kad saņemts *ODNI CLPO* paziņojums par pārbaudes pabeigšanu, un tajos jāiekļauj visa informācija, ko attiecīgā fiziskā persona vēlas sniegt *DPRC* (piemēram, argumenti par tiesību jautājumiem vai tiesību piemērošanu lietas faktiem) ([365]). Savienības datu subjekti var atkal iesniegt pieteikumu kompetentajai DAI (sk. 177. apsvērumu).

(185) *DPRC* ir neatkarīga tiesa, ko izveidojis ģenerālprokurors, pamatojoties uz IR Nr. 14086 ([366]). Tās sastāvā ir vismaz seši tiesneši, kurus, apspriežoties ar *PCLOB*, tirdzniecības sekretāru un nacionālās izlūkošanas direktoru, uz četriem gadiem ieceļ ģenerālprokurors, ar iespēju šo pilnvaru termiņu pagarināt ([367]). Ģenerālprokurors, ieceļot tiesnešus, vadās pēc kritērijiem, kurus izmanto izpildvara, izvērtējot kandidātus uz federālo tiesu amatiem, kur liela nozīme tiek piešķirta iepriekšējai pieredzei tieslietu jomā ([368]). Turklāt tiesnešiem ir jābūt praktizējošiem juristiem (t. i., aktīviem advokatūras biedriem ar labu reputāciju un ar atbilstošu licenci praktizēt jurisprudences nozarē), un viņiem ir jābūt atbilstošai pieredzei privātuma un nacionālās drošības tiesību jomā. Ģenerālprokuroram ir jācenšas nodrošināt, lai vismaz pusei tiesnešu jebkurā laikā būtu iepriekšēja pieredze tiesneša amatā, un visiem tiesnešiem ir jābūt drošības pielaidēm, lai varētu piekļūt klasificētai nacionālās drošības informācijai ([369]).

(186) *DPRC* var iecelt tikai tādas fiziskas personas, kuras atbilst 185. apsvērumā minētajām kvalifikācijas prasībām un iecelšanas brīdī nav darbinieki izpildvaras struktūrās vai tādi nav bijuši iepriekšējo divu gadu laikā. Tāpat, kamēr tiesneši pilda amata pienākumus *DPRC*, viņi nedrīkst pildīt nekādus oficiālus pienākumus vai strādāt ASV valdībā (izņemot tiesneša amatu *DPRC*) ([370]).

(187) Tiesas spriešanas procesa neatkarība tiek nodrošināta ar vairākām garantijām. Jo īpaši izpildvarai (ģenerālprokuroram un izlūkošanas aģentūrām) ir aizliegts iejaukties vai neatbilstoši ietekmēt *DPRC* veikto pārskatīšanu ([371]). *DPRC* pašai ir noteikts pienākums lietas izskatīt objektīvi ([372]), un tā darbojas saskaņā ar savu reglamentu (kas pieņemts ar balsu vairākumu). Turklāt *DPRC* tiesnešus var atlaist no amata tikai ģenerālprokurors un tikai pamatotu iemeslu dēļ (t. i., pārkāpuma, ļaunprātīgas rīcības, drošības pārkāpuma, nolaidības vai nespējas pildīt amata pienākumus dēļ), pienācīgi ņēmis vērā federālajiem tiesnešiem piemērojamos standartus, kas paredzēti Noteikumos par procedūrām saistībā ar tiesnešu uzvedību un tiesnešu nespēju pildīt amata pienākumus (*Rules for Judicial-Conduct and Judicial-Disability Proceedings*) ([373]).

---

([365]) *Sections 201.6(a)-(b)*, ĢP noteikumi.

([366]) *Section 3(d)(i))* un ĢP noteikumi. Amerikas Savienoto Valstu Augstākā tiesa ir atzinusi iespēju ģenerālprokuroram izveidot neatkarīgas struktūras ar lēmumu pieņemšanas pilnvarām, tajā skaitā, lai lemtu atsevišķas lietas, sk. jo īpaši *United States ex rel. Accardi | Shaughnessy*, 347 U.S. 260 (1954) un *United States | Nixon*, 418 U.S. 683, 695 (1974). Atbilstību dažādām IR Nr. 14086 prasībām, piemēram, *DPRC* tiesnešu amatā iecelšanas un atbrīvošanas kritēriji un procedūras, jo īpaši uzrauga Tieslietu ministrijas ģenerālinspektors (skatīt arī 109. apsvērumu par ģenerālinspektora tiesību aktos paredzētajām pilnvarām).

([367]) *Section 3(d)(i)(A)*, IR Nr. 14086, un *Section 201.3(a)*, ĢP noteikumi.

([368]) *Section 201.3(b)*, ĢP noteikumi.

([369]) *Section 3(d)(i)(B)*, IR Nr. 14086.

([370]) *Section 3(d)(i)(A)*, IR Nr. 14086, un *Section 201.3(a)* un *(c)*, ĢP noteikumi. *DPRC* amatā ieceltās personas var piedalīties ārpustiesas darbībās, tajā skaitā nodarboties ar uzņēmējdarbību, finanšu darbībām, bezpeļņas līdzekļu vākšanu un fiduciārām darbībām, kā arī praktizēt jurisprudenci, ja vien šādas darbības netraucē objektīvi pildīt to amata pienākumus vai *DPRC* darbības rezultativitāti vai neatkarību (ĢP noteikumu 201.7. iedaļas c) punkts).

([371]) *Sections 3(d)(iii)-(iv)*, IR NR. 14086, un *Section 201.7(d)*, ĢP noteikumi.

([372]) *Section 3(d)(i)(D)*, IR Nr. 14086, un *Section 201.9*, ĢP noteikumi.

([373]) *Section 3(d)(iv)*, IR Nr. 14086, un *Section 201.7(d)*, ĢP noteikumi. Skatīt arī lietu *Bumap | ASV*, 252 U.S. 512, 515 (1920), kurā tika apstiprināts ASV tiesībās ilgstoši pastāvējis princips, ka pilnvaras atcelt no amata ir piesaistītas pilnvarām iecelt amatā (kā tas arī norādīts Tieslietu ministrijas Juridisko konsultāciju biroja publikācijā *The Constitutional Separation of Powers Between the President and Congress*, 20 Op. O.L.C. 124, 166 (1996)).

(188) Pieteikumus *DPRC* izskata trīs tiesnešu kolēģijas, tajā skaitā arī kolēģijas sastāva priekšsēdētājs, kam jārīkojas saskaņā ar ASV Tiesnešu rīcības kodeksu ([374]). Katrai kolēģijai palīdz īpašais aizstāvis ([375]), kuram ir pieejama visa ar lietu saistītā informācija, arī klasificēta informācija ([376]). Īpašā aizstāvja uzdevums ir nodrošināt, lai tiktu pārstāvētas sūdzības iesniedzēja intereses un lai *DPRC* kolēģija būtu labi informēta par visiem relevantajiem tiesību un faktu jautājumiem ([377]). Lai sīkāk informētu par savu nostāju attiecībā uz pārskatīšanas pieteikumu, ko fiziskas persona iesniegusi *DPRC*, īpašais aizstāvis rakstisku jautājumu veidā var pieprasīt informāciju no sūdzības iesniedzēja ([378]).

(189) *DPRC* izskata *ODNI CLPO* izdarītos konstatējumus (gan par to, vai ir noticis piemērojamo ASV tiesību aktu pārkāpums, gan par atbilstošiem korektīviem pasākumiem), pamatojoties vismaz uz *ODNI CLPO* veiktās izmeklēšanas rezultātiem, kā arī jebkādu informāciju un dokumentāciju, ko iesniedzis sūdzības iesniedzējs, īpašais aizstāvis vai izlūkošanas aģentūra ([379]). *DPRC* kolēģijai ir piekļuve visai informācijai, kas nepieciešama pārskatīšanas veikšanai un ko tā var iegūt ar *ODNI CLPO* starpniecību (kolēģija var, piemēram, lūgt *CLPO* papildināt tās lietu ar papildu informāciju vai faktiem, ja tas nepieciešams pārskatīšanas veikšanai) ([380]).

(190) Noslēdzot pārskatīšanu, *DPRC* var 1) lemt, ka nav pierādījumu, kas liecinātu, ka ir notikušas sakaru izlūkošanas darbības, kurās iesaistīti sūdzības iesniedzēja personas dati, 2) lemt, ka *ODNI CLPO* konstatējumi ir juridiski pareizi un pamatoti ar pietiekamiem pierādījumiem, vai, 3) ja *DPRC* nepiekrīt *ODNI CLPO* konstatējumiem (vai ir noticis piemērojamo ASV tiesību aktu pārkāpums, vai ir piemēroti atbilstoši korektīvi pasākumi), – izdot savus konstatējumus ([381]).

([374]) *Section 3(d)(i)(B)*, IR Nr. 14086, un *Section 201.7(a)-(c)*, ĢP noteikumi. Tieslietu ministrijas Privātuma un pilsonisko brīvību birojs (*OPCL*), kas ir atbildīgs par administratīvā atbalsta sniegšanu *DPRC* un īpašajiem aizstāvjiem (sk. ĢP noteikumu 201.5. iedaļu), saskaņā ar rotācijas principu izvēlas trīs cilvēku kolēģiju un cenšas nodrošināt, lai katrā kolēģijā būtu vismaz viens tiesnesis ar iepriekšēju pieredzi tiesneša amatā (ja nevienam no kolēģijas tiesnešiem nav šādas pieredzes, kolēģijas sastāva priekšsēdētājs ir tiesnesis, kuru *OPCL* izvēlas pirmo).

([375]) *Section 201.4*, ĢP noteikumi. Vismaz divus īpašos aizstāvjus uz diviem atjaunojamiem pilnvaru termiņiem ieceļ ģenerālprokurors, apspriežoties ar tirdzniecības sekretāru, nacionālās izlūkošanas direktoru un *PCLOB*. Īpašajiem aizstāvjiem jābūt atbilstošai pieredzei privātuma un nacionālās drošības tiesību jomā, pieredzējušiem juristiem, aktīviem advokatūras biedriem ar labu reputāciju un ar atbilstošu licenci praktizēt jurisprudences nozarē. Turklāt sākotnējās iecelšanas brīdī viņi nedrīkst būt bijuši darbinieki izpildvaras struktūrās iepriekšējos divus gadus. Katra pieteikuma izskatīšanai priekšsēdētājs izvēlas īpašo aizstāvi, kas palīdz kolēģijai; sk. ĢP noteikumu 201.8. iedaļas a) punktu.

([376]) *Section 201.8(c)* un *201.11*, ĢP noteikumi.

([377]) *Section 3(d)(i)(C)*, IR Nr. 14086, un *Section 201.8(e)* ĢP noteikumi. Īpašais aizstāvis nerīkojas kā sūdzības iesniedzēja pārstāvis un viņam ar sūdzības iesniedzēju nav advokāta un klienta attiecību.

([378]) Sk. *Section 201.8(d)(e)*, ĢP noteikumi. Šādus jautājumus vispirms izskata *OPCL*, apspriežoties ar attiecīgo izlūkošanas kopienas struktūru, lai identificētu un izslēgtu jebkādu klasificētu vai privileģētu, vai aizsargātu informāciju, pirms to pārsūta sūdzības iesniedzējam. Papildu informācija, ko īpašais aizstāvis saņēmis, atbildot uz šādiem jautājumiem, ir iekļauta dokumentācijā, ko tas iesniedzis *DPRC*.

([379]) *Section 3(d)(i)(D)*, IR Nr. 14086.

([380]) *Section 3(d)(iii)*, IR Nr. 14086, un *Section 201.9(b)* ĢP noteikumi.

([381]) *Section 3(d)(i)(E)*, IR Nr. 14086, un *Section 201.9(c)-(e)*, ĢP noteikumi. Saskaņā ar IR Nr. 14086 4. iedaļas a) punktā doto termina "atbilstoši korektīvi pasākumi" definīciju, lemjot par korektīviem pasākumiem pārkāpuma pilnīgai novēršanai, *DPRC* ir jāņem vērā "veidi, kā identificētajam pārkāpumam līdzvērtīgi gadījumi parasti tiek risināti", t. i., *DPRC*citustarp ņems vērā to, kādi korektīvi pasākumi iepriekš ir piemēroti līdzīgam atbilstības pārkāpumam, lai nodrošinātu, ka korektīvais pasākums ir efektīvs un samērīgs.

(191) Visās lietās *DPRC* pieņem rakstisku lēmumu ar balsu vairākumu. Ja pārskatīšanā tiek atklāts piemērojamo noteikumu pārkāpums, lēmumā tiks norādīti visi atbilstošie korektīvie pasākumi, tajā skaitā nelikumīgi savākto datu dzēšana, neatbilstoši veikto vaicājumu rezultātu dzēšana, piekļuves ierobežošana likumīgi vāktiem datiem tikai pienācīgi apmācītiem darbiniekiem vai tādu izlūkošanas ziņojumu atsaukšana, kuros iekļauti dati, kas iegūti bez likumīgas atļaujas vai kas tikuši izplatīti nelikumīgi ([382]). *DPRC* lēmums ir saistošs un galīgs attiecībā uz tai iesniegto sūdzību ([383]). Turklāt, ja pārbaudē atklāj kādas *FISC* pārraudzībā esošas iestādes pārkāpumu, *DPRC* ir jāiesniedz arī klasificēts ziņojums nacionālās drošības ģenerālprokurora vietniekam, kura pienākums savukārt ir ziņot par neatbilstību *FISC*, kas var veikt turpmākas izpildes panākšanas darbības (saskaņā ar 173. un 174. apsvērumā aprakstīto procedūru) ([384]).

(192) Katru *DPRC* kolēģijas lēmumu nosūta *ODNI CLPO* ([385]). Gadījumos, kad *DPRC* pārbaudi sāk pēc sūdzības iesniedzēja pieteikuma, sūdzības iesniedzējs ar valsts iestādes starpniecību tiek informēts, ka *DPRC* ir pabeigusi pārbaudi un ka "vai nu pārbaudē nav konstatēti nekādi pārbaudāmie pārkāpumi, vai arī *DPRC* ir pieņēmusi lēmumu, kurā prasa veikt atbilstošus korektīvus pasākumus." ([386]) *DoJ* Privātuma un pilsonisko brīvību birojs glabā visu *DPRC* pārbaudīto informāciju un visus pieņemtos lēmumus, kas ir pieejami izskatīšanai kā nesaistošs precedents nākamajām *DPRC* kolēģijām ([387]).

(193) *DoC* ir arī jāuztur reģistrs par visiem sūdzību iesniedzējiem ([388]). Lai uzlabotu pārredzamību, *DoC* vismaz reizi piecos gados jāsazinās ar attiecīgajām izlūkošanas aģentūrām, lai pārbaudītu, vai informācija, kas attiecas uz *DPRC* veikto pārbaudi, ir deklasificēta ([389]). Šādā gadījumā fiziskā persona tiks informēta par to, ka šāda informācija var būt pieejama saskaņā ar piemērojamiem tiesību aktiem (t. i., ka attiecīgā persona var pieprasīt piekļuvi informācijai saskaņā ar Informācijas brīvības likumu, sk. 199. apsvērumu).

(194) Visbeidzot, tiks regulāri un neatkarīgi izvērtēta šī tiesiskās aizsardzības mehānisma pareiza darbība. Konkrētāk, saskaņā ar IR Nr. 14086 tiesiskās aizsardzības mehānisma darbību katru gadu pārskata *PCLOB*, kas ir neatkarīga struktūra (sk. 110. apsvērumu) ([390]). Veicot šo pārskatīšanu, *PCLOB* citustarp izvērtēs, vai *ODNI CLPO* un *DPRC* sūdzības izskatījušas savlaicīgi, vai tās ir ieguvušas pilnīgu piekļuvi nepieciešamajai informācijai, vai pārskatīšanas procesā ir pienācīgi ņemtas vērā IR Nr. 14086 paredzētās būtiskās garantijas un vai izlūkošanas kopienas struktūras ir pilnībā izpildījušas *ODNI CLPO* un *DPRC* noteiktās prasības. *PCLOB* sagatavos ziņojumu par pārskatīšanas rezultātiem prezidentam, ģenerālprokuroram, nacionālās izlūkošanas direktoram, izlūkošanas aģentūru vadītājiem, *ODNI CLPO* un Kongresa izlūkošanas komitejām. Tiks publiskota arī šī ziņojuma neklasificēta versija, kas savukārt tiks izmantota Komisijas veiktajā šā lēmuma darbības periodiskajā pārskatīšanā. Ģenerālprokuroram, nacionālās izlūkošanas direktoram, *ODNI CLPO* un izlūkošanas aģentūru vadītājiem ir jāīsteno vai kā citādi jārisina visi šādos ziņojumos iekļautie ieteikumi. Turklāt *PCLOB* katru gadu sagatavos publisku apliecinājumu par to, vai tiesiskās aizsardzības mehānisms sūdzības apstrādā atbilstīgi IR Nr. 14086 prasībām.

([382]) *Section 4(a)*, IR Nr. 14086.

([383]) *Section 3(d)(ii)*, IR Nr. 14086, un *Section 201.9(g)*, ĢP noteikumi. Ņemot vērā to, ka *DPRC* lēmums ir galīgs un saistošs, to nevar atcelt neviena cita izpildvaras vai administratīvā iestāde/struktūra (ieskaitot ASV prezidentu). To apstiprina arī Augstākās tiesas judikatūra, kurā ir precizēts, ka piešķirot ģenerālprokuroram unikālas pilnvaras izpildvaras ietvaros izdot neatkarīgām struktūrām saistošus lēmumus, pašam ģenerālprokuroram ir iespēja diktēt šīs struktūras lēmumu jebkurā virzienā (sk. lietu *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954).

([384]) *Section 3(d)(i)(F)*, IR Nr. 14086, un *Section 201.9(i)*, ĢP noteikumi.

([385]) *Section 201.9(h)*, ĢP noteikumi.

([386]) *Section 3(d)(i)(H)*, IR Nr. 14086, un *Section 201.9(h)*, ĢP noteikumi. Attiecībā uz paziņojuma raksturu skatīt ĢP noteikumu 201.9. iedaļas h) punkta 3. apakšpunktu.

([387]) *Section 201.9(j)*, ĢP noteikumi.

([388]) *Section 3(d)(v)(A)*, IR Nr. 14086.

([389]) *Section 3(d)(v)*, IR Nr. 14086.

([390]) *Section 3(e)*, IR Nr. 14086. Sk. arī https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Papildus īpašajam tiesiskās aizsardzības mehānismam, kas izveidots saskaņā ar IR Nr. 14086, jebkurai personai (neatkarīgi no valstspiederības vai dzīvesvietas) ir pieejami arī tiesiskās aizsardzības līdzekļi parastajās ASV tiesās ([391]).

(196) Jo īpaši *FISA* un ar to saistītais likums paredz iespēju fiziskām personām celt civilprasību pret Amerikas Savienotajām Valstīm par finansiālu zaudējumu atlīdzināšanu, ja informācija par šīm personām ir apzināti izmantota vai izpausta nelikumīgi ([392]); iesniegt prasību pret ASV valdības amatpersonām kā privātpersonām par finansiālu zaudējumu atlīdzināšanu ([393]); un tiesā vai administratīvajā kārtībā ASV apstrīdēt novērošanas likumību (un pieprasīt noklusēt informāciju) gadījumā, ja ASV valdība plāno izmantot vai izpaust jebkādu informāciju, kas iegūta vai atvasināta no elektroniskās novērošanas, kura tikusi vērsta pret attiecīgo fizisko personu ([394]). Raugoties vispārīgāk, ja valdība plāno izmantot izlūkošanas operāciju laikā iegūto informāciju pret aizdomās turēto personu krimināllietā, konstitucionālās un normatīvās prasības ([395]) uzliek par pienākumu izpaust noteiktu informāciju, lai apsūdzētais varētu apstrīdēt valdības veiktās pierādījumu vākšanas un izmantošanas likumību.

(197) Turklāt pastāv vairāki īpaši veidi, kā vērsties tiesā pret valdības amatpersonām par nelikumīgu valdības piekļuvi personas datiem vai to nelikumīgu izmantošanu, arī šķietami nacionālās drošības nolūkos (t. i., Krāpniecības ar datora starpniecību un tā ļaunprātīgas izmantošanas likums (*Computer Fraud and Abuse Act*) ([396]); Elektroniskās saziņas privātuma likums (*Electronic Communications Privacy Act*) ([397]); un Likums par tiesībām un finanšu datu aizsardzību (*Right to Financial Privacy Act*) ([398])). Visas šīs tiesiskās darbības attiecas uz konkrētiem datiem, mērķiem un/vai piekļuves veidiem (piemēram, attālināta piekļuve datoram, izmantojot internetu), un tās ir iespējamas, ja radušies noteikti apstākļi (piemēram, tīša/ļaunprātīga rīcība, rīcība ārpus dienesta pienākumiem, nodarīts kaitējums).

(198) Vispārīgāku pārsūdzības iespēju nodrošina *APA* ([399]), kurā noteikts, ka "ikvienai personai, kam nodarīta juridiska netaisnība aģentūras darbības rezultātā vai ko nelabvēlīgi ietekmē vai neapmierina aģentūras darbība", ir tiesības vērsties tiesā ([400]). 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 tiesību aktiem" ([401]). Piemēram, federālā apelācijas tiesa 2015. gadā saistībā ar *APA* prasību lēma, ka ASV valdības veiktā telefonijas metadatu lielapjoma vākšana nebija atļauta saskaņā ar *FISA* 501. pantu ([402]).

([391]) Piekļuve šiem tiesiskās aizsardzības līdzekļiem ir atkarīga no tā, vai ir pierādīta attiecīgās personas "tiesībspēja". Šis kritērijs, kas attiecas uz jebkuru fizisku personu neatkarīgi no valstspiederības, izriet no ASV Konstitūcijas III panta prasības par "lietu vai strīdu". Kā atzinusi Augstākā tiesa, tas prasa, lai 1) fiziskā persona būtu cietusi "faktisku kaitējumu" (t. i., ir ticis radīts tāds kaitējums tiesiski aizsargātai ieinteresētai personai, kas ir konkrēts un precizēts, faktisks vai nenovēršams), 2) pastāvētu cēloņsakarība starp kaitējumu un rīcību, par kuru iesniegta prasība tiesā, un 3) būtu ticams, nevis tiktu pieņemts, ka labvēlīgs tiesas lēmums novērsīs kaitējumu (sk. *Lujan / Defenders of Wildlife*, 504 U.S. 555 (1992)).

([392]) 18 U.S.C. § 2712.

([393]) 50 U.S.C. § 1810.

([394]) 50 U.S.C. § 1806.

([395]) Sk. attiecīgi spriedumu lietā *Brady / Maryland*, 373 U.S. 83 (1963) un *Jencks Act*, 18 U.S.C. 3500. iedaļa.

([396]) 18 U.S.C. § 1030.

([397]) 18 U.S.C. §§ 2701-2712.

([398]) 12 U.S.C. § 3417.

([399]) 5 U.S.C. § 702.

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

([401]) 5 U.S.C. § 706(2)(A).

([402]) *ACLU / Clapper*, 785 F.3d 787 (2d Cir. 2015). Šajās lietās apstrīdētā telefonijas datu lielapjoma vākšanas programma 2015. gadā tika izbeigta ar *USA FREEDOM Act*.

(199) Visbeidzot, papildus 176.–198. apsvērumā minētajiem tiesiskās aizsardzības līdzekļiem ikvienai personai ir tiesības pieprasīt piekļuvi esošajiem federālo aģentūru dokumentiem saskaņā ar *FOIA*, arī tad, ja tie satur personas datus ([403]). Šādas piekļuves iegūšana var arī atvieglot tiesvedības uzsākšanu parastajās tiesās – arī lai pierādītu tiesībspēju. Aģentūras var neizpaust informāciju, uz kuru attiecas daži noteikti izņēmumi, tajā skaitā piekļuve klasificētai nacionālās drošības informācijai un informācijai par tiesībaizsardzības izmeklēšanu ([404]), bet sūdzību iesniedzējiem, kuri nav apmierināti ar atbildi, ir iespēja to apstrīdēt, prasot administratīvu un vēlāk arī tiesas veiktu (federālajās tiesās) pārskatīšanu ([405]).

(200) No iepriekš minētā izriet, ka tad, ja ASV tiesībaizsardzības un nacionālās drošības iestādes piekļūst personas datiem, uz kuriem attiecas šis lēmums, šādu piekļuvi reglamentē tiesiskais regulējums, kurā izklāstīti nosacījumi, saskaņā ar kuriem šāda piekļuve var notikt, un nodrošina, ka piekļuve un turpmāka datu izmantošana aprobežojas ar to, kas ir nepieciešams un samērīgs izvirzītajiem sabiedrības interešu mērķiem. Šīs garantijas var pieprasīt fiziskas personas, kurām ir faktiskas tiesības uz tiesisko aizsardzību.

## 4. **SECINĀJUMS**

(201) Komisija uzskata, ka Amerikas Savienotās Valstis ar ASV *DoC* izdotajiem DPR principiem personas datiem, kas saskaņā ar ES un ASV datu privātuma regulējumu no Savienības tiek nosūtīti sertificētām organizācijām Amerikas Savienotajās Valstīs, nodrošina tādu aizsardzības līmeni, kurš būtībā ir līdzvērtīgs Regulā (ES) 2016/679 garantētajam.

(202) Turklāt Komisija uzskata, ka DPR principu efektīvu piemērošanu garantē pārredzamības pienākumi un *DoC* veiktā DPR pārvaldība. Turklāt kopumā ASV tiesību aktos paredzētie pārraudzības mehānismi un tiesiskās aizsardzības līdzekļi ļauj praksē konstatēt datu aizsardzības noteikumu pārkāpumus un piemērot par tiem sodus un nodrošina datu subjektam tiesību aizsardzības līdzekļus, lai tas iegūtu piekļuvi ar to saistītiem personas datiem, un galu galā iespēju labot vai dzēst šādus datus.

(203) Visbeidzot, pamatojoties uz pieejamo informāciju par ASV tiesisko regulējumu, tajā skaitā VI un VII pielikumā iekļauto informāciju, Komisija uzskata, ka jebkāda ASV valsts iestāžu sabiedrības interesēs veikta iejaukšanās – jo īpaši krimināltiesību aizsardzības un nacionālās drošības nolūkos – to personu pamattiesībās, kuru personas dati tiek nosūtīti no Savienības uz ASV saskaņā ar ES un ASV datu privātuma regulējumu, būs tikai tāda, kas ir absolūti nepieciešama, lai sasniegtu attiecīgo likumīgo mērķi, un ka pret šādu iejaukšanos pastāv efektīva tiesiskā aizsardzība. Tāpēc, ņemot vērā iepriekš minētos konstatējumus, būtu jālemj, ka Amerikas Savienotās Valstis nodrošina pietiekamu aizsardzības līmeni Regulas (ES) 2016/679 45. panta nozīmē, interpretējot to saskaņā ar Eiropas Savienības Pamattiesību hartu, attiecībā uz personas datiem, kas no Eiropas Savienības nosūtīti organizācijām, kuras sertificētas saskaņā ar ES un ASV datu privātuma regulējumu.

(204) Ņemot vērā, ka IR Nr. 14086 noteiktie ierobežojumi, garantijas un tiesiskās aizsardzības mehānisms ir būtiski elementi ASV tiesiskajā regulējumā, uz kuru balstās Komisijas novērtējums, šā lēmuma pieņemšana jo īpaši balstās uz to, ka visas ASV izlūkošanas aģentūras pieņem atjauninātu politiku un procedūras IR Nr. 14086 īstenošanai, un Savienība tiek atzīta par kvalificētu organizāciju tiesiskās aizsardzības mehānisma vajadzībām – tas ir noticis attiecīgi 2023. gada 3. jūlijā (sk. 126. apsvērumu) un 2023. gada 30. jūnijā (sk. 176. apsvērumu).

([403]) 5 U.S.C. § 552. Līdzīgi likumi pastāv štatu līmenī.

([404]) Tādā gadījumā persona parasti saņem tikai standarta atbildi, ar kuru aģentūra atsakās apstiprināt vai noliegt jebkādu ierakstu esību. Sk. *ACLU / CIA*, 710 F.3d 422 (D.C. Cir. 2014). Klasificēšanas kritēriji un ilgums ir noteikts izpildrīkojumā Nr. 13526, kas nosaka, ka deklasificēšanai parasti tiek noteikts konkrēts datums vai notikums, pamatojoties uz to, cik ilgi informācija ir uzskatāma par nacionālai drošībai sensitīvu, un pēc tam tā ir automātiski deklasificējama (sk. IR Nr. 13526 1.5. iedaļu).

([405]) Tiesa pieņem *de novo* nolēmums par to, vai informācijas neizpaušana ir likumīga, un tā var likt valdībai nodrošināt piekļuvi datiem (5 U.S.C. § 552(a)(4)(B)).

## 5. ŠĀ LĒMUMA SEKAS UN DATU AIZSARDZĪBAS IESTĀŽU RĪCĪBA

(205) Dalībvalstīm un to struktūrām ir pienākums veikt nepieciešamos pasākumus, lai izpildītu Savienības iestāžu aktus, jo tie 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 nelikumību.

(206) Tādējādi lēmums par aizsardzības līmeņa pietiekamību, ko Komisija pieņēmusi saskaņā ar Regulas (ES) 2016/679 45. panta 3. punktu, ir saistošs visām dalībvalstu struktūrām, kurām tas adresēts, arī to neatkarīgajām uzraudzības iestādēm. Konkrētāk, pārzinis vai apstrādātājs Savienībā var nosūtīt datus sertificētām organizācijām Amerikas Savienotajās Valstīs bez jebkādas turpmākas atļaujas saņemšanas.

(207) Vienlaikus būtu jāatgādina, ka saskaņā ar Regulas (ES) 2016/679 58. panta 5. punktu un kā Tiesa paskaidrojusi spriedumā *Schrems* lietā ([406]), ja valsts datu aizsardzības iestāde, arī pēc sūdzības saņemšanas, apšauba Komisijas lēmuma par aizsardzības līmeņa pietiekamību atbilstību fiziskas personas pamattiesībām uz privātumu un datu aizsardzību, tai valsts tiesību aktos ir jānodrošina tiesiskās aizsardzības līdzeklis, kas ļauj celt šādus iebildumus valsts tiesā, kurai var būt pienākums lūgt Tiesai sniegt prejudiciālu nolēmumu ([407]).

## 6. ŠĀ LĒMUMA PĀRRAUDZĪBA UN PĀRSKATĪŠANA

(208) Saskaņā ar Eiropas Savienības Tiesas judikatūru ([408]) un kā atzīts Regulas (ES) 2016/679 45. panta 4. punktā, Komisijai pēc lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas būtu pastāvīgi jāuzrauga norises attiecīgajā trešā valstī, lai novērtētu, vai trešā valsts joprojām nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni. Vajadzība pēc šāda vērtējuma katrā ziņā rodas, ja Komisija saņem informāciju, kura rada šaubas par to.

(209) Tāpēc Komisijai būtu pastāvīgi jāuzrauga situācija Amerikas Savienotajās Valstīs attiecībā uz personas datu apstrādes tiesisko regulējumu un faktisko praksi, kas novērtēta šajā lēmumā. Lai sekmētu šo procesu, ASV iestādēm būtu bez kavēšanās jāinformē Komisija par būtiskām ASV tiesiskās kārtības izmaiņām, kas ietekmē tiesisko regulējumu, uz kuru attiecas šis lēmums, kā arī par šajā lēmumā novērtētās personas datu apstrādes prakses maiņu gan attiecībā uz sertificētu organizāciju veiktu personas datu apstrādi Amerikas Savienotajās Valstīs, gan attiecībā uz ierobežojumiem un garantijām, ko piemēro publiskām iestādēm nodrošinātai piekļuvei personas datiem.

(210) Turklāt, lai Komisija varētu efektīvi pildīt savu uzraudzības funkciju, dalībvalstīm būtu jāinformē Komisija par visām būtiskajām darbībām, ko veikušas valstu datu aizsardzības iestādes, jo īpaši attiecībā uz Savienības datu subjektu vaicājumiem un sūdzībām par personas datu nosūtīšanu no Savienības uz sertificētām organizācijām Amerikas Savienotajās Valstīs. Komisiju vajadzētu informēt arī par visām pazīmēm, kas liecina, ka darbības, kuras veic ASV publiskās iestādes, kas atbild par noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai kriminālvajāšanu vai par nacionālo drošību, tajā skaitā jebkādas pārraudzības struktūras, nenodrošina vajadzīgo aizsardzības līmeni.

([406]) Spriedums lietā *Schrems*, 65. punkts.

([407]) Spriedums lietā *Schrems*, 65. punkts: "Valsts likumdevēja ziņā ir paredzēt tiesiskās aizsardzības līdzekļus, kas valsts uzraudzības iestādei ļauj valstu tiesās izvirzīt iebildes, ko tā uzskata par pamatotām, lai šīs tiesas – ja arī tās piekrīt šīs iestādes šaubām par Komisijas lēmuma spēkā esību – iesniegtu lūgumu sniegt prejudiciālu nolēmumu šī lēmuma spēkā esības izvērtēšanas nolūkos."

([408]) Spriedums lietā *Schrems*, 76. punkts.

(211) Piemērojot Regulas (ES) 2016/679 45. panta 3. punktu ([409]), Komisijai pēc šā lēmuma pieņemšanas būtu periodiski jāpārskata, vai konstatējumi par Amerikas Savienoto Valstu nodrošinātā aizsardzības līmeņa pietiekamību saskaņā ar ES un ASV DPR joprojām ir faktiski un juridiski pamatoti. Tā kā IR Nr. 14086 un ĢP noteikumos jo īpaši prasīts izveidot jaunus mehānismus un īstenot jaunas garantijas, šis lēmums pirmo reizi būtu jāpārskata viena gada laikā pēc tā stāšanās spēkā, lai pārbaudītu, vai visi attiecīgie elementi ir pilnībā īstenoti un rezultatīvi praksē. Pēc pirmās pārskatīšanas un atkarībā no tās rezultātiem Komisija ciešā sadarbībā ar komiteju, kas izveidota saskaņā ar Regulas (ES) 2016/679 93. panta 1. punktu, un Eiropas Datu aizsardzības kolēģiju pieņems lēmumu par turpmākas pārskatīšanas periodiskumu ([410]).

(212) Lai veiktu pārskatīšanu, Komisijai būtu jātiekas ar *DoC*, *FTC* un *DoT*, vajadzības gadījumā kopā ar citām ministrijām un aģentūrām, kas iesaistītas ES un ASV DPR īstenošanā, kā arī jautājumos, kas attiecas uz valdības piekļuvi datiem – ar *DoJ*, *ODNI* (tajā skaitā *CLPO*), citu izlūkošanas kopienas struktūru un *DPRC* pārstāvjiem, kā arī īpašajiem aizstāvjiem. Būtu jānodrošina iespēja arī Eiropas Datu aizsardzības kolēģijas pārstāvjiem apmeklēt šādas sanāksmes.

(213) Pārskatīšanās būtu jāiekļauj visi šā lēmuma darbības aspekti attiecībā uz personas datu apstrādi ASV, un jo īpaši tādi aspekti kā DPR principu piemērošana un īstenošana, īpašu uzmanību pievēršot pieejamiem aizsardzības pasākumiem datu tālākas nosūtīšanas gadījumā; relevantie jaunumi judikatūrā; individuālo tiesību izmantošanas rezultativitāte; DPR principu ievērošanas uzraudzība un izpilde; ierobežojumi un aizsardzības pasākumi attiecībā uz valdības piekļuvi, jo īpaši ar IR Nr. 14086 ieviesto aizsardzības pasākumu īstenošanai un piemērošanai, arī izlūkošanas aģentūru izstrādātās politikas un procedūru ietvaros; IR Nr. 14086, *FISA* 702. panta un IR Nr. 12333 mijiedarbība; pārraudzības mehānismu un tiesiskās aizsardzības līdzekļu efektivitāte (ieskaitot ar IR Nr. 14086 izveidotos jaunos tiesiskās aizsardzības mehānismus). Saistībā ar šādām pārskatīšanām uzmanība tiks pievērsta arī sadarbībai starp DAI un Amerikas Savienoto Valstu kompetentajām iestādēm, tostarp norādījumu un citu interpretējošu instrumentu izstrādei par DPR principu piemērošanu, kā arī citiem satvara darbības aspektiem.

(214) Pamatojoties uz pārskatīšanu, Komisijai būtu jāsagatavo publisks ziņojums, kas jāiesniedz Eiropas Parlamentam un Padomei.

## 7. ŠĀ LĒMUMA APTURĒŠANA, ATCELŠANA VAI GROZĪŠANA

(215) Ja pieejamā informācija, jo īpaši informācija, kas iegūta, uzraugot šo lēmumu, vai informācija, ko sniedz ASV vai dalībvalstu iestādes, atklāj, ka aizsardzības līmenis, kas nodrošināts saskaņā ar šo lēmumu nosūtītajiem datiem, iespējams, vairs nav pietiekams, Komisijai par to būtu ātri jāinformē ASV kompetentās iestādes un jāpieprasa, lai noteiktā un saprātīgā termiņā tiktu veikti attiecīgi pasākumi.

(216) Ja līdz noteiktā termiņa beigām ASV kompetentās iestādes nav veikušas minētos pasākumus vai kā citādi apmierinoši neparāda, ka šā lēmuma pamatā joprojām ir pietiekams aizsardzības līmenis, Komisija uzsāks Regulas (ES) 2016/679 93. panta 2. punktā minēto procedūru, lai daļēji vai pilnībā apturētu vai atceltu šo lēmumu.

(217) Alternatīvi Komisija uzsāks minēto procedūru, lai grozītu šo lēmumu, jo īpaši piemērojot papildu nosacījumus datu nosūtīšanai vai ierobežojot aizsardzības līmeņa pietiekamības konstatējuma darbības jomu tikai attiecībā uz tādu datu nosūtīšanu, kam joprojām tiek nodrošināts pietiekams aizsardzības līmenis.

([409]) Saskaņā ar Regulas (ES) 2016/679 45. panta 3. punktu "[ī]stenošanas aktā paredz periodiskas [..] pārskatīšanas mehānismu, kurā ņem vērā visas attiecīgās norises trešajā valstī vai starptautiskajā organizācijā".

([410]) Regulas (ES) 2016/679 45. panta 3. punkts paredz, ka periodiska pārskatīšana jāveic vismaz reizi četros gados. Sk. arī Eiropas Datu aizsardzības kolēģija, Pietiekamības atsauces, WP 254 rev. 01.

(218) Konkrēti, Komisijai būtu jāuzsāk apturēšanas vai atcelšanas procedūra, ja:

(a) ir norādes, ka organizācijas, kas ir saņēmušas personas datus no Savienības saskaņā ar šo lēmumu, neievēro DPR principus un ka kompetentās pārraudzības un izpildes struktūras nav rezultatīvi vērsušās pret šādu neatbilstību;

(b) ir norādes, ka ASV iestādes neievēro piemērojamos nosacījumus un ierobežojumus attiecībā uz ASV publisko iestāžu piekļuvi personas datiem, kas nosūtīti saskaņā ar ES un ASV DPR, tiesībaizsardzības un nacionālās drošības nolūkos, vai

(c) attiecīgās struktūras (arī *ODNI CLPO* un/vai *DPRC*) rezultatīvi nerisina Savienības datu subjektu sūdzības.

(219) Komisijai būtu jāapsver šā lēmuma grozīšanas, apturēšanas vai atcelšanas procedūras sākšana arī gadījumā, ja ASV kompetentās iestādes nesniedz informāciju vai paskaidrojumus, kas nepieciešami, lai novērtētu no Savienības uz Amerikas Savienotajām Valstīm nosūtīto personas datu aizsardzības līmeni vai atbilstību šim lēmumam. Šajā saistībā Komisijai būtu jāņem vērā tas, kādā apmērā attiecīgo informāciju var iegūt no citiem avotiem.

(220) Pienācīgi pamatotu nenovēršamu steidzamu iemeslu dēļ, piemēram, ja IR Nr. 14086 vai ĢP noteikumi tiktu grozīti tā, ka tiktu apdraudēts šajā lēmumā aprakstītais aizsardzības līmenis, vai ja tiek atsaukts ģenerālprokurora izdotais atzinums par Savienību kā kvalificētu organizāciju tiesiskās aizsardzības mehānisma kontekstā, Komisija izmantos iespēju saskaņā ar Regulas (ES) 2016/679 93. panta 3. punktā minēto procedūru pieņemt nekavējoties piemērojamus īstenošanas aktus, ar kuriem aptur, atceļ vai groza šo lēmumu.

## 8. **NOSLĒGUMA APSVĒRUMI**

(221) Eiropas Datu aizsardzības kolēģija ir publiskojusi savu atzinumu ([411]), un tas tika ņemts vērā, sagatavojot šo lēmumu.

(222) Eiropas Parlaments ir pieņēmis rezolūciju par ES un ASV datu privātuma regulējuma sniegtās aizsardzības pietiekamību ([412]).

(223) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Regulas (ES) 2016/679 93. panta 1. punktu,

IR PIEŅĒMUSI ŠO LĒMUMU.

*1. pants*

Regulas (ES) 2016/679 45. panta nolūkā Amerikas Savienotās Valstis nodrošina pietiekamu aizsardzības līmeni personas datiem, kas no Savienības nosūtīti Amerikas Savienoto Valstu organizācijām, kuras ir iekļautas datu privātuma regulējuma sarakstā, ko saskaņā ar I pielikuma I.3. iedaļu uztur un publisko ASV Tirdzniecības ministrija.

*2. pants*

Lai aizsargātu fiziskas personas attiecībā uz viņu personas datu apstrādi, ikreiz, kad kompetentās iestādes dalībvalstīs īsteno savas pilnvaras atbilstoši Regulas (ES) 2016/679 58. pantam attiecībā uz datu nosūtīšanu, kas minēta šā lēmuma 1. pantā, attiecīgā dalībvalsts nekavējoties informē Komisiju.

([411]) 2023. gada 28. februāra atzinums 5/2023 par Eiropas Komisijas īstenošanas lēmuma projektu par personas datu pienācīgu aizsardzību saskaņā ar ES un ASV datu privātuma regulējumu.

([412]) Eiropas Parlamenta 2023. gada 11. maija rezolūcija par ES un ASV datu privātuma regulējuma sniegtās aizsardzības pietiekamību (2023/2501(RSP)).

*3. pants*

1. Komisija pastāvīgi uzrauga to, kā tiek piemērots tiesiskais regulējums, kas ir šā lēmuma priekšmets, tajā skaitā nosacījumi, ar kādiem tiek veikta datu tālāka nosūtīšana, tiek īstenotas individuālās tiesības un ASV publiskajām iestādēm ir piekļuve datiem, kuri nosūtīti, balstoties uz šo lēmumu, lai novērtētu, vai Amerikas Savienotās Valstis turpina nodrošināt pietiekamu aizsardzības līmeni, kā tas minēts 1. pantā.

2. Dalībvalstis un Komisija informē cita citu par gadījumiem, kad tiek konstatēts, ka Amerikas Savienoto Valstu struktūras ar likumā noteiktām pilnvarām nodrošināt atbilstību I pielikumā izklāstītajiem DPR principiem nenodrošina iedarbīgus atklāšanas un uzraudzības mehānismus, kas ļauj praksē konstatēt I pielikumā izklāstīto DPR principu pārkāpumus un piemērot par tiem sodus.

3. Dalībvalstis un Komisija informē cita citu par visām pazīmēm, kas liecina par to, ka ASV publiskās iestādes, kuras atbild par nacionālās drošības, tiesībaizsardzības vai citu sabiedrības interešu īstenošanu, fizisku personu tiesībās attiecībā uz to personas datu aizsardzību iejaucas vairāk, nekā ir nepieciešami un samērīgi, un/vai ka pret šādu iejaukšanos nav efektīvas tiesiskās aizsardzības.

4. Vienu gadu pēc šā lēmuma paziņošanas dalībvalstīm un pēc tam periodiski (par periodu lemj ciešā saziņā ar komiteju, kas izveidota saskaņā ar Regulas (ES) 2016/679 93. panta 1. punktu, un Eiropas Datu aizsardzības kolēģiju) Komisija izvērtē 1. panta 1. punktā minēto konstatējumu, pamatojoties uz visu pieejamo informāciju, tajā skaitā informāciju, kas iegūta, veicot pārskatīšanu kopā ar Amerikas Savienoto Valstu kompetentajām iestādēm.

5. Ja Komisija ir konstatējusi pazīmes, ka vairs netiek nodrošināts pietiekams aizsardzības līmenis, Komisija informē ASV kompetentās iestādes. Vajadzības gadījumā Komisija lems šo lēmumu apturēt, grozīt vai atcelt vai ierobežot tā piemērošanas jomu saskaņā ar Regulas (ES) 2016/679 45. panta 5. punktu. Komisija var arī pieņemt šādu lēmumu, ja ASV valdības nesadarbošanās liedz Komisijai noteikt, vai Amerikas Savienotās Valstis turpina nodrošināt pietiekamu aizsardzības līmeni.

*4. pants*

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2023. gada 10. jūlijā

*Komisijas vārdā –*
*Komisijas loceklis*
Didier REYNDERS

***I PIELIKUMS***

# ES UN ASV DATU PRIVĀTUMA REGULĒJUMA PRINCIPI, KO IZDEVUSI ASV TIRDZNIECĪBAS MINISTRIJA

## I. PĀRSKATS

1. Lai gan Amerikas Savienotās Valstis un Eiropas Savienību ("ES") vieno kopīga apņemšanās uzlabot privātuma aizsardzību, tiesiskumu un atzīt transatlantisko datu plūsmu nozīmi mūsu attiecīgajiem pilsoņiem, ekonomikai un sabiedrībai, Amerikas Savienotajām Valstīm ir atšķirīga pieeja privātuma aizsardzībai nekā ES. Amerikas Savienotās Valstis izmanto nozaru pieeju, kuras pamatā ir gan ārēji, gan iekšēji normatīvie akti. ASV Tirdzniecības ministrija ("ministrija") izdod ES un ASV datu privātuma regulējuma principus, tajā skaitā papildprincipus (kopā – "DPR principi") un DPR principu I pielikumu ("I pielikums"), pamatojoties uz tai likumā noteiktajām pilnvarām veicināt, sekmēt un attīstīt starptautisko tirdzniecību (15 U.S.C. § 1512). DPR principi tika izstrādāti, apspriežoties ar Eiropas Komisiju ("Komisija"), nozares uzņēmumiem un citām ieinteresētajām personām, lai veicinātu tirdzniecību starp Amerikas Savienotajām Valstīm un ES. DPR principi, kas ir ES un ASV datu privātuma regulējuma ("ES un ASV DPR") būtiska daļa, nodrošina organizācijām Amerikas Savienotajās Valstīs uzticamu mehānismu personas datu nosūtīšanai no ES 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 tiek nosūtīti uz valstīm ārpus ES. DPR principus ir paredzēts izmantot tikai tādām organizācijām Amerikas Savienotajās Valstīs, kas ir tiesīgas saņemt personas datus no ES un izpilda ES un ASV DPR nosacījumus, un uz kurām līdz ar to attiecas Eiropas Komisijas lēmums par aizsardzības līmeņa pietiekamību ([1]). DPR principi neietekmē Regulas (ES) 2016/679 ("Vispārīgā datu aizsardzības regula" jeb "VDAR") ([2]), kas attiecas uz personas datu apstrādi ES dalībvalstīs, piemērošanu. DPR principi arī neierobežo privātuma saistības, kas ir citādi paredzētas ASV tiesību aktos.

2. Lai varētu nosūtīt personas datus no ES, pamatojoties uz ES un ASV DPR, organizācijai ir pašai jāapliecina ministrijai (vai tās pārstāvim), ka ievēro DPR principus. Lai gan organizāciju lēmumi par pievienošanos ES un ASV DPR ir pilnībā brīvprātīgi, to faktiska ievērošana ir obligāta – organizācijām, kuras ir veikušas pašsertifikāciju ministrijai un publiski paziņojušas par apņemšanos ievērot DPR principus, tie ir pilnībā jāievēro. Lai iesaistītos ES un ASV DPR, organizācijai a) jāpakļaujas Federālās tirdzniecības komisijas ("*FTC*"), ASV Satiksmes ministrijas ("*DoT*") vai citas tādas oficiālas iestādes izmeklēšanas un tiesībaizsardzības pilnvarām, kas rezultatīvi nodrošinās atbilstību, DPR principiem *(citas ES atzītas ASV oficiālās iestādes turpmāk varētu tikt uzskaitītas atsevišķā pielikumā)*; b) publiski jāpauž apņemšanās ievērot DPR principus: c) jāpublisko sava privātuma politika atbilstīgi šiem DPR principiem; un d) tie pilnībā jāīsteno ([3]). Ja organizācija neievēro noteikumus, *FTC* var pieprasīt to izpildi 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); tāpat to var pieprasīt *DoT* saskaņā ar 49 U.S.C. § 41712, kas aizliedz pārvadātājam vai biļešu pārdevējam iesaistīties negodīgā vai maldinošā praksē gaisa pārvadājumu nozarē vai gaisa pārvadājumu pakalpojumu pārdošanas jomā, vai saskaņā ar citiem tiesību aktiem vai noteikumiem, kas aizliedz šādu rīcību.

([1]) Ja Komisijas lēmums par ES un ASV DPR nodrošinātā aizsardzības līmeņa pietiekamību attieksies arī uz Islandi, Lihtenšteinu un Norvēģiju, ES un ASV DPR attieksies gan uz ES, gan uz šīm trim valstīm. Attiecīgi atsauces uz ES un tās dalībvalstīm būs lasāmas, ietverot arī Islandi, Lihtenšteinu un Norvēģiju.

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) 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).

([3]) Jēdziens "ES un ASV privātuma vairoga regulējuma principi" ir grozīts uz "ES un ASV datu privātuma regulējuma principi". (Sk. papildprincipu par pašsertifikāciju).

3. Ministrija uzturēs un darīs sabiedrībai pieejamu to ASV organizāciju autoritatīvu sarakstu, kuras veikušas pašsertifikāciju ministrijai un paziņojušas par apņemšanos ievērot DPR principus ("datu privātuma regulējuma saraksts"). Ar ES un ASV DPR saistītās priekšrocības tiek saņemtas no dienas, kad ministrija iekļauj organizāciju datu privātuma regulējuma sarakstā. Ministrija svītros no datu privātuma regulējuma saraksta tās organizācijas, kas brīvprātīgi izstājas no ES un ASV DPR vai nav pabeigušas ikgadējo atkārtotas sertifikācijas procesu ministrijā; šīm organizācijām ir vai nu jāturpina piemērot DPR principus personas datiem, ko tās ir saņēmušas saskaņā ar ES un ASV DPR, un katru gadu jāapliecina ministrijai sava apņemšanās to darīt (t. i., tik ilgi, kamēr tās glabā šādu informāciju), vai jānodrošina "pietiekama" informācijas aizsardzība ar citiem atļautiem līdzekļiem (piemēram, izmantojot līgumu, kas pilnībā atspoguļo attiecīgo Komisijas pieņemto līguma standartklauzulu prasības), vai arī attiecīgā informācija jāatgriež vai jādzēš. Turklāt ministrija svītros no datu privātuma regulējuma saraksta arī tās organizācijas, kuras pastāvīgi neievēro DPR principus; šīm organizācijām ir jāatgriež vai jādzēš personas dati, ko tās ir saņēmušas ES un ASV DPR ietvaros. Ja organizācija no datu privātuma regulējuma saraksta ir svītrota, tā vairs nav tiesīga izmantot Komisijas lēmumu par aizsardzības līmeņa pietiekamību, lai saņemtu personas datus no ES.

4. Ministrija arī uzturēs un darīs sabiedrībai pieejamu to ASV organizāciju autoritatīvu reģistru, kuras iepriekš ir apliecinājušas ministrijai apņemšanos ievērot DPR principus, taču ir svītrotas no datu privātuma regulējuma saraksta. Ministrija sagatavos skaidru brīdinājumu, ka šīs organizācijas nav ES un ASV DPR dalībnieces; ka pēc svītrošanas no datu privātuma regulējuma saraksta šādas organizācijas nevar apgalvot, ka tās atbilst ES un ASV DPR nosacījumiem, un tām nevajadzētu izplatīt paziņojumus vai īstenot maldinošu praksi, kas norādītu uz to dalību ES un ASV DPR; un ka uz šādām organizācijām vairs nevar attiecināt Komisijas lēmumu par aizsardzības līmeņa pietiekamību,, kas tām ļautu saņemt personas datus no ES. Attiecībā uz organizāciju, kas pēc tās svītrošanas no datu privātuma regulējuma saraksta turpina apgalvot, ka piedalās ES un ASV DPR, vai nāk klajā ar citādu ar ES un ASV DPR saistītu sagrozītu informāciju, FTC, Transporta ministrija vai citas izpildes iestādes var īstenot izpildes panākšanas darbību.

5. Šo DPR principu ievērošanu var ierobežot: a) ciktāl tas vajadzīgs, lai izpildītu tiesas rīkojumu vai ievērotu sabiedrības intereses, tiesībaizsardzības vai nacionālās drošības prasības, arī tad, ja likums vai valdības noteikumi paredz pretrunīgus pienākumus; b) ar likumu, tiesas rīkojumu vai valdības noteikumiem, kas paredz skaidru atļauju, ar noteikumu, ka, izmantojot šādu atļauju, organizācija var pierādīt, ka DPR principus tā neievēro vienīgi tiktāl, ciktāl šāda neievērošana ir vajadzīga, lai ievērotu sevišķi svarīgas likumīgās intereses, kuras izriet no šādas atļaujas, vai c) ja VDAR pieļauj izņēmumus vai atkāpes saskaņā ar VDAR ar nosacījumu, ka šādus izņēmumus vai atkāpes piemēro līdzvērtīgās situācijās. Šajā kontekstā ASV tiesību aktos privātuma un pilsonisko brīvību aizsardzības pasākumi ietver tos, kas paredzēti Izpildrīkojumā Nr. 14086 ([4]) saskaņā ar tajā izklāstītajiem nosacījumiem (arī prasībām par nepieciešamību un samērīgumu). Saskaņā ar mērķi uzlabot privātuma aizsardzību organizācijām jācenšas šos principus īstenot pilnībā un pārredzamā veidā, tajā skaitā cenšoties savā privātuma politikā norādīt, vai tiks piemēroti ar b) punktu atļautie DPR principu izņēmumi. Tā paša iemesla dēļ organizācijām, ja iespējams, jāizvēlas labāka aizsardzība, ja izvēli atļauj DPR principi un/vai ASV tiesību akti.

6. Organizācijām ir pienākums piemērot DPR principus visiem personas datiem, kas nosūtīti, pamatojoties uz ES un ASV DPR, pēc tam, kad tās iesaistījušās ES un ASV DPR. Organizācijai, kas vēlas ES un ASV DPR priekšrocības attiecināt arī uz cilvēkresursu personas datiem, kas no ES nosūtīti izmantošanai saistībā ar darba attiecībām, tas jānorāda ministrijai, kad tā veic pašsertifikāciju, un tai jāievēro papildprincipā par pašsertifikāciju izvirzītās prasības.

([4]) 2022. gada 7. oktobra Izpildrīkojums "Drošības pasākumu uzlabošana Amerikas Savienoto Valstu sakaru izlūkošanas darbībām" (*Enhancing Safeguards for United States Signals Intelligence Activities*).

7. Jautājumus par to, kā organizācijas, kas iesaistījušās ES un ASV DPR, interpretē un ievēro DPR 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 DPR principu noteikumus piemēro atbilstoši situācijai.

8. Definīcijas:

   a. "personas dati" ir tādi dati par identificētu vai identificējamu fizisku personu, uz kuriem attiecas VDAR un kurus Amerikas Savienoto Valstu organizācija ir saņēmusi no ES 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. DPR principi un to I pielikums stājas spēkā dienā, kad stājas spēkā Eiropas Komisijas lēmums par aizsardzības līmeņa pietiekamību.

## II. DPR PRINCIPI

### 1. PAZIŅOŠANA

a. Organizācijai jāinformē fiziskas personas par:

   i. savu dalību ES un ASV DPR un jānorāda saite uz datu privātuma regulējuma sarakstu vai tā tīmekļa adrese;

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

   iii. tās apņemšanos piemērot DPR principus visiem personas datiem, kas no ES saņemti, pamatojoties uz ES un ASV DPR;

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

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

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

   vii. fizisku personu tiesībām piekļūt saviem personas datiem;

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

   ix. neatkarīgo strīdu izšķiršanas struktūru, kas izraudzīta sūdzību izskatīšanai un atbilstošas tiesību aizsardzības nodrošināšanai bez maksas fiziskai personai, un to, vai šī struktūra ir: 1) DAI izveidota kolēģija; 2) strīdu alternatīvas izšķiršanas pakalpojumu sniedzējs, kas iedibināts ES; vai 3) strīdu alternatīvas izšķiršanas pakalpojumu sniedzējs, kas iedibināts Amerikas Savienotajās Valstīs;

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

   xi. fizisku personu iespēju konkrētos apstākļos ierosināt saistošu šķīrējtiesas procesu ([5]);

   xii. prasību izpaust personas datus, atbildot uz likumīgiem publisko iestāžu pieprasījumiem, tajā skaitā ievērot ar nacionāli drošību vai tiesībaizsardzību saistītas prasības, un

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

([5]) Sk., piemēram, tiesību aizsardzības, izpildes un atbildības principa c) iedaļu.

b. Šis paziņojums jāsniedz skaidrā un viegli saprotamā veidā, kad personas pirmo reizi tiek lūgtas sniegt personas datus organizācijai vai cik drīz vien iespējams pēc tam, bet jebkurā gadījumā pirms organizācija šādu informāciju izmanto citiem nolūkiem, izņemot tos, kuriem nosūtītāja organizācija to sākotnēji ievākusi vai apstrādājusi, vai to pirmo reizi izpaudusi trešai personai.

2. **IZVĒLE**

a. Organizācijai jāpiedāvā fiziskām personām iespēja izvēlēties (t. i, atteikties), vai viņu personas datus i) izpaudīs trešajai personai vai ii) izmantos nolūkam, kas būtiski atšķiras no nolūka(-iem), kuram(-iem) to sākotnēji vāca vai fiziskās personas pēc tam atļāva izmantot. Lai fiziskās personas varētu izdarīt izvēli, tām jānodrošina 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., personas datus, kas ietver medicīniskos datus vai datus par veselības stāvokli, norāda fiziskas personas rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībā, vai ietver datus par fiziskas personas seksuālo dzīvi) organizācijām ir jāsaņem skaidri izteikta fizisku personu piekrišana, ja šādu informāciju i) izpaudīs trešajai personai vai ii) izmantos citam nolūkam, kas nav tas, kuram tā sākotnēji vākta vai kuram fiziskas personas, izdarot attiecīgu izvēli, pēc tam atļāvuši to izmantot. Turklāt organizācijai jebkādi personas dati, kas ir saņemta no trešās personas, būtu jāapstrādā kā sensitīva informācija, ja trešā persona to identificē un apstrādā kā sensitīvu.

3. **ATBILDĪBA PAR TĀLĀKU NOSŪTĪŠANU**

a. Lai personas datus nosūtītu trešai personai, kas darbojas kā pārzinis, organizācijām jāievēro paziņošanas un izvēles princips. Tām ar pārzini, kas ir trešā persona, ir arī jānoslēdz līgums, kurā noteikts, ka šādus datus drīkst apstrādāt vienīgi ierobežotos un precizētos nolūkos, kas atbilst fiziskās personas sniegtajai piekrišanai, un ka saņēmējs nodrošinās tādu pašu aizsardzības līmeni, kādu DPR principi, un informēs organizāciju, ja tiks konstatēts, ka pārzinis vairs nevar pildīt šo pienākumu. Līgumā paredz, ka šāda konstatējuma gadījumā pārzinis, kas ir trešā persona, pārtrauc personas datu apstrādi vai veic citus pamatotus un atbilstošus pasākumus, lai labotu situāciju.

b. Lai nosūtītu personas datus trešajai personai, kas darbojas 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 DPR principos; iii) jāveic pamatotas un atbilstošas darbības, lai nodrošinātu, ka pārstāvis apstrādā nosūtītos personas datus, ievērojot no DPR 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 DPR principi; v) saņemot attiecīgu paziņojumu, arī atbilstīgi iv) punktam, jāveic pamatotas un atbilstošas darbības, lai apturētu neatļautu apstrādi un koriģētu tās sekas; un vi) pēc ministrijas pieprasījuma jāiesniedz tai ar pārstāvi noslēgtā līguma attiecīgo privātuma noteikumu kopsavilkums vai reprezentatīva kopija.

4. **DROŠĪBA**

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

5. **DATU INTEGRITĀTE UN NOLŪKA IEROBEŽOJUMI**

a. Saskaņā ar DPR principiem personas dati ir jāierobežo līdz tādai informācijai, kas ir relevanta apstrādes nolūkiem ([6]). Organizācija nedrīkst personas datus apstrādāt tādā veidā, kas ir nesaderīgs ar tiem nolūkiem, kuriem tie sākotnēji vākti vai kuriem fiziska persona pēc tam atļāvusi tos izmantot. Ciktāl tas vajadzīgs minētajiem nolūkiem, organizācijai jāveic samērīgi pasākumi, lai nodrošinātu, ka dati saistībā ar paredzētajiem nolūkiem ir ticami, precīzi, pilnīgi un atjaunināti. Kamēr organizācija glabā šādu informāciju, tai jāievēro DPR principi.

b. Informāciju var saglabāt tādā veidā, kas ļauj identificēt vai padarīt identificējamu ([7]) fizisko personu tikai tik ilgi, cik tas nepieciešams apstrādes nolūkam 5. punkta a apakšpunkta nozīmē. Šis pienākums neliedz organizācijām apstrādāt personas datus 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 citus ES un ASV DPR principus un noteikumus. Organizācijām būtu jāveic samērīgi un piemēroti pasākumi šo noteikumu ievērošanai.

6. **PIEKĻUVE**

a. Fiziskām personām jābūt piekļuvei personas datiem par sevi, kas ir organizācijas rīcībā, un iespējai šo informāciju labot, mainīt vai dzēst, ja šie dati ir neprecīzi vai arī tikuši apstrādāti, pārkāpjot DPR principus, izņemot, ja apgrūtinājums vai izmaksas saistībā ar piekļuves nodrošināšanu būtu neatbilstīgas fiziskās personas privātuma apdraudējumam attiecīgajā gadījumā vai ja tas pārkāptu citu personu tiesības.

7. **TIESĪBU AIZSARDZĪBA, IZPILDES PANĀKŠANA UN ATBILDĪBA**

a. Rezultatīvai privātuma aizsardzībai jāietver stingri mehānismi, ar ko nodrošināt DPR principu ievērošanu, to fizisko personu tiesību aizsardzību, kuras ietekmē DPR principu neievērošana, un sekas, kas rodas organizācijai, ja šie principi netiek ievēroti. Šādiem mehānismiem jāietver vismaz šādi elementi:

i. gatavi, pieejami un neatkarīgi tiesību aizsardzības mehānismi, ar ko izmeklēt un ātri risināt katras fiziskas personas sūdzības un domstarpības, neradot fiziskajai personai nekādas izmaksas un ievērojot DPR principus, kā arī atlīdzināt kaitējumu, ja to paredz piemērojamie tiesību akti vai privātā sektora iniciatīvas;

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

iii. pienākums risināt problēmas, kas rodas, ja organizācijas, kuras paziņo, ka ievēro DPR principus, tos neievēro, un sekas 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 ES un ASV DPR. Visām organizācijām ir ātri jāreaģē uz sūdzībām par atbilstību DPR 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.

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

([7]) 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 fizisko personu, tad attiecīgā fiziskā persona ir "identificējama".

c. Ja fiziska persona, iesniedzot attiecīgajai organizācijai paziņojumu un ievērojot I pielikumā izklāstītās procedūras un nosacījumus, ir pieprasījusi šķīrējtiesu, kuras lēmums ir saistošs, tai ir pienākums piedalīties šķīrējtiesas procesā un izpildīt I pielikumā paredzētos noteikumus.

d. Saistībā ar tālāku nosūtīšanu dalīborganizācija ir atbildīga par to personas datu apstrādi, ko tā saņem saskaņā ar ES un ASV DPR un pēc tam nosūta trešai personai, kura tās vārdā darbojas kā pārstāvis. Dalīborganizācija saskaņā ar DPR principiem joprojām ir atbildīga, ja tās pārstāvis apstrādā šādus personas datus DPR principiem neatbilstīgā veidā, izņemot, ja organizācija var pierādīt, ka nav atbildīga par notikumu, kas izraisījis kaitējumu.

e. Ja par organizāciju tās neatbilstības dēļ pieņem tiesas rīkojumu vai ASV oficiālas iestādes (piemēram, *FTC* vai *DoT*) izdotu rīkojumu, kas minēts DPR principos vai to turpmākajā pielikumā, organizācija publisko visas attiecīgās ar ES un ASV DPR saistītās iedaļas jebkurā tiesai vai ASV oficiālajai iestādei iesniegtajā atbilstības vai novērtējuma ziņojumā, ciktāl tas atbilst konfidencialitātes prasībām. Ministrija ir izveidojusi speciālu kontaktpersonu, ar ko DAI var sazināties par jebkādām ar dalīborganizāciju atbilstību saistītām problēmām. *FTC* un *DoT* prioritāri izskatīs ministrijas un ES dalībvalstu iestāžu pieprasījumus par neatbilstību DPR principiem un, ievērojot spēkā esošos konfidencialitātes ierobežojumus, ar pieprasījumu iesniedzējām valsts iestādēm savlaicīgi apmainīsies ar informāciju par pieprasījumiem.

## III. **PAPILDPRINCIPI**

### 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

vi. saistīta ar datiem, ko fiziskā personā acīmredzami ir publiskojusi.

### 2. **Izņēmumi attiecībā uz žurnālistiku**

a. Ņemot vērā ASV nodrošināto preses brīvības konstitucionālo aizsardzību, gadījumos, kad ASV Konstitūcijas Pirmajā grozījumā noteiktās brīvas preses tiesības saduras ar privātuma aizsardzības interesēm, Pirmajam grozījumam jāreglamentē šo interešu līdzsvarošana attiecībā uz ASV personu vai organizāciju darbībām.

b. DPR principu prasības neattiecas uz personas datiem, kas ir savākti publicēšanai, pārraidīšanai vai citām žurnālistikas materiālu publiskas paziņošanas formām, neatkarīgi no tā, vai tie ir izmantoti, kā arī uz informāciju iepriekš publicētos materiālos, kas tiek izplatīti no mediju arhīviem.

### 3. **Sekundārā atbildība**

a. Interneta pakalpojumu sniedzēji ("IPS"), telekomunikāciju uzņēmumi un citas organizācijas nav atbildīgas saskaņā ar DPR principiem, ja tās citas organizācijas vārdā informāciju tikai pārsūta, maršrutē, komutē vai uzglabā kešatmiņā. ES un ASV DPR nerada sekundāru atbildību. Ciktāl organizācija darbojas tikai kā kanāls trešās personas nosūtītajiem datiem un nenosaka šo personas datu apstrādes nolūkus un līdzekļus, tai atbildība nav jāuzņemas.

4. **Pienācīga pārbaude un revīziju veikšana**

a. Revidentu un investīciju baņķieru darījumi var būt saistīti ar personas datu apstrādi bez fiziskas personas piekrišanas vai ziņas. Paziņošanas, izvēles un piekļuves princips to pieļauj, ja vien apstrāde notiek tālāk aprakstītajos apstākļos.

b. Regulāri tiek veikta valsts akciju sabiedrību un šauram lokam piederošu uzņēmumu – arī dalīborganizāciju – revīzija. Priekšlaicīgi izpaužot informāciju par šādām revīzijām, jo īpaši tām, kurās izskata iespējamus pārkāpumus, var tās nelabvēlīgi ietekmēt. Arī dalīborganizācijai, kas ir iesaistīta iespējamā apvienošanas vai pārņemšanas darījumā, būs jāveic "pienācīgas rūpības" pārbaudes 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. Investīciju baņķieri un advokāti, kuri iesaistīti pienācīgas rūpības pārbaudē, vai revidenti, kas veic revīziju, var informāciju apstrādāt bez fiziskas personas 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 DPR principu piemērošana kaitētu organizācijas likumīgajām interesēm. Šīs likumīgās intereses ir, piemēram, uzraudzīt, vai organizācijas pilda savus juridiskos pienākumus un veic likumīgas grāmatvedības darbības, kā arī vajadzība pēc konfidencialitātes, kas ir saistīta ar iespējamu iegādi, apvienošanos, kopuzņēmumu veidošanu vai citiem tamlīdzīgiem darījumiem, ko veic investīciju baņķieri vai revidenti.

5. **Datu aizsardzības iestāžu loma**

a. Organizācijas īstenos savu apņemšanos sadarboties ar DAI, kā aprakstīts tālāk. Atbilstīgi ES un ASV DPR ASV organizācijām, kuras saņem personas datus no ES, jāapņemas izmantot rezultatīvus mehānismus, ar ko nodrošināt DPR principu ievērošanu. Konkrētāk, kā izklāstīts tiesību aizsardzības, izpildes panākšanas un atbildības principā, dalīborganizācijām jānodrošina: a) i) to fizisko personu tiesību aizsardzība, uz kuriem dati attiecas; a) ii) turpmākas kontroles procedūras, lai pārbaudītu, vai to sniegtie apliecinājumi un apgalvojumi par privātuma praksi ir patiesi; un a) iii) pienākums risināt problēmas, kas rodas, ja netiek ievēroti DPR principi, un sekas šādām organizācijām. Ja organizācija 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 ES un ASV DPR pašsertifikācijas pieteikumā ministrijai (sk. papildprincipu par pašsertifikāciju) paziņojot, ka tā:

i. ir nolēmusi izpildīt 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 DPR principiem iesniegto sūdzību izmeklēšanu un risināšanu; un

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

c. <u>DAI komisiju darbība</u>

i. Sadarbība ar DAI tiks nodrošināta kā informācija un ieteikumi šādā veidā:

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

2. Komisija attiecīgajām ASV organizācijām sniegs ieteikumus par neatrisinātām fizisku personu sūdzībām par tādu personas datu apstrādi, kas saskaņā ar ES un ASV DPR satvarā ir nosūtīti no ES un ASV. Šie ieteikumi būs izstrādāti, lai nodrošinātu, ka DPR principus piemēro pareizi, un tajos būs iekļauti tādi tiesiskās aizsardzības līdzekļi attiecīgajai(-ām) fiziskajai(-ām) personai(-ām), ko DAI uzskata par piemērotiem.

3. Komisija šādus ieteikumus sniegs, atbildot uz attiecīgo organizāciju pieprasījumiem un/vai nepastarpinātām fizisku personu sūdzībām par organizācijām, kas ir apņēmušās sadarboties ar DAI ES un ASV DPR īstenošanas nolūkā, vienlaikus iedrošinot un, ja vajadzīgs, palīdzot šādām fiziskām personām 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 DAI nekādu atbildību.

ii. Kā iepriekš minēts, organizācijām, kas izvēlas šo strīdu izšķiršanas veidu, jāapņemas ievērot DAI ieteikumus. Ja organizācija 25 dienās no ieteikumu sniegšanas tos neievēro un nav sniegusi pietiekamu pamatojumu par kavēšanos, komisija pati paziņo par savu nodomu vai nu nodot lietu *FTC*, *DoT* vai citai ASV federālajai vai štata iestādei, kam ir likumā noteiktas pilnvaras veikt izpildes panākšanas darbības krāpšanas vai sagrozījumu gadījumā vai secināt, ka vienošanās par sadarbību ir būtiski pārkāpta un tādēļ jāuzskata par spēkā neesošu. Pēdējā gadījumā komisija informēs ministriju, lai tā varētu atbilstoši grozīt datu privātuma regulējuma sarakstu. Ja organizācija neievēro apņemšanos sadarboties ar DAI, kā arī DPR principus, saskaņā ar *FTC* likuma 5. pantu (15 U.S.C. § 45), 49 U.S.C. § 41712 vai citu attiecīgu likumu var vērsties tiesā ar prasību par maldinošu praksi.

d) Ja organizācija vēlas, lai tās ES un ASV DPR priekšrocības attiektos arī uz cilvēkresursu datiem, ko no ES nosūta izmantošanai saistībā ar darba attiecībām, tai attiecībā uz šādiem datiem jāapņemas sadarboties ar DAI (sk. papildprincipu par cilvēkresursu datiem).

e) Organizācijām, kas izvēlēsies šo iespēju, būs jāmaksā gada maksa, kura paredzēta komisijas darbības izmaksu segšanai. Tām var papildus prasīt segt visas vajadzīgās tulkošanas izmaksas, kuras rodas saistībā ar tādu pieprasījumu vai sūdzību izskatīšanu komisijā, kuri vērsti pret šīm organizācijām. Maksas apmēru nosaka ministrija pēc apspriešanās ar Eiropas Komisiju. Maksu var iekasēt ministrijas izvēlēta trešā persona, kas darbojas kā šim nolūkam iekasēto līdzekļu pārvaldītājs. Ministrija cieši sadarbosies ar Komisiju un DAI, lai izstrādātu atbilstošas procedūras maksas veidā iekasēto līdzekļu sadalei, kā arī citus komisijas procesuālos un administratīvos aspektus. Ministrija un Komisija var vienoties mainīt maksas iekasēšanas biežumu.

6. **Pašsertifikācija**

a. Ar ES un ASV DPR saistītās priekšrocības tiek saņemtas no dienas, kad ministrija iekļauj organizāciju datu privātuma regulējuma sarakstā. Ministrija iekļaus organizāciju datu privātuma regulējuma sarakstā tikai pēc tam, kad būs konstatējusi, ka organizācijas sākotnējais pašsertifikācijas pieteikums ir pilnīgs, un svītros organizāciju no minētā saraksta, ja tā brīvprātīgi izstāsies, nepabeigs ikgadējo atkārtoto sertifikāciju vai pastāvīgi neievēros DPR principus (sk. papildprincipu par strīdu izšķiršanu un izpildes panākšanu).

b. Lai sākotnēji veiktu pašsertifikāciju vai pēc tam veiktu atkārtotu ES un ASV DPR sertifikāciju, organizācijai katru reizi jāiesniedz ministrijai pieteikums, ko organizācijas, kura veic pašsertifikāciju vai (attiecīgā gadījumā) atkārtotu sertifikāciju, vārdā iesniedz amatpersona, kas apliecina, ka organizācija ievēro principus ([8]), minētajā pieteikumā ir iekļauta vismaz šāda informācija:

([8]) Pieteikums ministrijas datu privātuma regulējuma tīmekļa vietnē jāiesniedz fiziskai personai, kura ir pilnvarota organizācijas un jebkuras tās aptverto struktūru vārdā sniegt paziņojumus par DPR principu ievērošanu.

i. ASV organizācijas, kura veic pašsertifikāciju vai atkārtotu sertifikāciju, nosaukums, kā arī visu tās ASV struktūrvienību vai ASV meitasuzņēmumu nosaukums(-i), kuras arī ievēro DPR principus un uz kurām organizācija vēlas piemērot tās pašsertifikāciju;

ii. organizācijas darbību apraksts attiecībā uz personas datiem, kas tiktu saņemti no ES saskaņā ar ES un ASV DPR;

iii. organizācijas attiecīgā privātuma politikas dokumenta vai dokumentu apraksts attiecībā uz šādiem personas datiem, cita starpā 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; un

2. tās īstenošanas sākuma datumu;

iv. organizācijas kontaktinformāciju, ko izmantot saistībā ar sūdzību izskatīšanu, piekļuves pieprasījumiem un jebkādiem citiem ar DPR principiem saistītiem jautājumiem ([9]), tajā skaitā:

1. attiecīgās(-o) personas(-u) vārdu(-us), amatu(-us) (attiecīgā gadījumā), e-pasta adresi(-es) un tālruņa numuru(-us) vai attiecīgo(-s) kontaktbiroju(-us) organizācijā; un

2. organizācijas attiecīgo ASV pasta adresi;

v. 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 DPR principos vai to turpmākā pielikumā);

vi. visu to privātuma programmu nosaukumus, kuros kā dalībniece iesaistīta organizācija;

vii. pārbaudes metodi (t. i., pašnovērtējums vai ārējas atbilstības pārbaudes, norādot arī trešo personu, kas veic šādas pārbaudes) ([10]); un

viii. ar DPR principiem saistīto neatrisināto sūdzību izmeklēšanas nolūkiem pieejamo(-s) attiecīgo(-s) neatkarīgo(-s) tiesību aizsardzības mehānismu(-s) ([11]).

c. Ja organizācija vēlas, lai tās ES un ASV DPR priekšrocības attiektos arī uz cilvēkresursu informāciju, ko no ES nosūta izmantošanai saistībā ar darba attiecībām, tā var šādi rīkoties tad, ja DPR principos vai turpmākā šo principu pielikumā uzskaitītai oficiālajai iestādei ir jurisdikcija uzklausīt pret organizāciju ierosinātas prasības, kas izriet no cilvēkresursu informācijas apstrādes. Turklāt organizācijai tas jānorāda tās sākotnējā pašsertifikācijas pieteikumā, kā arī atkārtotas sertifikācijas pieteikumos, un jāpauž apņemšanās sadarboties ar attiecīgo ES iestādi vai iestādēm atbilstīgi piemērojamiem papildprincipiem 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.

([9]) Galvenā "organizācijas kontaktpersona" vai "organizācijas amatpersona" nedrīkst būt ārējs darba pakalpojumu sniedzējs (piemēram, ārējs padomdevējs vai ārējs konsultants).

([10]) Sk. papildprincipu par pārbaudi.

([11]) Sk. papildprincipu par strīdu izšķiršanu un izpildi.

d. Ministrija uzturēs un darīs publiski pieejamu datu privātuma regulējuma sarakstu ar organizācijām, kuras ir iesniegušas pilnīgus sākotnējos pašsertifikācijas pieteikumus, un atjaunināsšo sarakstu, pamatojoties uz aizpildītiem ikgadējiem atkārtotas sertifikācijas pieteikumiem, kā arī paziņojumiem, kas saņemti saskaņā ar papildprincipu par strīdu izšķiršanu un izpildes panākšanu. Šādi atkārtotas sertifikācijas pieteikumi jāiesniedz ne retāk kā reizi gadā; pretējā gadījumā organizācija tiks svītrota no datu privātuma regulējuma saraksta , un ES un ASV DPR priekšrocības vairs netiks nodrošinātas. Visām organizācijām, kuras ministrija ir iekļāvusi datu privātuma regulējuma sarakstā, ir jābūt attiecīgai privātuma politikai, kas atbilst paziņošanas principam, un šajā privātuma politikā jānorāda, ka attiecīgā organizācija ievēro DPR principus ([12]). Ja organizācijas privātuma politika ir pieejama tiešsaistē, tajā jāiekļauj hipersaite uz ministrijas datu privātuma regulējuma tīmekļa vietni un hipersaite uz tīmekļa vietni vai sūdzību iesniegšanas veidlapu saistībā ar neatkarīgu tiesību aizsardzības mehānismu, kas fiziskajai personai bez maksas pieejams, lai izmeklētu ar DPR principiem saistītas neatrisinātas sūdzības.

e. DPR principus piemēro uzreiz pēc pašsertifikācijas. Dalīborganizācijām, kas iepriekš veikušas pašsertifikāciju saistībā ar ES un ASV privātuma vairoga regulējuma principu ievērošanu, būs jāatjaunina sava privātuma politika, tajā ievietojot atsauci uz "ES un ASV datu privātuma regulējuma principiem". Šādas organizācijas iekļauj šo atsauci pēc iespējas drīz un katrā ziņā ne vēlāk kā trīs mēnešu laikā pēc ES un ASV datu privātuma regulējuma principu spēkā stāšanās dienas.

f. Organizācijai ir jāpiemēro DPR principi visiem personas datiem, kas no ES saņemti, pamatojoties uz ES un ASV DPR. Apņemšanās ievērot DPR principus laika ziņā nav ierobežota attiecībā uz personas datiem, kas saņemti periodā, kad organizācija izmanto ES un ASV DPR 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 ES un ASV DPR izstāsies. Organizācijai, kas vēlas izstāties no ES un ASV DPR, par to iepriekš jāpaziņo ministrijai. Šajā paziņojumā ir arī jānorāda, ko organizācija darīs ar personas datiem, kurus tā saņēmusi, pamatojoties uz ES un ASV DPR (t. i., saglabās, atgriezīs vai dzēsīs datus; ja tā datus saglabās, jānorāda, ar kādiem atļautiem līdzekļiem tā nodrošinās datu aizsardzību). Organizācijai, kas izstājas no ES un ASV DPR, taču vēlas attiecīgos datus glabāt arī turpmāk, katru gadu jāapstiprina ministrijai apņemšanās turpināt DPR principu piemērošanu datiem vai nodrošināt "pietiekamu" datu aizsardzību ar citiem atļautiem līdzekļiem (piemēram, izmantojot līgumu, kurā ir pilnīgi atspoguļotas attiecīgo Komisijas pieņemto līguma standartklauzulu prasības); pretējā gadījumā organizācijai informācija jāatgriež vai jādzēš ([13]). Organizācijai, kas izstājas no ES un ASV DPR, jādzēš no attiecīgās privātuma politikas visas atsauces uz ES un ASV DPR, kuras norāda, ka organizācija aktīvi turpina piedalīties ES un ASV DPR un ir tiesīga saņemt ar to saistītās priekšrocības.

([12]) Organizācija, kas pašsertifikāciju veic pirmo reizi, savā galīgajā privātuma politikā nedrīkst norādīt uz dalību ES un ASV DPR, līdz brīdim, kad ministrija paziņo organizācijai, ka tā var to darīt. Iesniedzot pirmo pašsertifikācijas pieteikumu, organizācijai jāiesniedz ministrijai DPR principiem atbilstošs privātuma politikas projekts. Kad ministrija būs konstatējusi, ka organizācijas sākotnējais pašsertifikācijas pieteikums ir pilnīgs, ministrija paziņos organizācijai, ka tai ir jāpabeidz (piemēram, attiecīgā gadījumā jāpublicē) tās ES un ASV DPR atbilstošā privātuma politika. Organizācijai nekavējoties jāinformē ministrija, tiklīdz attiecīgā privātuma politika ir pabeigta, un tad ministrija iekļauj organizāciju datu privātuma regulējuma sarakstā.

([13]) Ja organizācija izstāšanās brīdī izvēlas saglabāt personas datus, ko tā saņēmusi, pamatojoties uz ES un ASV DPR, un katru gadu apliecināt ministrijai, ka tā turpina piemērot DPR principus šādiem datiem, organizācijai reizi gadā pēc izstāšanās ir jāapliecina ministrijai (t. i., ja vien un kamēr organizācija nenodrošina "pietiekamu" šādu datu aizsardzību ar citiem atļautiem līdzekļiem vai neatgriež vai neizdzēš visus šādus datus un neinformē par to ministriju), kādas darbības tā veikusi ar šiem personas datiem, kādas darbības tā veiks ar visiem personas datiem, kurus tā turpinās glabāt, un kas būs pastāvīgais kontaktpunkts ar DPR principiem saistītiem jautājumiem.

g. Organizācijai, kas korporatīvā statusa maiņas dēļ (piemēram, apvienošanās, pārņemšanas, bankrota vai likvidācijas rezultātā) pārstās pastāvēt kā atsevišķa juridiska persona, par to iepriekš jāpaziņo ministrijai. Paziņojumā būtu arī jānorāda, vai struktūra, kas tiks radīta korporatīvā statusa maiņas rezultātā, i) turpinās piedalīties ES un ASV DPR, izmantojot esošu pašsertifikāciju; ii) veiks pašsertifikāciju kā jauna ES un ASV DPR dalībniece (piemēram, ja jaunajai vai pārveidotajai struktūrai jau nav spēkā esošas pašsertifikācijas, uz kuru pamatojoties, tā varētu piedalīties ES un ASV DPR); vai iii) ieviesīs citas garantijas, piemēram, rakstisku vienošanos, kas nodrošinās DPR principu nepārtrauktu piemērošanu attiecībā uz visiem personas datiem, kurus organizācija saņēmusi saskaņā ar ES un ASV DPR un kuri tiks glabāti arī turpmāk. Ja nav piemērojams ne i), ne ii), ne iii) punkts, visi personas dati, kas saņemti saskaņā ar ES un ASV DPR, ir nekavējoties jāatgriež vai jāizdzēš.

h. Ja organizācija kāda iemesla dēļ pārtrauc dalību ES un ASV DPR, tai jādzēš visi paziņojumi, kas norāda, ka tā turpina piedalīties ES un ASV DPR vai ir tiesīga saņemt no tā izrietošās priekšrocības. Ja tiek izmantota ES un ASV DPR sertifikācijas zīme, arī tā ir jānoņem. *FTC*, *DoT* vai cita attiecīga valdības iestāde var tiesiski apstrīdēt jebkuru plašai sabiedrībai sniegtu sagrozītu paziņojumu par to, ka organizācija ievēro DPR 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. **Pārbaude**

a. Organizācijām ir jānodrošina turpmākas kontroles procedūras, ar ko pārbaudīt, vai apliecinājumi un apgalvojumi, ko tās ir izteikušas par savu ar ES un ASV DPR saistīto privātuma praksi, ir patiesi un vai šo praksi īsteno, kā aprakstīts, un atbilstīgi DPR 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 organizācija ir izvēlējusies pašnovērtēšanu, ar šādu pārbaudi jāpierāda, ka tās privātuma politika attiecībā uz personas datiem, kas saņemti no ES, ir precīza, visaptveroša, viegli pieejama, atbilst DPR principiem un ir pilnībā īstenota (t. i., tiek ievērota). Pārbaudē arī jānorāda, ka fiziskas personas ir informētas par iekšējo sūdzību izskatīšanas kārtību un par neatkarīgu(-iem) tiesību aizsardzības mehānismu(-iem), ar kura(-u) starpniecību tās var iesniegt sūdzības; 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. Vismaz reizi gadā organizācijas amatpersonai vai citam organizācijas pilnvarotam pārstāvim jāparaksta paziņojums, kas apliecina pašnovērtēšanas pabeigšanu, un jādara tas pieejams pēc fizisku personu pieprasījuma vai saistībā ar izmeklēšanu vai sūdzību par neatbilstību.

d. Ja organizācija ir izvēlējusies ārēju atbilstības pārbaudi, ar šādu pārbaudi ir jāpierāda, ka tās privātuma politika attiecībā uz personas datiem, kas saņemti no ES, ir precīza, visaptveroša, viegli pieejama, atbilst DPR principiem un ir pilnībā īstenota (t. i., tiek ievērota). Tajā arī jānorāda, ka fiziskās personas ir informētas par mehānismu(-iem), ar kuru(-iem) tās var iesniegt sūdzības. Pārbaudes metodes var neierobežoti un atbilstoši vajadzībai ietvert revīziju, izlases veida pārskatīšanu, "mānekļu" vai tehnoloģisku rīku izmantošanu. Vismaz reizi gadā vai nu pārbaudes veicējam, vai arī organizācijas amatpersonai vai citam organizācijas pilnvarotam pārstāvim jāparaksta paziņojums, kas apliecina ārējas atbilstības pārbaudes sekmīgu pabeigšanu, un jādara tas pieejams pēc fizisku personu pieprasījuma vai saistībā ar izmeklēšanu vai sūdzību par neatbilstību.

e. Organizācijām jāglabā dokumentācija par ES un ASV DPR privātuma prakses īstenošanu un pēc pieprasījuma saistībā ar izmeklēšanu vai sūdzību par neatbilstību jāuzrāda tā neatkarīgai strīdu izšķiršanas 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 no ministrijas par DPR principu ievērošanu organizācijā.

8. **Piekļuve**

a. Piekļuves principa īstenošana praksē

i. Saskaņā ar DPR principiem tiesības uz piekļuvi ir būtiskas privātuma aizsardzībai. Jo īpaši tās ļauj fiziskām personām pārliecināties par tās informācijas precizitāti, ko par viņām glabā. Piekļuves princips nozīmē, ka fiziskām personām ir tiesības:

1. iegūt no organizācijas apstiprinājumu par to, vai tā apstrādā vai neapstrādā ar minētajām fiziskajām personām saistītus personas datus ([14]);

2. uz datu paziņošanu, lai tās varētu pārbaudīt to precizitāti un apstrādes likumību; un

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

ii. Fiziskām personām nav jāpamato pieprasījumi piekļūt saviem personas datiem. Atbildot uz fizisku personu piekļuves pieprasījumiem, organizācijām vispirms būtu jāņem vērā pieprasījuma iemesls(-i). Piemēram, ja piekļuves pieprasījums ir neskaidrs vai attiecas uz plašu jomu, organizācija var sākt ar dialogu ar attiecīgo fizisko personu, lai labāk saprastu pieprasījuma cēloni un atrastu attiecīgo informāciju. Organizācija varētu jautāt, ar kuru organizācijas daļu(-ām) fiziskā persona ir sazinājusies, 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 pārējiem personas datiem, 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 fiziskajai personai, 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 fiziskās personas privātuma apdraudējumiem. Izmaksas un apgrūtinājums ir svarīgi faktori, un tie būtu jāņem vērā, taču tie nav galvenie aspekti, nosakot, vai piekļuves nodrošināšana ir pamatota.

ii. Piemēram, ja personas datus izmanto, lai pieņemtu lēmumus, kas fizisko personu būtiski ietekmēs (piemēram, par tādu svarīgu priekšrocību kā apdrošināšana, hipotēka vai darbs piešķiršanu vai atteikšanu), atbilstīgi šo papildprincipu pārējiem noteikumiem organizācijai informācija būtu jāizpauž arī tad, ja tās sniegšana būtu diezgan sarežģīta vai dārga. Ja pieprasītie personas dati nav sensitīvi vai tos neizmanto, pieņemot lēmumus, kas būtiski ietekmēs fizisko personu, un tie ir gatavi, pieejami 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.

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

ii. Ja konfidenciālu komercinformāciju var viegli nošķirt no pārējiem personas datiem, kuriem prasa piekļuvi, organizācijai būtu jānošķir konfidenciālā komercinformācija un jādara pieejama nekonfidenciālā informācija.

d. Datubāzu organizācija

i. Organizācija var sniegt piekļuvi, izpaužot fiziskai personai attiecīgos personas datus; tai nav jānodrošina fiziskajai personai piekļuve organizācijas datubāzei.

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

e. Kad var ierobežot piekļuvi

i. Tā kā organizācijām vienmēr godprātīgi jācenšas nodrošināt fiziskām personām piekļuvi viņu personas datiem, tās var šādu piekļuvi ierobežot tikai noteiktos apstākļos un visiem piekļuves ierobežošanas iemesliem jābūt konkrētiem. Saskaņā ar VDAR organizācija var ierobežot piekļuvi informācijai, ja tās izpaušana var būt pretrunā svarīgu sabiedrības interešu aizsardzībai, piemēram, valsts (nacionālajai) drošībai, aizsardzībai vai sabiedrības drošībai. Turklāt piekļuvi var liegt, ja personas datus 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, tajā skaitā 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 fiziskajām personām piekļuves ierobežošanas iemesli, kā arī, kur tās var saņemt papildu informāciju.

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

i. Fiziskai personai ir tiesības saņemt apstiprinājumu par to, vai konkrētās organizācijas rīcībā ir ar viņu saistīti personas dati. Fiziskai personai arī ir tiesības pieprasīt, lai tai 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 fiziskā persona piedāvā tās segt.

g. Atkārtoti vai apgrūtinoši piekļuves pieprasījumi

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

h. Krāpnieciski piekļuves pieprasījumi

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

i. Atbilžu sniegšanas termiņš

i. Organizācijām būtu jāatbild uz piekļuves pieprasījumiem saprātīgā laikposmā, ar pieņemamām metodēm un fiziskajai personai 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. ES un ASV DPR 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 ES un ASV DPR, tādiem personas datiem par saviem (pašreizējiem vai bijušajiem) darbiniekiem, kuri ir savākti saistībā ar darba attiecībām, uz nosūtīšanu attiecas ar ES un ASV DPR saistītās priekšrocības. Tādos gadījumos uz informācijas vākšanu un tās apstrādi pirms nosūtīšanas attiecas tās ES dalībvalsts tiesību akti, kurā informācija savākta, un jāievēro visi nosacījumi vai ierobežojumi attiecībā uz tās nosūtīšanu atbilstīgi šiem tiesību aktiem.

ii. DPR 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. Paziņošanas un izvēles principa piemērošana

i. ASV organizācija, kas saskaņā ar ES un ASV DPR ir no ES saņēmusi informāciju par darbiniekiem, drīkst to izpaust trešajām personām vai izmantot citos nolūkos vienīgi atbilstīgi paziņošanas un izvēles principiem. Piemēram, ja organizācija ir paredzējusi darba attiecību laikā savāktus personas datus izmantot ar nodarbinātību nesaistītiem mērķiem, piemēram, tirdzniecības paziņojumu izstrādei, ASV organizācijai pirms tam jādod attiecīgajām fiziskajām personām nepieciešamā izvēle, ja vien tie jau nav atļāvuši informāciju izmantot šādos nolūkos. Šāda izmantošana nedrīkst būt nesaderīga ar nolūkiem, kuros personas dati ir vākti vai kuriem fiziskā persona pēc tam atļāvusi tos 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 nosūtīšanu no dažām ES dalībvalstīm var liegt šādu informāciju izmantot citādi pat pēc nosūtīšanas ārpus ES, un šādi nosacījumi ir jāievēro.

iii. Turklāt darba devējiem jādara viss iespējamais, lai ievērotu darbinieku vēlmes attiecībā uz privātumu. 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 paziņošanas 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

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

d. Izpilde

i. Ciktāl personas datus 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 personas datu iespējami pretlikumīgu apstrādi ir atbildīga tā ASV organizācija, kas ir saņēmusi informāciju no darba devēja, un tādējādi tas nozīmē, ka, iespējams, ir pārkāpti DPR 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, kura piedalās ES un ASV DPR, kura izmanto ES cilvēkresursu datus, kas nosūtīti no ES saistībā ar darba attiecībām, un kura vēlas, lai uz šādu nosūtīšanu attiektos ES un ASV DPR, ir jāapņemas sadarboties ES kompetento iestāžu veiktajā izmeklēšanā un šādos gadījumos ievērot to ieteikumus.

e. Atbildības par tālāku nosūtīšanu principa piemērošana

i. Ja dalīborganizācijai rodas neregulāras ar nodarbinātību saistītas operatīvās vajadzības attiecībā uz personas datiem, ko pārsūta ES un ASV DPR satvarā, piemēram, lidojuma, viesnīcas numura rezervāciju vai apdrošināšanas segumu, neliela darbinieku skaita personas datus var nosūtīt pārziņiem, nepiemērojot piekļuves principu un neslēdzot līgumu ar pārzini, kas ir trešā persona, kā tiek prasīts citkārt saskaņā ar atbildības par tālāku nosūtīšanu principu, ja vien dalīborganizācija ir izpildījusi paziņošanas un izvēles principus.

10. **Obligāti līgumi par tālāku nosūtīšanu**

a. Datu apstrādes līgumi

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

ii. ES datu pārziņiem vienmēr jānoslēdz līgums, ja nosūtīšana tiek veikta tikai apstrādei, neatkarīgi no tā, vai apstrādes darbību veic Eiropas Savienībā vai ārpus tās, un no tā, vai apstrādātājs ir ES un ASV DPR dalībnieks. Līguma mērķis ir nodrošināt, ka datu apstrādātājs:

1. rīkojas tikai saskaņā ar pārziņa norādījumiem;

2. paredz atbilstošus tehniskus un organizatoriskus pasākumus, lai aizsargātu personas datus no nejaušas vai nelikumīgas iznīcināšanas vai nejaušas pazaudēšanas, pārveidošanas, neatļautas izpaušanas vai piekļuves, un saprot, vai tālāka nosūtīšana ir atļauta; un

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

iii. Tā kā dalīborganizācijas nodrošina pienācīgu aizsardzību, lai ar tām noslēgtu līgumus tikai par apstrādi, iepriekšēja atļauja nav vajadzīga.

b. Nosūtīšana kontrolētā uzņēmumu vai struktūru grupā

i. Ja personas datus nosūta starp diviem pārziņiem kontrolētā uzņēmumu vai struktūru grupā, saskaņā ar atbildības par tālāku nosūtīšanu principu līgums ne vienmēr ir nepieciešams. Datu pārziņi, kas darbojas kontrolētā uzņēmumu vai struktūru grupā, var datus šādi nosūtīt, pamatojoties uz citiem instrumentiem, piemēram, ES saistošiem uzņēmumu noteikumiem vai citiem grupas līmeņa instrumentiem (piemēram, atbilstības un kontroles programmām), kas nodrošina personas datu aizsardzības nepārtrauktību atbilstīgi DPR principiem. Šādas datu nosūtīšanas gadījumā dalīborganizācijai joprojām ir jānodrošina atbilstība DPR principiem.

c. Nosūtīšana starp pārziņiem

i. Datus var nosūtīt starp pārziņiem arī tad, ja saņēmējs pārzinis nav dalīborganizācija un nav nodrošinājis neatkarīgu tiesību aizsardzības mehānismu. Dalīborganizācijai ar saņēmēju pārzini, kurš ir trešā persona, jānoslēdz līgums, kas nodrošina tādu pašu aizsardzības līmeni, kāds ir pieejams saskaņā ar ES un ASV DPR, nenosakot, ka pārzinim, kas ir trešā persona, jābūt dalīborganizācijai 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 ES un ASV DPR izpildes panākšanu. Tas, kā izpildīt šā principa a) punkta ii) apakšpunkta prasības, ir izklāstīts papildprincipā par pārbaudi. Šis papildprincips 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 DPR 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 fizisku personu sūdzību izskatīšanu un strīdu izšķiršanu; vai iii) apņemoties sadarboties ar DAI, kas atrodas Eiropas Savienībā, vai to pilnvarotajiem pārstāvjiem.

b. Šis saraksts ir ilustratīvs piemērs 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 papildprincipu prasībām. Jāpiebilst, ka tiesību aizsardzības, izpildes panākšanas un atbildības principa prasības papildina prasību, ka pašregulatīvajiem centieniem jābūt izpildāmiem saskaņā ar *FTC* likuma 5. pantu (15 U.S.C. § 45), kas aizliedz negodīgas vai maldinošas darbības, un 49 U.S.C. § 41712, kas aizliedz pārvadātājam vai biļešu pārdevējam iesaistīties negodīgā vai maldinošā praksē gaisa pārvadājumu nozarē vai gaisa pārvadājumu pakalpojumu pārdošanas jomā, vai saskaņā ar citiem tiesību aktiem vai noteikumiem, kas aizliedz šādu rīcību.

c. Lai palīdzētu nodrošināt savu no ES un ASV DPR izrietošo saistību izpildi un veicinātu programmas pārvaldību, organizācijām un to neatkarīgajiem tiesību aizsardzības mehānismiem jāsniedz ar ES un ASV DPR saistīta informācija, kad ministrija to pieprasa. Organizācijām arī ātri jāatbild uz sūdzībām par to atbilstību DPR 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, fiziskās personas jārosina iesniegt sūdzības, kas tām var rasties par attiecīgo organizāciju. Organizācijām jāatbild fiziskajai persona 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, fiziskām personām pieejamai tiesību aizsardzībai jābūt viegli pieejamai un bez maksas. Neatkarīgām strīdu izšķiršanas struktūrām jāizskata visas sūdzības, kas saņemtas no fiziskām personām, ja vien tās nav acīmredzami nepamatotas vai nenozīmīgas. Tas neliedz neatkarīgai strīdu izšķiršanas struktūrai, 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 likumīgi pamatotas sūdzības. Turklāt ar tiesību aizsardzības mehānismiem fiziskām personām jāsniedz pilnīga un viegli pieejama informācija par to, kā darbojas strīdu izšķiršanas procedūra, kad tās iesniedz sūdzību. Šādā informācijā atbilstīgi DPR principiem vajadzētu būt iekļautam paziņojumam par mehānisma privātuma praksi. Tiem arī būtu jāsadarbojas tādu līdzekļu izstrādē kā standarta sūdzību veidlapas, lai veicinātu sūdzību atrisināšanas procesu.

ii. Neatkarīgajiem tiesību aizsardzības mehānismiem savās publiskajās tīmekļa vietnēs jāiekļauj informācija par principiem un pakalpojumiem, ko tie sniedz saskaņā ar ES un ASV DPR. Tajā jānorāda: 1) informācija par DPR principu prasībām attiecībā uz neatkarīgiem tiesību aizsardzības mehānismiem vai saite uz šādām prasībām, 2) saite uz ministrijas izstrādāto datu privātuma regulējuma tīmekļa vietni, 3) paskaidrojums, ka ES un ASV DPR ietvaros sniegtos strīdu izšķiršanas pakalpojumus fiziskas personas var saņemt bez maksas, 4) apraksts par to, kā var iesniegt ar DPR principiem saistītu sūdzību, 5) ar DPR principiem saistītu sūdzību apstrādes laikposms, un 6) iespējamo koriģējošo pasākumu apraksts.

iii. Neatkarīgajiem tiesību aizsardzības mehānismiem jāpublicē gada pārskats, kurā izklāstīta apkopota statistika par to sniegtajiem strīdu izšķiršanas pakalpojumiem. Gada pārskatā jāiekļauj šāda informāciju: 1) kopējais pārskata gada laikā saņemto ar DPR principiem saistīto sūdzību skaits, 2) saņemto sūdzību veidi, 3) strīdu izšķiršanas kvalitātes rādītāji, piemēram, sūdzību izskatīšanas ilgums, un 4) saņemto sūdzību rezultāti, jo īpaši noteikto tiesiskās aizsardzības līdzekļu vai sankciju skaits un veidi.

iv. Kā izklāstīts I pielikumā, fiziska persona var izmantot šķīrējtiesas procesu, lai neatrisinātas prasības gadījumā tiktu noteikts, vai dalīborganizācija attiecībā uz šo fizisko personu ir pārkāpusi no DPR 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 DPR principu ([15]) piemērošanas izņēmumiem vai apgalvojumiem par ES un ASV DPR nodrošinātās aizsardzības pietiekamību. Ja tiek izmantots šķīrējtiesas process, ES un ASV datu privātuma regulējuma kolēģijai (kuras sastāvā atkarībā no pušu vienošanās ir viens vai trīs šķīrējtiesneši) ir pilnvaras noteikt individuālu, specifisku, nemonetāru un taisnīgu koriģējošu pasākumu (piemēram, piekļuvi, labošanu, dzēšanu vai attiecīgo fiziskās personas datu atgriešanu), kas vajadzīgs, lai labotu DPR principu pārkāpumu vienīgi attiecībā uz konkrēto fizisko personu. Saskaņā ar Federālo šķīrējtiesas procesa likumu (*Federal Arbitration Act*) fiziskas personas un dalīborganizācijas varēs lūgt šķīrējtiesnešu lēmumu pārskatīšanu tiesā un izpildes panākšanu atbilstīgi ASV tiesību aktiem.

e. Tiesiskās aizsardzības līdzekļi un sankcijas

i. Visu neatkarīgo strīdu izšķiršanas struktūru noteikto aizsardzības līdzekļu rezultātā neatbilstība organizācijā jānovērš vai jālabo, ciktāl tas ir iespējams, un jānodrošina, ka turpmāka organizācijas veiktā apstrāde atbildīs DPR principiem un ka attiecīgā gadījumā pārtrauks tās fiziskās personas datu apstrādi, kas ir iesniegusi sūdzību. Sankcijām jābūt pietiekami stingrām, lai nodrošinātu, ka organizācija ievēro DPR principus. Vairākas dažādas stingrības pakāpes sankcijas ļaus strīdu izšķiršanas struktūrām pienācīgi reaģēt

([15]) "DPR Principi", "Pārskats", 5. punkts.

uz dažādas pakāpes neatbilstību. Sankcijām būtu jāietver gan neatbilstības konstatējumu publicēšana, gan prasība konkrētos apstākļos datus dzēst ([16]). Neatkarīgajiem tiesību aizsardzības mehānismiem jāpublicē gada pārskats, kurā izklāstīta apkopota statistika par to strīdu izšķiršanas pakalpojumiem. Privātā sektora neatkarīgām strīdu izšķiršanas struktūrām un pašregulējuma struktūrām par to, ka dalīborganizācijas neievēro to nolēmumus, jāziņo attiecīgi kompetentajai valdības iestādei vai tiesām un ministrijai.

f. *FTC* darbība

i. *FTC* ir apņēmusies prioritāri izskatīt pieprasījumus ar apgalvojumiem par DPR principu neievērošanu, kurus iesniegušas: i) privātuma pašregulējuma struktūras un citas neatkarīgas strīdu izšķiršanas struktūras; ii) ES dalībvalstis; un iii) ministrija, lai noteiktu, vai ir pārkāpts *FTC* likuma 5. pants, kurā ir aizliegtas negodīgas vai maldinošas darbības vai šāda komercprakse. Ja *FTC* secina, ka tai ir pamats uzskatīt, ka 5. pants ir pārkāpts, tā var jautājumu risināt, pieprasot administratīvu pretlikumīgas darbības pārtraukšanas rīkojumu, 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 tādu organizāciju apgalvojumiem par DPR principu ievērošanu vai dalību ES un ASV datu privātuma regulējumā, kuras vai nu vairs nav iekļautas datu privātuma regulējuma sarakstā, vai arī nekad nav ministrijai pašsertificējušas tā ievērošanu. *FTC* var panākt civiltiesisku sodu piemērošanu par administratīva pretlikumīgas darbības pārtraukšanas rīkojuma neievērošanu un par federālās tiesas nolēmuma neievērošanu var vērsties tiesā par tiesas rīkojuma nepildīšanu vai necieņu pret tiesu. FTC par visām šādām darbībām, ko tā veikusi, paziņo ministrijai. Ministrija aicina citas valdības iestādes tai ziņot par šādu lietu iznākumiem un citiem nolēmumiem, kas nosaka atbilstību DPR principiem.

g. Pastāvīga neievērošana

i. Ja organizācija pastāvīgi neievēro DPR principus, tā vairs nav tiesīga izmantot ES un ASV DPR priekšrocības. Organizācijas, kas pastāvīgi neievēro DPR principus, ministrija svītros no datu privātuma regulējuma saraksta, un tām ir jāatgriež vai jāizdzēš ES un ASV DPR ietvaros saņemtie personas dati.

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

iii. Ministrija svītros organizāciju no datu privātuma regulējuma saraksta, ja no pašas organizācijas, privātuma pašregulējuma struktūras vai citas neatkarīgas strīdu izšķiršanas struktūras, vai valdības iestādes saņems paziņojumu par pastāvīgu neievērošanu, bet tikai pēc tam, kad vispirms organizācijai 30 dienas iepriekš ir sniegts attiecīgs paziņojums un iespēja atbildēt ([17]). Tādējādi ministrijas uzturētais datu privātuma regulējuma saraksts skaidri parādīs, kuras organizācijas saņem ar ES un ASV DPR saistītās priekšrocības un kurām tādu vairs nav.

iv. Organizācijai, kas piesakās līdzdarboties pašregulējuma struktūrā, lai atkal varētu pretendēt uz dalību ES un ASV DPR, jāsniedz šai struktūrai pilnīga informācija par tās iepriekšējo dalību ES un ASV DPR.

([16]) Neatkarīgām strīdu izšķiršanas struktūrām ir rīcības brīvība attiecībā uz apstākļiem, kuros tās šīs sankcijas izmanto. Attiecīgo datu sensitivitāte ir viens faktors, kas jāņem vērā, lemjot, vai dati jādzēš, kā arī vai organizācija informāciju ir ieguvusi, izmantojusi vai izpaudusi pretrunā DPR principiem.

([17]) Ministrija šajā paziņojumā norādīs, cik ilgā laikā (kas obligāti ir īsāks par 30 dienām) organizācijai jāatbild uz paziņojumu.

12. **Izvēle – atteikuma laiks**

a. Parasti izvēles principa mērķis ir nodrošināt, ka personas datus izmanto un izpauž fiziskās personas vēlmēm un izvēlei atbilstošos veidos. Tāpēc fiziskajai personai būtu jāvar jebkurā laikā izvēlēties liegt personas datus izmantot tiešai tirgvedībai, ievērojot samērīgus ierobežojumus, ko nosaka organizācija, piemēram, dodot organizācijai laiku atteikumu īstenot. Organizācija var arī prasīt pietiekamu informāciju, lai apstiprinātu tās fiziskās personas identitāti, kas vēlas izmantošanu liegt. Amerikas Savienotās Valstīs fiziskas personas šo izvēli var izdarīt, izmantojot centralizētu atteikuma programmu. Jebkurā gadījumā fiziskai personai šīs iespējas izmantošanai būtu jānodrošina viegli pieejams un cenas ziņā pieņemams mehānisms.

b. Tāpat organizācija var izmantot informāciju atsevišķiem tiešas tirgvedības mērķiem, kad nav iespējams pirms informācijas izmantošanas dot fiziskajai personai iespēju šādu izmantošanu liegt, ja tikām organizācija nekavējoties (un pēc pieprasījuma jebkurā laikā) dod fiziskajai personai iespēju (bez maksas) atteikties no turpmākas tirgvedības paziņojumu saņemšanas un organizācija ievēro fiziskās personas vēlmes.

13. **Ceļošanas informācija**

a. Organizācijām, kas atrodas ārpus ES, vairākos gadījumos var nosūtīt 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 VDAR, ja nav lēmuma par aizsardzības līmeņa pietiekamību, personas datus var nosūtīt uz trešo valsti, ja saskaņā ar VDAR 46. pantu ir paredzētas atbilstošas datu aizsardzības garantijas vai – īpašās situācijās – ja ir izpildīts kāds no VDAR 49. panta nosacījumiem (piemēram, ja datu subjekts ir skaidri piekritis nosūtīšanai). ASV organizācijas, kas ievēro ES un ASV DPR principus, nodrošina personas datu pietiekamu aizsardzību un tāpēc var saņemt no ES nosūtītos datus, pamatojoties uz VDAR 45. pantu, un tām nav jāievieš datu nosūtīšanas instruments saskaņā ar VDAR 46. pantu vai jāizpilda VDAR 49. panta nosacījumi. Tā kā ES un ASV DPR paredz īpašus noteikumus attiecībā uz sensitīvu informāciju, šādu informāciju (kas, iespējams, jāvāc, piemēram saistībā ar patērētāju vajadzību saņemt fizisku palīdzību) var iekļaut dalīborganizācijām nosūtītajos datos. 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. **Zāles un medicīniskie izstrādājumi**

a. ES/dalībvalstu tiesību aktu vai DPR principu piemērošana

i. Uz personas datu vākšanu un jebkādu apstrādi, kas notiek pirms nosūtīšanas uz Amerikas Savienotajām Valstīm, attiecas ES/dalībvalstu tiesību akti. DPR principus datiem piemēro, tiklīdz tie ir nosūtīti 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 dati, kas savākti vienam pētījumam, tiek nosūtīti ES un ASV DPR organizācijai ASV, tā var datus izmantot jaunai zinātniskās pētniecības darbībai, ja pirms tam ir izpildīti paziņošanas un izvēles principi. Šādā paziņojumā jāsniedz ziņas par visiem turpmākiem specifiskiem datu izmantošanas mērķiem, piemēram, periodiskas turpmākas 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) fiziskā persona pēc tam piekritusi, ir jāsaņem jauna piekrišana.

c. Dalības klīniskā izmēģinājumā pārtraukšana

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

d. Datu nosūtīšana reglamentējošos un uzraudzības nolūkos

i. Farmācijas un medicīnisko ierīču uzņēmumiem ir atļauts personas datus no ES veiktajiem klīniskajiem izmēģinājumiem sniegt regulatoriem Amerikas Savienotajās Valstīs reglamentēšanas un uzraudzības nolūkiem. Ar nosacījumu, ka tiek ievērots paziņošanas un izvēles princips, līdzīga nosūtīšana ir atļauta personām, kas nav regulatori, piemēram, uzņēmumiem un citiem pētniekiem.

e. Maskētie klīniskie pētījumi

i. Lai nodrošinātu objektivitāti daudzos klīniskajos izmēģinājumos, dalībniekiem un bieži vien arī pētniekiem nevar piešķirt piekļuvi informācijai par to, kā katru dalībnieku ārstē. Tas apdraudētu zinātnisko izmēģinājumu un rezultātu pamatotību. Šādu klīnisko izmēģinājumu (dēvētu par "maskētiem pētījumiem") dalībniekiem izmēģinājuma laikā nav jāsaņem piekļuve datiem par viņu ārstēšanu, ja šis ierobežojums tika izskaidrots, kad dalībnieks iesaistījās izmēģinājumā, un ja šādas informācijas izpaušana apdraudētu veikto pētījumu integritāti.

ii. Vienošanās par dalību klīniskajā izmēģinājumā saskaņā ar šiem nosacījumiem ir pamatota atteikšanās no tiesībām uz piekļuvi. Pēc izmēģinājuma noslēgšanās un rezultātu analīzes dalībniekiem jāspēj piekļūt saviem datiem, ja viņi to prasa. Piekļuve vispirms būtu jālūdz no ārsta vai cita veselības aprūpes sniedzēja, kas viņus klīniskā izmēģinājuma laikā ārstēja, un pēc tam – sponsorējošajai organizācijai.

f. Produktu drošuma un efektivitātes uzraudzība

i. Farmācijas vai medicīnisko ierīču uzņēmumam nav jāpiemēro DPR principi – paziņošanas, izvēles, atbildības par tālāku nosūtīšanu un piekļuves principi –, veicot savu produktu drošuma un efektivitātes uzraudzību, tajā skaitā ziņojot par blakusefektiem un sekojot līdzi tādiem pacientiem/subjektiem, kas izmanto konkrētas zāles vai medicīniskās ierīces, ciktāl DPR principu ievērošana traucē reglamentējošu prasību izpildi. Tas attiecas gan, piemēram, uz veselības aprūpes sniedzēju ziņojumiem farmācijas un medicīnisko ierīču uzņēmumiem, gan uz farmācijas un medicīnisko ierīču uzņēmumu ziņojumiem tādām valdības aģentūrām kā Pārtikas un zāļu pārvalde.

g. Ar šifru kodēti dati

i. Galvenais pētnieks sākotnējos izpētes datus vienmēr ir īpaši kodējis ar šifru tā, lai neatklātu atsevišķu datu subjektu identitāti. Farmācijas uzņēmumi, kas šādu izpēti sponsorē, šifru nesaņem. Unikālais šifra kods ir pieejams tikai pētniekam, lai īpašos apstākļos viņš vai viņa varētu pētījuma subjektu identificēt (piemēram, ja tam pēcāk ir vajadzīga medicīniska uzraudzība). Uz šādi kodētu datu, kas saskaņā ar ES tiesību aktiem ir ES personas dati, nosūtīšanu no ES uz ASV attiektos DPR principi.

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

a. Organizācijai jāpiemēro drošības, datu integritātes un nolūka ierobežošanas, kā arī tiesību aizsardzības, izpildes panākšanas un atbildības princips personas datiem no publiski pieejamiem avotiem. Šos principus piemēro arī personas datiem, kas savākti no publiskiem reģistriem (t. i., reģistriem, ko uztur valdības aģentūras vai struktūrvienības jebkurā līmenī un kas parasti ir sabiedrībai pieejami).

b. Informēšanas, izvēles vai atbildības par tālāku nosūtīšanu princips nav jāpiemēro publisko reģistru informācijai, ja tā nav kopā ar nepublisku reģistru informāciju un ir ievēroti visi attiecīgajā jurisdikcijā paredzētie izmantošanas nosacījumi. Parasti paziņošanas, izvēles vai atbildības par tālāku nosūtīšanu princips nav jāpiemēro arī publiski pieejamai informācijai, ja vien Eiropas nosūtītājs nenorāda, ka uz šādu informāciju attiecas ierobežojumi, kas prasa, lai organizācija minētos principus piemērotu 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 DPR principiem apzināti publiskojusi personas datus, lai tā vai citi varētu izmantot šos izņēmumus, tā vairs nevarēs pretendēt uz ES un ASV DPR priekšrocībām.

d. Uz publisko reģistru informāciju nav jāattiecina piekļuves princips, kamēr tā nav apvienota ar citiem personas datiem (izņemot gadījumus, kad personas datu neliela daļa ir izmantota publiskā reģistra rādītāja sagatavošanai vai organizēšanai). Tomēr jāievēro visi izmantošanas nosacījumi, ko noteikusi attiecīgā kompetentā iestāde. Savukārt, ja publiskā reģistra informācija ir kopā ar citu informāciju no nepubliska reģistra (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, atbildot uz piekļuves pieprasījumiem, var iekasēt organizācijas parasto samaksu. Alternatīvi fiziskas personas var prasīt piekļuvi savai informācijai no organizācijas, kas datus apkopojusi sākotnēji.

16. **Publisko iestāžu piekļuves pieprasījumi**

a. Lai nodrošinātu pārredzamību attiecībā uz publisko iestāžu likumīgiem pieprasījumiem piekļūt personas datiem, dalīborganizācijas var brīvprātīgi sagatavot periodiskus pārredzamības ziņojumus par to, cik personas datu pieprasījumu tās no publiskajām iestādēm saņēmušas saistībā ar tiesībaizsardzības vai nacionālās drošības apsvērumiem, ciktāl šādu ziņu izpaušana ir atļauta piemērojamos tiesību aktos.

b. Šajos dalīborganizāciju ziņojumos sniegto informāciju kopā ar izlūkošanas kopienas publiskoto un citu informāciju, ievērojot DPR principus, var izmantot periodiskajā kopīgajā pārskatā par ES un ASV DPR darbību.

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

*I PIELIKUMS. ŠĶĪRĒJTIESAS MODELIS*

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

## A. **Darbības joma**

Fiziska persona var izmantot šķīrējtiesas procesu, lai neatrisinātas prasības gadījumā tiktu noteikts, vai dalīborganizācija attiecībā uz šo fizisko personu ir pārkāpusi tās no DPR 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 DPR principu ([1]) piemērošanas izņēmumiem vai apgalvojumiem par ES un ASV DPR nodrošinātās aizsardzības pietiekamību.

## B. **Pieejamie koriģējošie pasākumi**

Ja tiek izmantots šķīrējtiesas process, ES un ASV datu privātuma regulējuma kolēģijai (šķīrējtiesas kolēģijai, kuras sastāvā atkarībā no pušu vienošanās ir viens vai trīs šķīrējtiesneši) ir pilnvaras noteikt individuālu, specifisku, nemonetāru un taisnīgu koriģējošu pasākumu (piemēram, piekļuvi, labošanu, dzēšanu vai attiecīgo fiziskās personas datu atgriešanu), kas vajadzīgs, lai labotu DPR principu pārkāpumu vienīgi attiecībā uz konkrēto fizisko personu. Tās ir ES un ASV datu privātuma regulējuma kolēģijas vienīgās pilnvaras attiecībā uz koriģējošiem pasākumiem. Apsverot koriģējošos pasākumus, ES un ASV DPR kolēģijai ir jāņem vērā arī citi koriģējošie pasākumi, kas jau noteikti citu ES un ASV DPR mehānismu ietvaros. Kaitējuma, izdevumu, maksu kompensācija vai citi koriģējoši pasākumi nav pieejami. Katra puse sedz sava advokāta honorāru.

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

Fiziskai personai, kas nolemj izmantot šķīrējtiesas procesu, pirms prasības iesniegšanas jāveic šādas darbības: 1) par iespējamo pārkāpumu tieši jāinformē organizācija un jāsniedz tai iespēja problēmu atrisināt papildprincipa par strīdu izšķiršanu un izpildes panākšanu d) punkta i) apakšpunktā noteiktajā termiņā; 2) jāizmanto DPR principos paredzētais neatkarīgais tiesību aizsardzības mehānisms, par kuru fiziskajai personai nav jāmaksā; un (3) ar fiziskās personas DAI starpniecību par problēmu jāinformē ministrija un jāļauj tai pēc iespējas un bez maksas censties atrisināt problēmu termiņos, kas noteikti vēstulē no ministrijas Starptautiskās tirdzniecības pārvaldes.

Šo šķīrējtiesas procesu nevar izmantot, ja fiziskās personas apgalvojums par DPR principu pārkāpumu 1) jau ir izskatīts saistošā šķīrējtiesas procesā; 2) par to ir pieņemts galīgs spriedums tiesas procesā, kura puse bija fiziskā persona; vai 3) puses jau iepriekš ir panākušas mierizlīgumu. Turklāt šo iespēju nevar izmantot, ja DAI (1) ir pilnvaras atbilstīgi papildprincipam par datu aizsardzības iestāžu lomu vai papildprincipam par cilvēkresursu datiem, vai 2) tai ir pilnvaras izskatīt apgalvojumu par pārkāpumu, tieši iesaistot organizāciju. DAI pilnvaras izskatīt tādu pašu prasību pret ES datu pārzini pašas par sevi neliedz pieprasīt šķīrējtiesas procesu pret citu juridisku personu, kas nav pakļauta DAI pilnvarām.

## D. **Lēmumu saistošais spēks**

Fiziskas personas lēmums pieprasīt šķīrējtiesu, kuras lēmums ir saistošs, ir pilnīgi brīvprātīgs. Šķīrējtiesas lēmumi būs saistoši visām šķīrējtiesas pusēm. Pieprasot procesu, fiziskā persona atsakās no iespējas saistībā ar vienu un to pašu iespējamo pārkāpumu lūgt koriģējošu pasākumu citā forumā, izņemot gadījumus, kad iespējamo pārkāpumu nav iespējams pilnā apmērā labot ar nemonetāru koriģējošu pasākumu – tad fiziskās personas pieprasītā šķīrējtiesa neliedz iespēju pieprasīt kaitējuma kompensāciju, kas citādi ir pieejama tiesās.

([1]) "DPR principi", "Pārskats", 5. punkts.

E. **Pārskatīšana un izpildes panākšana**

Saskaņā ar Federālo šķīrējtiesas procesa likumu (*Federal Arbitration Act*) fiziskas personas un dalīborganizācijas varēs lūgt šķīrējtiesnešu lēmumu pārskatīšanu tiesā un izpildes panākšanu atbilstīgi ASV tiesību aktiem ([2]). Visas attiecīgās lietas ir jāierosina tajā federālajā apgabaltiesā, kuras teritoriālajā jurisdikcijā ir dalīborganizācijas galvenā darījumdarbības vieta.

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

F. **Šķīrējtiesas kolēģija**

Puses izvēlas ES un ASV šķīrējtiesnešus Datu privātuma regulējuma kolēģijai no tālāk aprakstītā šķīrējtiesnešu saraksta.

Saskaņā ar piemērojamiem tiesību aktiem ministrija un Komisija, ievērojot piemērojamos tiesību aktus, izveidos sarakstu, kurā iekļaus vismaz 10 šķīrējtiesnešu, kas izvēlēti to neatkarības, godprātības un kompetences dēļ. Saistībā ar šo procesu jāievēro tālāk uzskaitītie nosacījumi.

Šķīrējtiesneši:

1) sarakstā ir trīs gadus, ja vien neradīsies ārkārtas apstākļi vai izslēgšanas iemesli; ministrija sarakstā iekļautos speciālistus var vienu reizi atkārtoti iekļaut sarakstā vēl uz trim gadiem, par to iepriekš nepaziņojot Komisijai;

2) nesaņem norādījumus no kādas procesa puses, dalīborganizācijas, ASV, ES vai kādas ES dalībvalsts vai kādas citas valdības iestādes, publiskas iestādes vai izpildes iestādes un nav ar tām saistīta; un

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

([2]) Atbilstīgi Federālā šķīrējtiesas procesa likuma ("*FAA*") 2. nodaļai "uz arbitrāžas vienošanos vai šķīrējtiesas nolēmumu, kas izriet no juridiskām – līgumiskām vai cita veida – attiecībām, ko uzskata par komerciālām attiecībām, arī 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. No. 6997 ("Ņujorkas konvencija")]. " 9 U.S.C. § 202. Turklāt *FAA* ir papildus noteikts, ka "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 minētajā [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.

G. **Šķīrējtiesas procedūras**

Ministrija un Komisija saskaņā ar piemērojamiem tiesību aktiem ir vienojušās pieņemt šķīrējtiesas noteikumus, kas reglamentē procedūras ES un ASV datu privātuma regulējuma kolēģijā ([3]). Gadījumā, ja būs jāmaina procedūru noteikumi, ministrija un Komisija vienosies grozīt šos noteikumus vai pieņemt citu spēkā esošu, ASV iedibinātu šķīrējtiesas procedūru kopumu, vajadzības gadījumā ņemot vērā tālāk minētos apsvērumus.

1. Fiziska persona 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 fiziskā persona vēlas, jebkādus pavaddokumentus un materiālus un/vai ar iespējamo pārkāpumu saistīta tiesību akta aprakstu.

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

3. Vienlaikus šķīrējtiesas procesam var notikt prasības izskatīšana *FTC*.

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

5. Process noris Amerikas Savienotajās Valstīs, un fiziskā persona 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 fizisko personu pārstāv advokāts, tai bez maksas nodrošinās šķīrējtiesas sēdes mutisko tulkojumu, kā arī materiālu rakstisko tulkojumu, ja vien ES un ASV datu privātuma regulējuma kolēģija 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 fizisko personu 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.

([3]) Ministrija izvēlējās Starptautisko strīdu izšķiršanas centru ("*ICDR*"), Amerikas Šķīrējtiesu asociācijas ("*AAA*") starptautisko nodaļu (tālāk "*ICDR AAA*"), lai pārvaldītu šķīrējtiesas procesus saskaņā ar DPR principu I pielikumu un vadītu minētajā pielikumā norādīto šķīrējtiesas fondu. 2017. gada 15. septembrī ministrija un Komisija vienojās pieņemt šķīrējtiesas noteikumus, kas reglamentē saistošās šķīrējtiesas procedūras, kuras aprakstītas DPR principu I pielikumā, kā arī šķīrējtiesnešu rīcības kodeksu, kas atbilst vispārpieņemtajiem komerciālo šķīrējtiesnešu ētikas standartiem un DPR principu I pielikumam. Ministrija un Komisija vienojās pielāgot šķīrējtiesas noteikumus un rīcības kodeksu, lai atspoguļotu ES un ASV DPR atjauninājumus, un ministrija sadarbosies ar *ICDR AAA*, lai tos īstenotu.

H. **Izmaksas**

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

Saskaņā ar piemērojamiem tiesību aktiem ministrija veicinās tāda fonda uzturēšanu, kurā dalīborganizācijām būs jāveic no to lieluma daļēji atkarīgas iemaksas, ar kurām tiks segtas šķīrējtiesas procesa izmaksas, ieskaitot šķīrējtiesnešu honorārus, kuri nepārsniedz maksimālo apmēru ("robežvērtību"). Fondu pārvaldīs trešā persona, kas regulāri ziņos ministrijai par tā darbību. Ministrija sadarbosies ar trešo personu, lai periodiski pārskatītu fonda darbību, tajā skaitā nepieciešamību pielāgot iemaksu vai šķīrējtiesas procesa izmaksu robežvērtību apmēru, un cita starpā izskatīs šķīrējtiesas procesu skaitu, izmaksas un ilgumu, saprotot, ka nevajadzētu radīt dalīborganizācijām pārmērīgu finansiālo slogu. Ministrija informēs Komisiju par šādu pārskatīšanu ar trešo personu rezultātiem un sniegs Komisijai iepriekšēju paziņojumu par jebkādām iemaksu summas korekcijām. Šā noteikuma un neviena saskaņā ar to izveidota fonda darbības joma neattiecas uz advokātu honorāriem.

*II PIELIKUMS*

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

2023. gada 6. jūlijā

Tiesiskuma komisāram
cien. *Didier Reynders*
European Commission
Rue de la Loi/ Westraat 200
1049 Brussels
Belgium

Cien. komisār *Didier Reynders*!

Amerikas Savienoto Valstu vārdā ar gandarījumu pārsūtu Jums ES un ASV datu privātuma regulējuma materiālu paketi, kas kopā ar Izpildrīkojumu Nr. 14086 "Drošības pasākumu uzlabošana Amerikas Savienoto Valstu sakaru izlūkošanas darbībām" un *CFR* 28. sadaļas 201. daļu, ar ko groza Tieslietu ministrijas noteikumus ar mērķi izveidot Datu aizsardzības pārskatīšanas tiesu, atspoguļo svarīgas un detalizētas sarunas par privātuma un pilsonisko brīvību aizsardzības stiprināšanu. Šo sarunu rezultātā ir izstrādātas jaunas garantijas, kuru nolūks ir nodrošināt, ka ASV sakaru izlūkošanas darbības ir nepieciešamas un samērīgas, lai sasniegtu noteiktos nacionālās drošības mērķus, un jauns mehānisms fiziskām personām no Eiropas Savienības ("ES"), lai tās varētu izmantot tiesisko aizsardzību, ja uzskata, ka sakaru izlūkošanas darbības pret tām vērstas nelikumīgi. Tas viss kopā nodrošinās ES personas datu privātumu. ES un ASV datu privātuma regulējums būs iekļaujošas un konkurētspējīgas digitālās ekonomikas pamatā. Mums, abām pusēm, vajadzētu būt lepnām par uzlabojumiem, kas atspoguļoti minētajā regulējumā un kas uzlabos privātuma aizsardzību visā pasaulē. Kopā ar izpildrīkojumu, noteikumiem un citiem materiāliem, kas pieejami no publiskiem avotiem, šis materiālu kopums veido ļoti spēcīgu pamatu jaunam Eiropas Komisijas konstatējumam par aizsardzības līmeņa pietiekamību ([1]).

Pievienoti šādi materiāli:

— ES un ASV datu privātuma regulējuma principi, tajā skaitā papildprincipi (kopā – "DPR principi") un DPR principu I pielikums (t. i., pielikums, kurā paredzēti noteikumi, saskaņā ar kuriem datu privātuma regulējuma organizācijām ir pienākums izskatīt šķīrējtiesas procesā konkrētas neatrisinātas prasības par personas datiem, uz kuriem attiecas DPR principi);

— ministrijas Starptautiskās tirdzniecības pārvaldes, kura pārvalda datu privātuma regulējuma programmu, vēstule, kurā aprakstītas saistības, ko mūsu ministrija uzņēmusies, lai nodrošinātu ES un ASV datu privātuma regulējuma iedarbīgumu;

— vēstule no Federālās tirdzniecības komisijas, kurā aprakstīts, kā tā panāk DPR principu izpildi;

— vēstule no Satiksmes ministrijas, kurā aprakstīts, kā tā panāk DPR principu izpildi;

— Nacionālās izlūkošanas direktora biroja sagatavota vēstule par ASV nacionālās drošības iestādēm piemērojamajām garantijām un ierobežojumiem; un

— Tieslietu ministrijas sagatavota vēstule par garantijām un ierobežojumiem attiecībā uz ASV valdības piekļuvi datiem tiesībaizsardzības un sabiedrības interešu nolūkos.

([1]) Ja Komisijas lēmums par ES un ASV DPR nodrošinātā aizsardzības līmeņa pietiekamību attieksies arī uz Islandi, Lihtenšteinu un Norvēģiju, ES un ASV datu privātuma regulējuma pakete attieksies gan uz Eiropas Savienību, gan uz šīm trim valstīm.

Pilna ES un ASV datu privātuma regulējuma pakete tiks publicēta ministrijas datu privātuma regulējuma tīmekļa vietnē, un DPR principi un to I pielikums stāsies spēkā dienā, kad stāsies spēkā Eiropas Komisijas lēmums par aizsardzības līmeņa pietiekamību.

Varat būt drošs, ka Amerikas Savienotās Valstis uztver savas saistības nopietni. Ceram uz turpmāku savstarpēju sadarbību, strādājot pie ES un ASV datu privātuma regulējuma īstenošanas un kopīgi sākot šā procesa nākamo posmu.

Ar cieņu

Gina M. RAIMONDO

*III PIELIKUMS*


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

2022. gada 12. decembrī

Tiesiskuma komisāram
cien. *Didier Reynders*
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgium

Cien. komisār *Didier Reynders*!

Starptautiskās tirdzniecības pārvaldes ("*ITA*") vārdā aprakstīšu saistības, ko ir uzņēmusies Tirdzniecības ministrija ("ministrija") ar mērķi nodrošināt personas datu aizsardzību, pārvaldot un uzraugot Datu privātuma regulējuma programmu. ES un ASV datu privātuma regulējuma ("ES un ASV DPR") pabeigšana ir nozīmīgs sasniegums privātuma nodrošināšanai un uzņēmumiem abās Atlantijas okeāna pusēs, jo tas ES fiziskām personām sniegs pārliecību, ka viņu dati tiks aizsargāti un ka viņām būs pieejami tiesiskās aizsardzības līdzekļi, lai risinātu ar viņu datiem saistītus jautājumus, kā arī ļaus tūkstošiem uzņēmumu turpināt investēt un citādi iesaistīties tirdzniecībā un komercdarbībā pāri Atlantijas okeānam – tas dos labumu gan mūsu ekonomikai, gan pilsoņiem. ES un ASV DPR ir rezultāts vairākus gadus ilgam smagam darbam un sadarbībai ar jums un jūsu kolēģiem Eiropas Komisijā ("Komisija"). Mēs labprāt arī turpmāk strādāsim kopā ar Komisiju, lai gādātu, ka šie sadarbības centieni būtu rezultatīvi.

ES un ASV DPR sniegs būtiskus ieguvumus gan fiziskām personām, gan uzņēmumiem. Pirmkārt, tā nodrošina svarīgu privātuma aizsardzības pasākumu kopumu attiecībā uz ES fizisko personu datiem, kas tiek nosūtīti uz Amerikas Savienotajām Valstīm. Saskaņā ar regulējumu iesaistītajām ASV organizācijām ir jāizstrādā atbilstīga privātuma politika; publiski jāapņemas ievērot ES un ASV datu privātuma regulējuma principus, tajā skaitā papildprincipus (kopā – "DPR principi") un DPR principu I pielikumu (t. i., pielikumu, kurā paredzēti noteikumi, saskaņā ar kuriem ES un ASV DPR organizācijām ir pienākums izskatīt šķīrējtiesas procesā konkrētas neatrisinātas prasības par personas datiem, uz kuriem attiecas DPR principi), lai saistības kļūtu izpildāmas atbilstīgi ASV tiesību aktiem ([1]); reizi gadā no jauna jāapliecina šo saistību izpilde ministrijai; jānodrošina ES fiziskām personām neatkarīga un bezmaksas strīdu izšķiršana; kā arī jāpakļaujas izmeklēšanas un izpildes pilnvarām, ko īsteno DPR principos uzskaitītās ASV oficiālās iestādes (piemēram, Federālā tirdzniecības komisija ("*FTC*") un Satiksmes ministrija ("*DoT*")) vai arī ASV oficiālā iestāde, kas tālāk tiks norādīta DPR principu pielikumā. Lai gan organizācijas lēmums par pašsertifikāciju ir brīvprātīgs, tiklīdz organizācija publiski apņemas ievērot ES un ASV DPR, tās saistības kļūtu izpildāmas atbilstīgi ASV tiesību aktiem, un šo izpildi var panākt *FTC*, Transporta ministrija vai cita ASV oficiāla iestāde atkarībā no tā, kuras iestādes jurisdikcijā ir dalīborganizācija. Otrkārt, ES un ASV DPR Amerikas Savienoto Valstu uzņēmumiem – arī Eiropas uzņēmumu filiālēm, kas darbojas ASV, – sniegs iespēju saņemt personas datus no Eiropas Savienības, lai atvieglotu transatlantiskajā tirdzniecībā vajadzīgās datu plūsmas.

([1]) Organizācijām, kas veikušas pašsertifikāciju saistībā ar ES un ASV privātuma vairoga regulējuma principu ievērošanu un vēlas izmantot priekšrocības, ko sniedz dalība ES un ASV DPR, ir jāievēro ES un ASV datu privātuma regulējuma principi. Šo apņemšanos ievērot ES un ASV datu privātuma regulējuma principus šādu dalīborganizāciju privātuma politikā atspoguļo pēc iespējas drīz un katrā ziņā ne vēlāk kā trīs mēnešu laikā pēc ES un ASV datu privātuma regulējuma principu spēkā stāšanās dienas. (Sk. papildprincipa par pašsertifikāciju e) iedaļu).

Datu plūsmas starp Amerikas Savienotajām Valstīm un Eiropas Savienību ir vislielākās pasaulē un balsta ASV un ES ekonomiskās attiecības, kuru vērtība sasniedz 7,1 triljonu USD, kas nodrošina miljoniem darbvietu abās Atlantijas okeāna pusēs. 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. Transatlantiskās datu plūsmas ļauj ASV organizācijām apstrādāt datus, kas vajadzīgi, lai piedāvātu preces, pakalpojumus un nodarbinātības iespējas Eiropas iedzīvotājiem.

Ministrija ir apņēmusies cieši un produktīvi sadarboties ar ES kolēģiem, lai rezultatīvi pārvaldītu un uzraudzītu datu privātuma regulējuma programmu. Šo apņemšanos atspoguļo ministrijas izstrādātie un pastāvīgi pilnveidotie dažādie resursi, kuru mērķis ir palīdzēt organizācijām pašsertifikācijas procesā, tīmekļa vietnes izveide, kurā ieinteresētajām personām tiek sniegta tām pielāgota informācija, sadarbība ar Komisiju un Eiropas datu aizsardzības iestādēm ("DAI") ar mērķi izstrādāt vadlīnijas, kurās precizēti svarīgi ES un ASV DPR elementi, informācijas sniegšana nolūkā veicināt labāku izpratni par organizāciju datu aizsardzības pienākumiem, kā arī pārraudzība un uzraudzība attiecībā uz organizāciju atbilstību programmas prasībām.

Mūsu pastāvīgā sadarbība ar cienījamajiem ES kolēģiem ļaus ministrijai nodrošināt, ka ES un ASV DPR darbojas rezultatīvi. Amerikas Savienoto Valstu valdība jau ilgstoši sadarbojas ar Komisiju, lai veicinātu kopīgus datu aizsardzības principus, mazinot atšķirības mūsu attiecīgajās juridiskajās pieejās un vienlaikus veicinot tirdzniecību un ekonomisko izaugsmi Eiropas Savienībā un Amerikas Savienotajās Valstīs. Uzskatām, ka ES un ASV DPR, kas ir šādas sadarbības piemērs, ļaus Komisijai izdot jaunu lēmumu par aizsardzības līmeņa pietiekamību, kas ļaus organizācijām izmantot ES un ASV DPR, lai nosūtītu personas datus no Eiropas Savienības uz ASV atbilstīgi ES tiesību aktiem.

**Datu privātuma regulējuma programmas pārvaldība un uzraudzība, ko veic Tirdzniecības ministrija**

Ministrija ir stingri apņēmusies rezultatīvi pārvaldīt un uzraudzīt datu privātuma regulējuma programmu un veiks atbilstošus pasākumus un piešķirs atbilstošus resursus, lai nodrošinātu šo rezultātu. Ministrija uzturēs un darīs publiski pieejamu autoritatīvu to ASV organizāciju sarakstu, kuras ir veikušas pašsertifikāciju ministrijā un paziņojušas par apņemšanos ievērot DPR principus ("datu privātuma regulējuma saraksts"). Ministrija šo sarakstu atjauninās, pamatojoties uz dalīborganizāciju iesniegtajiem ikgadējiem atkārtotas sertifikācijas pieteikumiem un svītrojot organizācijas no saraksta, ja tās brīvprātīgi atteiksies no dalības, nepabeigs ikgadējo atkārtoto sertifikāciju saskaņā ar ministrijas procedūrām vai tiks konstatēts, ka tās pastāvīgi neievēro DPR principus. Ministrija arī uzturēs un darīs publiski pieejamu autoritatīvu reģistru par ASV organizācijām, kas ir svītrotas no datu privātuma regulējuma saraksta, un norādīs iemeslu, kāpēc katra organizācija tikusi svītrota. Iepriekš minētais autoritatīvais saraksts un reģistrs joprojām būs publiski pieejams ministrijas datu privātuma regulējuma tīmekļa vietnē. Datu privātuma regulējuma tīmekļa vietnē būs labi redzamā vietā ievietots skaidrojums par to, ka jebkurai organizācijai, kas svītrota no datu privātuma regulējuma saraksta, ir jāpārtrauc apgalvot, ka tā piedalās ES un ASV DPR vai ievēro tā prasības un ka tā var saņemt personas datus saskaņā ar ES un ASV DPR. Tomēr šādai organizācijai ir jāturpina piemērot principus attiecībā uz personas datiem, ko tā saņēmusi, piedaloties ES un ASV DPR, kamēr vien tā glabā šādu informāciju. Ministrija, turpinot savu visaptverošo un pastāvīgo apņemšanos rezultatīvi pārvaldīt un uzraudzīt datu privātuma regulējuma programmu, konkrēti apņemas veikt tālāk aprakstītos pasākumus.

Pašsertifikācijas prasību izpildes pārbaude

— Pirms organizācijas pašsertifikācijas vai ikgadējās atkārtotās sertifikācijas (kopā – "pašsertifikācija") pabeigšanas un tās iekļaušanas datu privātuma regulējuma sarakstā ministrija pārliecināsies, vai organizācija ir izpildījusi vismaz attiecīgās prasības, kas izklāstītas pašsertifikācijas papildprincipā saistībā ar to, kāda informācija organizācijai ir jāsniedz pašsertifikācijas pieteikumā ministrijai, un vai tā ir savlaicīgi iesniegusi attiecīgu privātuma politiku, kas informē fiziskas personas par visiem 13 paziņošanas principā uzskaitītajiem elementiem. Ministrija pārbaudīs, vai organizācija ir:

— norādījusi organizāciju, kas iesniedz pašsertifikāciju, kā arī visas pašsertifikāciju veikušās organizācijas ASV struktūras vai ASV meitasuzņēmumus, kuras arī ievēro DPR principus un uz kurām organizācija vēlas attiecināt tās pašsertifikāciju;

— iesniegusi prasīto organizācijas kontaktinformāciju (piemēram, kontaktinformāciju par konkrētu(-ām) fizisko(-ām) personu(-ām) un/vai biroju(-iem) pašsertifikāciju veikušajā organizācijā, kas atbild par sūdzību, piekļuves pieprasījumu un citu jautājumu izskatīšanu saskaņā ar ES un ASV DPR);

— aprakstījusi nolūku(-s), kādam(-iem) organizācija vāc un izmanto no Eiropas Savienības saņemtos personas datus;

— norādījusi, kādi personas dati tiks saņemti no Eiropas Savienības, pamatojoties uz ES un ASV DPR, un tādēļ uz tiem attieksies organizācijas pašsertifikācija;

— ja organizācijai ir publiska tīmekļa vietne – norādījusi tīmekļa adresi, kurā ir viegli pieejama tās relevantā privātuma politika, vai, ja organizācijai nav publiskas tīmekļa vietnes, – iesniegusi ministrijai attiecīgās privātuma politikas kopiju un norādījusi, kur ar šo privātuma politiku var iepazīties skartās fiziskās personas (t. i., skartie darbinieki, ja relevantā privātuma politika ir cilvēkresursu privātuma politika, vai plašāka sabiedrība, ja relevantā privātuma politika nav cilvēkresursu privātuma politika);

— savā attiecīgajā privātuma politikā atbilstošā laikā (t. i., sākotnēji tikai privātuma politikas projektā, kas iesniegts kopā ar pieteikumu, ja šis pieteikums ir sākotnēja pašsertifikācija; pretējā gadījumā – galīgajā un attiecīgā gadījumā publicētajā privātuma politikā) iekļāvusi paziņojumu, ka tā ievēro DPR principus, un ievietojusi hipersaiti uz ministrijas datu privātuma regulējuma tīmekļa vietni (piemēram, vietnes sākumlapu vai datu privātuma regulējuma saraksta tīmekļa lapu);

— savā attiecīgajā privātuma politikā savlaicīgi iekļāvusi visus pārējos 12 paziņošanas principā uzskaitītos elementus (piemēram, iespēju konkrētos apstākļos skartajai ES fiziskajai personai ierosināt saistošu šķīrējtiesas procesu; prasību izpaust personas datus, atbildot uz likumīgiem publisko iestāžu pieprasījumiem, tajā skaitā ievērot ar nacionālo drošību vai tiesībaizsardzību saistītas prasības, un tās atbildību, ja informāciju tālāk nosūta trešajām personām);

— 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 DPR principos vai to turpmākā pielikumā);

— norādījusi kādu privātuma programmu, kurā iesaistīta organizācija;

— norādījusi, vai attiecīgā metode (t. i., turpmākas kontroles procedūras, kas tai jānodrošina), ar ko nodrošina tās atbilstību DPR principiem, ir "pašnovērtējums" (t. i., iekšēja pārbaude) vai "ārējā atbilstības pārbaude" (t. i., trešās personas veikta pārbaude), un, ja tā norādījusi, ka attiecīgā metode ir ārēja atbilstības pārbaude, norādījusi arī trešo personu, kas šo pārbaudi ir veikusi;

— noteikusi atbilstošu neatkarīgu tiesību aizsardzības mehānismu, kas ir pieejams, lai izskatītu sūdzības, kas iesniegtas saskaņā ar DPR principiem, un bez maksas nodrošinātu attiecīgu tiesību aizsardzību skartajai fiziskajai personai.

— Ja organizācija ir izvēlējusies privātā sektora strīdu alternatīvas izšķiršanas struktūras nodrošināto neatkarīgo tiesību aizsardzības mehānismu, tā savā attiecīgajā privātuma politikā ir iekļāvusi hipersaiti uz attiecīgo tīmekļa vietni vai sūdzības iesniegšanas veidlapu mehānismam, kas ir pieejams, lai izmeklētu neatrisinātas sūdzības, kuras iesniegtas saskaņā ar DPR principiem, vai arī norādījusi minēto resursu tīmekļu adreses.

— Ja organizācijai vai nu ir pienākums (t. i., attiecībā uz cilvēkresursu datiem, kas nosūtīti no Eiropas Savienības saistībā ar darba attiecībām), vai tā ir izvēlējusies sadarboties ar attiecīgajām DAI tādu sūdzību izmeklēšanā un risināšanā, kas iesniegtas saskaņā ar DPR principiem, tā ir deklarējusi apņemšanos sadarboties ar DAI un ievērot to attiecīgos ieteikumus veikt konkrētus pasākumus DPR principu ievērošanai.

— Ministrija arī pārbaudīs, vai organizācijas iesniegtais pašsertifikācijas pieteikums atbilst tās relevantajam(-iem) privātuma politikas dokumentam(-iem). Ja pašsertifikāciju veikusī organizācija vēlas ietvert jebkuru no savām ASV struktūrām vai ASV meitasuzņēmumiem, kam ir atsevišķi, relevanti privātuma politikas dokumenti, ministrija pārskatīs arī šādu ietverto struktūru vai meitasuzņēmumu relevantos privātuma politikas dokumentus, lai nodrošinātu, ka tajos ir iekļauti visi paziņošanas principā noteiktie nepieciešamie elementi.

— Ministrija sadarbosies ar oficiālajām struktūrām (piemēram, *FTC* un *DoT*), lai pārbaudītu, vai organizācijas ir tās attiecīgās oficiālās struktūras jurisdikcijā, kura norādīta organizāciju pašsertifikācijas pieteikumos, ja ministrijai ir pamats apšaubīt, ka tās ir minētās struktūras jurisdikcijā.

— Ministrija sadarbosies ar strīdu alternatīvas izšķiršanas struktūrām no privātā sektora, lai pārbaudītu, vai organizācijas ir aktīvi reģistrētas neatkarīgā tiesību aizsardzības mehānismā, kas norādīts to pašsertifikācijas pieteikumos, kā arī sadarbosies ar šīm struktūrām, lai pārbaudītu, vai organizācijas ir aktīvi reģistrētas ārējai atbilstības pārbaudei, kas norādīta pašsertifikācijas pieteikumos, ja minētās struktūras var piedāvāt abu veidu pakalpojumus.

— Ministrija sadarbosies ar trešo personu, kuru ministrija izraudzījies par DAI komisijas maksas veidā iekasēto līdzekļu (t. i., gada maksas, kas paredzēta DAI komisijas darbības izmaksu segšanai) turētāju, lai pārbaudītu, vai organizācijas ir samaksājušas šo maksu par attiecīgo gadu, ja organizācijas ir norādījušas DAI kā relevanto neatkarīgo tiesību aizsardzības mehānismu.

— Ministrija sadarbosies ar trešo personu, ko ministrija izvēlēsies, lai pārvaldītu šķīrējtiesas procesus saskaņā ar DPR principu I pielikumu un vadītu minētajā pielikumā norādīto šķīrējtiesas fondu, lai pārbaudītu, vai organizācijas ir veikušas iemaksas šajā šķīrējtiesas fondā.

— Ja ministrija, pārbaudot organizāciju pašsertifikācijas pieteikumus, konstatēs kādas problēmas, tā informēs organizācijas, ka tām visas šīs problēmas ir jārisina atbilstošā ministrijas noteiktā termiņā ([2]). Ministrija tās arī informēs, ka gadījumā, ja atbilde netiks sniegta ministrijas noteiktajā termiņā vai kā citādi pašsertifikācija netiks pabeigta saskaņā ar ministrijas procedūrām, pašsertifikācijas pieteikumi tiks uzskatīti par atsauktiem un jebkāda sagrozīta informācija par organizācijas dalību ES un ASV DPR vai tās atbilstību ES un ASV DPR, *FTC*, *DoT* vai cita attiecīga valsts iestāde var ierosināt izpildes panākšanas darbības. Ministrija informēs organizācijas, izmantojot kontaktinformāciju, ko organizācijas norādījušas ministrijai.

Sadarbības veicināšana ar strīdu alternatīvas izšķiršanas struktūrām, kas sniedz ar DPR principiem saistītus pakalpojumus

— Ministrija sadarbosies ar privātā sektora strīdu alternatīvas izšķiršanas struktūrām, kas nodrošina neatkarīgus tiesību aizsardzības mehānismus, kuri ir pieejami, lai izmeklētu neatrisinātas sūdzības, kas iesniegtas saskaņā ar DPR principiem, nolūkā pārbaudīt, vai tās atbilst vismaz prasībām, kas izklāstītas papildprincipā par strīdu izšķiršanu un izpildes panākšanu. Ministrija pārbaudīs, vai:

  — tās savās publiskajās tīmekļa vietnēs iekļauj informāciju par DPR principiem un pakalpojumiem, ko tās sniedz saskaņā ar ES un ASV DPR; minētajā informācijā jāiekļauj šādas ziņas: 1) informācija par DPR principu prasībām attiecībā uz neatkarīgiem tiesību aizsardzības mehānismiem vai hipersaite uz šādām prasībām, 2) hipersaite uz ministrijas datu privātuma regulējuma tīmekļa vietni, 3) paskaidrojums, ka ES un ASV DPR ietvaros sniegtos strīdu izšķiršanas pakalpojumus fiziskas personas var saņemt bez maksas, 4) apraksts par to, kā var iesniegt ar DPR principiem saistītu sūdzību, 5) ar DPR principiem saistītu sūdzību apstrādes laikposms, un 6) iespējamo koriģējošo pasākumu apraksts. Ministrija savlaicīgi informēs šīs struktūras par būtiskām izmaiņām, kas saistītas ar datu privātuma regulējuma programmas uzraudzību un pārvaldību, ja šādas izmaiņas ir tūlītējas vai jau ir veiktas un ja tās ir saistītas ar struktūru uzdevumiem ES un ASV DPR ietvaros;

([2]) Piemēram, attiecībā uz atkārtotu sertifikāciju sagaidāms, ka organizācijas visas šādas problēmas atrisinās 45 dienu laikā (ministrija var noteikt citu atbilstošu termiņu).

— tās publicē gada pārskatu, kurā izklāstīta apkopota statistika par to sniegtajiem strīdu izšķiršanas pakalpojumiem, kurā jāiekļauj šādas ziņas: 1) kopējais pārskata gada laikā saņemto ar DPR principiem saistīto sūdzību skaits, 2) saņemto sūdzību veidi, 3) strīdu izšķiršanas kvalitātes rādītāji, piemēram, sūdzību izskatīšanas ilgums, un 4) saņemto sūdzību rezultāti, jo īpaši noteikto tiesiskās aizsardzības līdzekļu vai sankciju skaits un veidi. Ministrija struktūrām sniegs konkrētus papildu norādījumus par to, kāda informācija tām būtu jāsniedz šajos gada ziņojumos, un sniegs prasību sīkāku izklāstu (piemēram, uzskaitīs konkrētus kritērijus, kuriem sūdzībai jāatbilst, lai gada ziņojuma vajadzībām to uzskatītu par sūdzību, kas saistīta ar DPR principiem), kā arī norādīs cita veida informāciju, kas tām būtu jāsniedz (piemēram, ja struktūra sniedz arī ar DPR principiem saistītu pārbaudes pakalpojumu, – aprakstu par to, kā struktūra novērš jebkādus faktiskus vai iespējamus interešu konfliktus situācijās, kad tā sniedz organizācijai gan pārbaudes pakalpojumus, gan strīdu izšķiršanas pakalpojumus). Ministrijas papildu norādījumos tiks precizēts arī datums, līdz kuram jāpublicē struktūru gada pārskati par attiecīgo pārskata periodu.

Turpmākie pasākumi saistībā ar organizācijām, kuras paudušas vēlmi tikt svītrotas no datu privātuma regulējuma saraksta vai kuras tikušas no tā svītrotas

— Ja kāda organizācija vēlēsies izstāties no ES un ASV DPR, ministrija pieprasīs, lai organizācija no jebkuras attiecīgās privātuma politikas svītrotu jebkādas atsauces uz ES un ASV DPR, kuras norāda, ka tā turpina piedalīties ES un ASV DPR un ka tā var saņemt personas datus saskaņā ar ES un ASV DPR (sk. aprakstu par ministrijas apņemšanos meklēt nepatiesus apgalvojumus par dalību). Ministrijas arī pieprasīs, lai organizācija aizpilda un iesniedz ministrijai attiecīgu anketu, lai apliecinātu:

  — tās vēlmi izstāties;

  — ko no tālāk minētā tā darīs ar personas datiem, kurus tā saņēmusi, pamatojoties uz ES un ASV DPR, kamēr tā bija minētā regulējuma dalībniece: a) saglabās šādus datus, turpinās piemērot šiem datiem DPR principus un katru gadu apliecinās ministrijai apņemšanos piemērot DPR principus šādiem datiem, b) saglabās šādus datus un nodrošinās šādu datu "pietiekamu" aizsardzību, izmantojot citus atļautus līdzekļus, vai c) atgriezīs vai dzēsīs visus šādus datus līdz noteiktam datumam; un

  — kas organizācijā būs par pastāvīgu kontaktpunktu ar DPR principiem saistītos jautājumos.

— Ja organizācija ir izvēlējusies iepriekš minēto a) punktu, ministrija arī pieprasīs, lai tā katru gadu pēc izstāšanās (t. i., katru gadu līdz dienai, kad pagājis viens gads kopš tās izstāšanās dienas, kā arī līdz katra nākamā gada attiecīgajam datumam, ja vien un kamēr organizācija nenodrošina "pietiekamu" šādu datu aizsardzību ar citiem atļautiem līdzekļiem vai neatgriež vai neizdzēš visus šādus datus un neinformē par to ministriju) aizpilda un iesniedz ministrijai atbilstošu anketu, lai apliecinātu, kādas darbības tā veikusi ar šiem personas datiem, kādas darbības tā veiks ar visiem personas datiem, kurus tā turpinās glabāt, un kas būs pastāvīgs kontaktpunkts ar DPR principiem saistītiem jautājumiem.

— Ja organizācija ir pieļāvusi pašsertifikācijas termiņa izbeigšanos (t. i., nav pabeigusi ikgadējo atkārtoto sertifikāciju par DPR principu ievērošanu vai arī ir svītrota no datu privātuma regulējuma saraksta kāda cita iemesla, piemēram, izstāšanās, dēļ), ministrija tai uzdos aizpildīt un iesniegt ministrijai attiecīgu anketu, lai apliecinātu, vai tā vēlas izstāties vai veikt atkārtotu sertifikāciju:

  — un – ja tā vēlas izstāties – papildus apliecināt, ko tā darīs ar personas datiem, kurus tā saņēma, pamatojoties uz ES un ASV DPR, kamēr tā piedalījās ES un ASV DPR (sk. iepriekšējo aprakstu par to, kas organizācijai ir jāapliecina, ja tā vēlas izstāties);

  — un – ja tā plāno veikt atkārtotu sertifikāciju – papildus apliecināt, vai tās sertifikācijas statusa termiņa laikā ir piemērojusi DPR principus personas datiem, kas saņemti saskaņā ar ES un ASV DPR, un paskaidrot, kādus pasākumus tā veiks, lai atrisinātu neatrisinātos jautājumus, kas aizkavēja tās atkārtotu sertifikāciju.

— Ja organizācija tiek svītrota no datu privātuma regulējuma saraksta jebkura šāda iemesla dēļ: a) izstāšanās no ES un ASV DPR, b) ikgadējās atkārtotās sertifikācijas neveikšana (t. i., organizācija vai nu sāka, bet savlaicīgi nepabeidza ikgadējās atkārtotas sertifikācijas procesu, vai pat nebija sākusi ikgadējo atkārtotas sertifikācijas procesu) vai c) "pastāvīga neievērošana", tad ministrija nosūtīs paziņojumu organizācijas pašsertifikācijas pieteikumā norādītajai(-ām) kontaktpersonai(-ām), kurā būs norādīts svītrošanas iemesls, un sniegs paskaidrojums par to, ka tai jāizbeidz apgalvot, ka tā piedalās ES un ASV DPR vai ievēro tā prasības un ka tā var saņemt personas informāciju saskaņā ar ES un ASV DPR. Paziņojumā, kurā var būt iekļauts arī cits saturs, kas pielāgots svītrošanas iemeslam, būs norādīts, ka pret organizācijām, kas sniedz sagrozītu informāciju par to dalību ES un ASV datu DPR vai atbilstību tam (arī ja tās apgalvo, ka piedalās ES un ASV DPR pēc svītrošanas no datu privātuma regulējuma saraksta), *FTC*, *DoT* vai cita attiecīgā valsts iestāde var vērst izpildes panākšanas darbības.

Nepatiesu apgalvojumu par dalību meklēšana un reaģēšana uz tiem

— Vienmēr, kad organizācija: a) izstājas no dalības ES un ASV DPR, b) neveic ikgadējo atkārtoto sertifikāciju (t. i., vai nu ir sākusi, bet savlaicīgi nav pabeigusi ikgadējās atkārtotās sertifikācijas procesu, vai pat nav sākusi ikgadējo atkārtoto sertifikācijas procesu), c) tiek izslēgta no ES un ASV DPR dalībnieku loka, jo īpaši noteikumu "pastāvīgas neievērošanas dēļ", vai d) nav pabeigusi sākotnējo pašsertifikācijas procesu, kurā apliecināts, ka tā ievēro DPR principus (t. i., organizācija ir sākusi, bet savlaicīgi nav pabeigusi sākotnējās pašsertifikācijas procesu), ministrija *ex officio* veiks darbības, lai pārbaudītu, vai nevienā attiecīgajā publicētajā organizācijas privātuma politikā nav atsauču uz ES un ASV DPR, kuras norāda, ka organizācija piedalās ES un ASV DPR un ka tā var saņemt personas datus saskaņā ar ES un ASV DPR. Ja ministrija konstatēs šādas atsauces, tā informēs organizāciju par to, ka attiecīgi nodos lietu attiecīgajai aģentūrai, lai tā varētu veikt izpildes panākšanas darbības, ja organizācija turpinās sniegt sagrozītu informāciju par dalību ES un ASV DPR. Ministrija informēs organizāciju, izmantojot kontaktinformāciju, ko organizācija norādījusi ministrijai, vai vajadzības gadījumā izmantojot citus piemērotus līdzekļus. Ja organizācija nesvītros atsauces un neveiks pašsertifikāciju par atbilstību ES un ASV DPR saskaņā ar ministrijas procedūrām, ministrija *ex officio* nodos lietu *FTC*, *DoT* vai citai atbilstošai izpildes aģentūrai vai veiks citas atbilstošas darbības, lai nodrošinātu ES un ASV DPR sertifikācijas zīmes pareizu izmantošanu;

— ministrija veiks citus pasākumus, lai atklātu nepatiesus apgalvojumus par dalību ES un ASV DPR un ES un ASV DPR sertifikācijas zīmes nepareizu izmantošanu, arī saistībā ar organizācijām, kuras, atšķirībā no iepriekš aprakstītajām organizācijām, nekad nav sākušas pašsertifikācijas procesu (piemēram, veicot attiecīgu meklēšanu internetā, lai noteiktu atsauces uz ES un ASV DPR organizāciju privātuma politiku). Ja, veicot šādus pasākumus, ministrija konstatē nepatiesus apgalvojumus par dalību ES un ASV DPR un ES un ASV DPR sertifikācijas zīmes neatbilstošu izmantošanu, ministrija informēs organizāciju par to, ka vajadzības gadījumā nodos lietu attiecīgajai aģentūrai, lai tā varētu veikt izpildes panākšanas darbības, ja organizācija turpinās sniegt sagrozītu informāciju par savu dalību ES un ASV DPR. Ministrija informēs organizāciju, izmantojot kontaktinformāciju, ko organizācija norādījusi ministrijai (ja tāda būs norādīta), vai vajadzības gadījumā izmantojot citus piemērotus līdzekļus. Ja organizācija nesvītros atsauces un neveiks pašsertifikāciju par atbilstību ES un ASV DPR saskaņā ar ministrijas procedūrām, ministrija *ex officio* nodos lietu *FTC*, *DoT* vai citai atbilstošai izpildes aģentūrai vai veiks citas atbilstošas darbības, lai nodrošinātu ES un ASV DPR sertifikācijas zīmes pareizu izmantošanu;

— ministrija nekavējoties izskatīs un risinās tai iesniegtas konkrētas un nozīmīgas sūdzības par nepatiesiem apgalvojumiem par dalību ES un ASV DPR (piemēram, sūdzības, kas saņemtas no DAI, neatkarīgiem tiesību aizsardzības mehānismiem, ko nodrošinājušas privātā sektora strīdu alternatīvas izšķiršanas struktūras, datu subjektiem, ES un ASV uzņēmumiem un cita veida trešām personām); un

— ministrija var veikt citas atbilstošas korektīvas darbības. Ja ministrijai tiek sniegta sagrozīta informācija, var piemērot sankcijas saskaņā ar Likumu par nepatiesu ziņu sniegšanu (18 U.S.C. § 1001).

Datu privātuma regulējuma programmas periodiskas *ex officio* atbilstības pārbaudes un novērtējumi

— Ministrija pastāvīgi centīsies uzraudzīt ES un ASV DPR organizāciju faktisko atbilstību, lai noteiktu problēmas, kuru risināšanai varētu būt nepieciešami turpmāki pasākumi. Jo īpaši ministrija *ex officio* regulāri veiks nejauši izvēlētu ES un ASV DPR organizāciju izlases veida pārbaudes, kā arī *ad hoc* izlases veida pārbaudes konkrētās ES un ASV DPR organizācijās, ja tiks konstatēti iespējami atbilstības pārkāpumi (piemēram, iespējami atbilstības pārkāpumi, par kuriem ministriju informējušas trešās personas), lai pārbaudītu: a) ka ir pieejams(-i) kontaktpunkts(-i), kas atbild par sūdzību, piekļuves pieprasījumu un citu jautājumu izskatīšanu, kuri izriet no ES un ASV DPR; b) attiecīgā gadījumā – ka organizācijas publiski pieejamā privātuma politika ir viegli pieejama sabiedrībai gan organizācijas publiskajā tīmekļa vietnē, gan ar hipersaiti datu privātuma regulējuma sarakstā; c) ka organizācijas privātuma politika joprojām atbilst DPR principos aprakstītajām pašsertifikācijas prasībām; un d) ka organizācijas norādītais neatkarīgais tiesību aizsardzības mehānisms ir pieejams, lai izskatītu sūdzības, kas iesniegtas saskaņā ar ES un ASV DPR. Ministrija arī aktīvi sekos līdzi ziņām, lai atklātu ziņojumus, kas sniedz ticamus pierādījumus par ES un ASV DPR organizāciju neatbilstību.

— Atbilstības pārbaudes ietvaros ministrija arī pieprasīs, lai ES un ASV DPR organizācija aizpilda un iesniedz ministrijai detalizētu anketu, ja: a) ministrija ir saņēmusi konkrētas, nozīmīgas sūdzības saistībā ar organizācijas atbilstību DPR principiem, b) organizācija nesniedz apmierinošu atbildi uz ministrijas pieprasījumiem sniegt informāciju saistībā ar ES un ASV DPR vai c) pastāv ticami pierādījumi, ka organizācija nepilda savas saistības saskaņā ar ES un ASV DPR. Ja ministrija ir nosūtījusi organizācijai šādu detalizētu anketu un organizācija nav sniegusi apmierinošas atbildes uz anketas jautājumiem, ministrija informēs organizāciju, ka gadījumā, ja ministrija no organizācijas nesaņems savlaicīgu un apmierinošu atbildi, ministrija attiecīgā gadījumā nodos lietu attiecīgajai aģentūrai, lai tā veiktu iespējamas izpildes panākšanas darbības. Ministrija informēs organizāciju, izmantojot kontaktinformāciju, ko organizācija norādījusi ministrijai, vai vajadzības gadījumā izmantojot citus piemērotus līdzekļus. Ja organizācija nesniegs savlaicīgu un apmierinošu atbildi, ministrija *ex officio* nodos lietu *FTC*, *DoT* vai citai atbilstošai izpildes aģentūrai vai veiks citus atbilstošus pasākumus, lai nodrošinātu atbilstību. Attiecīgā gadījumā ministrija par šādām atbilstības pārbaudēm konsultēsies ar kompetentajām datu aizsardzības iestādēm, un

— ministrija periodiski izvērtēs datu privātuma regulējuma programmas pārvaldību un uzraudzību, lai nodrošinātu, ka tā uzraudzības pasākumi – arī jebkādi šādi pasākumi, ko veic, izmantojot meklēšanas rīkus (piemēram, lai pārbaudītu, vai nav bojātas saites uz ES un ASV DPR organizāciju privātuma politikas dokumentiem) – ir piemēroti, lai risinātu esošās problēmas un jebkuras jaunas problēmas, kad tādas rodas.

Datu privātuma regulējuma tīmekļa vietnes pielāgošana konkrētām mērķauditorijas grupām

Ministrija pielāgos Datu privātuma regulējuma tīmekļa vietni šādām mērķauditorijām: ES fiziskām personām, ES uzņēmumiem, ASV uzņēmumiem un DAI. Iekļaujot vietnē tieši ES fiziskām personām un ES uzņēmumiem paredzētus materiālus, vairākos veidos tiks veicināta pārredzamība. Attiecībā uz ES fiziskām personām tīmekļa vietnē tiks skaidri izskaidrota šāda informācija: 1) tiesības, ko ES un ASV DPR nodrošina ES fiziskām personām; 2) tiesību aizsardzības mehānismi, kas pieejami ES fiziskām personām, ja viņas uzskata, ka kāda organizācija ir pārkāpusi savas DPR principu ievērošanas saistības; un 3) kā atrast informāciju par organizācijas ES un ASV DPR pašsertifikāciju. Attiecībā uz ES uzņēmumiem tā veicinās šādas informācijas pārbaudi: 1) vai organizācija ir ES un ASV DPR dalībniece; 2) informācijas veids, uz kuru attiecas organizācijas ES un ASV DPR pašsertifikācija; 3) attiecīgajai informācijai piemērotā privātuma politika; un 4) metode, ko organizācija izmanto, lai pārbaudītu, kā tā ievēro DPR principus. Attiecībā uz ASV uzņēmumiem tajā būs skaidri paskaidrota šāda informācija: 1) dalības ES un ASV DPR priekšrocības; 2) kā pievienoties ES un ASV DPR un kā veikt atkārtotu sertifikāciju un izstāties no ES un ASV DPR; un 3) kā ASV pārvalda ES un ASV DPR un panāk tā noteikumu izpildi. Iekļaujot materiālus, kas paredzēti tieši DAI (piemēram, informāciju par ministrijas īpašo kontaktpunktu saziņai ar DAI un hipersaiti uz *FTC* tīmekļa vietnes saturu, kas saistīts ar DPR principiem), tiks veicināta gan sadarbība, gan pārredzamība. Ministrija arī uz *ad hoc* pamata sadarbosies ar Komisiju un Eiropas Datu aizsardzības kolēģiju ("EDAK"), lai izstrādātu papildu tematiskus materiālus (piemēram, atbildes uz bieži uzdotajiem jautājumiem) izmantošanai datu privātuma regulējuma tīmekļa vietnē, ja šāda informācija veicinātu datu privātuma regulējuma programmas efektīvu pārvaldību un uzraudzību.

Sadarbības ar DAI veicināšana

Lai palielinātu iespējas sadarboties ar DAI, ministrija, pirmkārt, uzturēs īpašu kontaktpunktu, kas koordinēs sadarbību ar DAI. Ja DAI uzskatīs, ka kāda ES un ASV DPR organizācija neievēro principus, arī no ES iedzīvotājiem saņemtu sūdzību gadījumos, DAI varēs vērsties pie ministrijas īpašā kontaktpunkta un nodot informāciju par organizāciju turpmākai pārbaudei. Tā, cik vien iespējams, centīsies sekmēt sūdzības risināšanu ar ES un ASV DPR organizāciju. Ministrija 90 dienu laikā no sūdzības saņemšanas sniegs DAI jaunāko informāciju. Īpašais kontaktpunkts saņems arī pieprasījumus par organizācijām, kuras nepatiesi apgalvo, ka piedalās ES un ASV DPR. Īpašais kontaktpunkts reģistrēs visus ministrijai iesniegtos DAI pieprasījumus, un ministrija turpmāk aprakstītajā kopīgajā pārskatā sniegs ziņojumu, kurā apkopotā veidā analizēs katru gadu saņemtās sūdzības. Īpašais kontaktpunkts palīdzēs DAI, kas meklē informāciju saistībā ar konkrētas organizācijas pašsertifikāciju vai iepriekšēju dalību ES un ASV DPR, un īpašais kontaktpunkts atbildēs uz DAI pieprasījumiem par konkrētu ES un ASV DPR prasību īstenošanu. Ministrija sadarbosies ar Komisiju un EDAU arī saistībā ar procesuālajiem un administratīvajiem aspektiem, kas attiecas uz DAI komisiju, tajā skaitā izveidojot piemērotas procedūras to līdzekļu sadalei, kas iekasēti DAI komisijas maksas veidā. Mēs saprotam, ka Komisija sadarbosies ar ministriju, lai veicinātu jebkuru jautājumu risināšanu, kas var rasties saistībā ar šīm procedūrām. Turklāt ministrija nodrošinās DAI materiālus par ES un ASV DPR, lai tās šos materiālus varētu ievietot savās tīmekļa vietnēs un tādējādi palielinātu pārredzamību ES fiziskajām personām un ES uzņēmumiem. Lielākai informētībai par ES un ASV DPR un no tā izrietošajām tiesībām un pienākumiem vajadzētu veicināt problēmu konstatēšanu uzreiz pēc to rašanās un tādējādi to atbilstošu risināšanu.

Saistību pildīšana saskaņā ar DPR principu I pielikumu

Ministrija pildīs savas saistības saskaņā ar DPR principu I pielikumu, tajā skaitā uzturēs to šķīrējtiesnešu sarakstu, kas kopā ar Komisiju izvēlēti, ņemot vērā to neatkarību, godprātību un kompetenci, un vajadzības gadījumā atbalstīs trešās personas, ko ministrija izvēlējusies, lai pārvaldītu šķīrējtiesas procesus saskaņā ar DPR principu I pielikumā norādīto šķīrējtiesas fondu un vadītu to ([3]). Ministrija sadarbosies ar attiecīgo trešo personu, lai cita starpā pārbaudītu, vai trešā persona uztur tīmekļa vietni, kurā sniegti norādījumi par šķīrējtiesas procesu, tajā skaitā šāda informācija: 1) kā uzsākt šķīrējtiesas procesu un iesniegt dokumentus; 2) ministrijas uzturētais šķīrējtiesnešu saraksts un apraksts par to, kā izvēlēties šķīrējtiesnešus no šā saraksta; 3) reglamentējošās šķīrējtiesas procedūras un šķīrējtiesnešu rīcības kodekss, ko pieņēmusi ministrija un Komisija ([4]); un 4) informācija par šķīrējtiesnešu honorāru iekasēšanu un apmaksu. Turklāt ministrija sadarbosies ar trešo personu, lai periodiski pārskatītu šķīrējtiesas fonda darbību, tajā skaitā nepieciešamību pielāgot iemaksu vai šķīrējtiesas procesa izmaksu robežvērtību (t. i., maksimālo summu) apmēru, un cita starpā izskatīs šķīrējtiesas procesu skaitu, izmaksas un ilgumu, saprotot, ka nevajadzētu radīt ES un ASV DPR organizācijām pārmērīgu finansiālo slogu. Ministrija informēs Komisiju par šādu pārskatīšanu ar trešo personu rezultātiem un sniegs Komisijai iepriekšēju paziņojumu par jebkādām iemaksu summas korekcijām.

ES un ASV DPR darbības kopīga pārskatīšana

Ministrija un citas aģentūras vajadzības gadījumā periodiski rīkos sanāksmes ar Komisiju, ieinteresētajām DAI un attiecīgajiem EDAU pārstāvjiem, kurās ministrija sniegs jaunāko informāciju par ES un ASV DPR. Sanāksmēs tiks apspriesti aktuālie jautājumi, kas saistīti ar datu privātuma regulējuma programmas darbību, īstenošanu, uzraudzību un izpildi. Attiecīgā gadījumā sanāksmēs var apspriest saistītus tematus, piemēram, citus datu nosūtīšanas mehānismus, kuriem piemēro ES un ASV DPR.

([3]) Ministrija izvēlējās Starptautisko strīdu izšķiršanas centru (“*ICDR*”), Amerikas Šķīrējtiesu asociācijas (“*AAA*”) starptautisko nodaļu (tālāk “*ICDR AAA*”), lai pārvaldītu šķīrējtiesas procesus saskaņā ar DPR principu I pielikumu un vadītu minētajā pielikumā norādīto šķīrējtiesas fondu.

([4]) 2017. gada 15. septembrī ministrija un Komisija vienojās pieņemt šķīrējtiesas noteikumus, kas reglamentē saistošās šķīrējtiesas procedūras, kuras aprakstītas DPR principu I pielikumā, kā arī šķīrējtiesnešu rīcības kodeksu, kas atbilst vispārpieņemtajiem komerciālo šķīrējtiesnešu ētikas standartiem un DPR principu I pielikumam. Ministrija un Komisija vienojās pielāgot šķīrējtiesas noteikumus un rīcības kodeksu, lai atspoguļotu ES un ASV DPR atjauninājumus, un ministrija sadarbosies ar *ICDR AAA*, lai tos īstenotu.

Tiesību aktu atjaunināšana

Ministrija darīs visu iespējamo, lai informētu Komisiju par būtiskām izmaiņām Amerikas Savienoto Valstu tiesību aktos, ciktāl tās ir relevantas ES un ASV DPR datu privātuma aizsardzības jomā, kā arī par ierobežojumiem un garantijām, kas piemērojami ASV iestāžu piekļuvei personas datiem un to turpmākai izmantošanai.

ASV valdības piekļuve personas datiem

Amerikas Savienotās Valstis ir izdevušas Izpildrīkojumu Nr. 14086 "Drošības pasākumu uzlabošana Amerikas Savienoto Valstu sakaru izlūkošanas darbībām" un *CFR* 28. sadaļas 201. daļu, ar ko groza Tieslietu ministrijas noteikumus ar mērķi izveidot Datu aizsardzības pārskatīšanas tiesu ("*DPRC*"), kas nodrošina stingru personas datu aizsardzību attiecībā uz valdības piekļuvi datiem nacionālās drošības nolūkos. Nodrošinātā aizsardzība ietver šādas darbības: privātuma un pilsonisko brīvību garantiju stiprināšana, lai nodrošinātu, ka ASV sakaru izlūkošanas darbības ir nepieciešamas un samērīgas, lai sasniegtu noteiktos nacionālās drošības mērķus, jauna tiesiskās aizsardzības mehānisma ar neatkarīgām un saistošām pilnvarām izveide un pašreizējās stingrās un daudzlīmeņu pārraudzības uzlabošana attiecībā uz ASV sakaru izlūkošanas darbībām. Izmantojot šos aizsardzības pasākumus, fiziskas personas no ES var vērsties pēc tiesiskās aizsardzības pie jauna daudzlīmeņu tiesiskās aizsardzības mehānisma, kas ietver neatkarīgu *DPRC*, kuras sastāvā būtu personas, kas izraudzītas ārpus ASV valdības un kurām būtu pilnīgas pilnvaras iztiesāt sūdzības un vajadzības gadījumā noteikt koriģējošus pasākumus. Ministrija reģistrēs fiziskas personas no ES, kas iesniedz kvalificētu sūdzību saskaņā ar Izpildrīkojumu Nr. 14086 un *CFR* 28. sadaļas 201. daļu. Piecus gadus pēc šīs vēstules sagatavošanas dienas un pēc tam reizi piecos gados ministrija sazināsies ar attiecīgajām aģentūrām par to, vai ir deklasificēta informācija, kas attiecas uz kvalificētu sūdzību izskatīšanu vai jebkādu *DPRC* iesniegto pārbaudes pieteikumu izskatīšanu. Ja šāda informācija būs deklasificēta, ministrija sadarbosies ar attiecīgo DAI, lai informētu konkrēto fizisko personu no ES. Šie uzlabojumi ir par apliecinājumu tam, ka ES personas dati, kas nosūtīti uz Amerikas Savienotajām Valstīm, tiks apstrādāti saskaņā ar ES tiesību aktu prasībām attiecībā uz valdības piekļuvi datiem.

Pamatojoties uz DPR principiem, Izpildrīkojumu Nr. 14086, *CFR* 28. sadaļas 201. daļu un pievienotajām vēstulēm un materiāliem – arī ministrijas saistībām attiecībā uz datu privātuma regulējuma programmas pārvaldību un uzraudzību –, mēs ceram, ka Komisija noteiks, ka ES un ASV DPR nodrošina pietiekamu aizsardzību atbilstoši ES tiesību aktiem un ka turpināsies datu nosūtīšana no Eiropas Savienības uz organizācijām, kas ir ES un ASV DPR dalībnieces. Mēs arī ceram, ka minētā regulējuma nosacījumi vēl vairāk atvieglos datu nosūtīšanu ASV organizācijām, kas veikta, pamatojoties uz ES līguma standartklauzulām vai ES saistošajiem uzņēmuma noteikumiem.

Ar cieņu

Marisa Lago

Marisa LAGO

*IV PIELIKUMS*

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

Office of the Chair

2023. gada 9. jūnijā

Tiesiskuma komisāram
Didier Reynders
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Cien. komisār *Didier Reynders*!

Amerikas Savienoto Valstu Federālā tirdzniecības komisija ("FTC") novērtē iespēju izklāstīt savu izpildes panākšanas funkcijas saistībā ar ES un ASV datu privātuma regulējumu ("ES un ASV DPR") principiem. *FTC* jau ievērojamu laiku strādā, lai aizsargātu patērētāju tiesības un privātumu pāri robežām, un esam apņēmušies īstenot šī regulējuma aspektus saistībā ar komerciālo sektoru. *FTC* šādus uzdevumus ir pildījusi kopš 2000. gada saistībā ar ASV un ES "drošības zonas" regulējumu un pavisam nesen – kopš 2016. gada – saistībā ar ES un ASV privātuma vairoga regulējumu ([1]). 2020. gada 16. jūlijā Eiropas Savienības Tiesa ("EST"), balstoties nevis uz komerciāliem principiem, kurus īstenoja *FTC*, bet uz citiem aspektiem, atzina par spēkā neesošu Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību, kas ir ES un ASV privātuma vairoga regulējuma pamatā. Kopš tā laika ASV un Eiropas Komisija ir risinājušas sarunas par ES un ASV datu privātuma regulējumu, lai ņemtu vērā EST nolēmumu.

Rakstu, lai apstiprinātu *FTC* apņemšanos panākt ES un ASV DPR principu stingru izpildi. Mēs apstiprinām savu apņemšanos trīs pamatjomās: 1) pieprasījumu prioritāra izskatīšana un izmeklēšana; 2) rīkojumu pieprasīšana un uzraudzība un 3) sadarbība izpildes panākšanas jomā ar ES datu aizsardzības iestādēm ("DAI").

## I. **Ievads**

### a. ***FTC* darbs privātuma izpildes panākšanas jomā un politikas darbs**

*FTC* ir plašas civiltiesiskās izpildes pilnvaras, lai veicinātu patērētāju aizsardzību un konkurenci komerciālajā jomā. Īstenojot savas patērētāju un to datu aizsardzības pilnvaras, *FTC* panāk plaša tiesību aktu klāsta izpildi, lai aizsargātu patērētāju datu privātumu un drošību. Primārajā tiesību aktā, kura izpildi nodrošina *FTC* (proti, *FTC* likumā), ir aizliegtas "negodīgas" vai

([1]) Priekšsēdētājas *Edith Ramirez* vēstule Eiropas Komisijas tieslietu, patērētāju un dzimumu līdztiesības komisārei *Věra Jourová*, kurā aprakstīti Federālās tirdzniecības komisijas veiktie jaunā ES un ASV privātuma vairoga regulējuma izpildes pasākumi (2016. gada 29. februāris), *pieejama* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. *FTC* arī iepriekš apņēmās īstenot ASV un ES "drošības zonas" programmu. FTC priekšsēdētāja *Robert Pitofsky* vēstule Eiropas Komisijas Iekšējā tirgus ģenerāldirektorāta direktoram *John Mogg* (2000. gada 14. jūlijs), *pieejama*https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Šī vēstule aizstāj iepriekšējās saistības.

"maldinošas" darbības vai prakse, ko veic tirdzniecībā vai kuras to ietekmē ([2]). *FTC* veic arī tādu mērķtiecīgi pieņemtu likumu izpildi, kas aizsargā informāciju, kura attiecas uz veselību, kreditēšanu un citiem finanšu jautājumiem, kā arī bērnu informāciju tiešsaistē, un ir izdevusi noteikumus, ar kuriem īsteno katru no šiem likumiem ([3]).

*FTC* nesen arī īstenojusi vairākas iniciatīvas, lai stiprinātu mūsu darbu privātuma jomā. 2022. gada augustā *FTC* paziņoja, ka apsver noteikumus, lai cīnītos pret kaitējošu komerciālo novērošanu un datu nepietiekamu drošību ([4]). Projekta mērķis ir sagatavot pārliecinošu publisku informāciju par to, vai *FTC* būtu jāizdod noteikumi par komerciālās novērošanas un datu drošības praksi, un par to, kādiem šiem noteikumiem vajadzētu būt. Esam labprāt uzklausījuši ES ieinteresēto personu piezīmes par šo un citām iniciatīvām.

Mūsu "PrivacyCon" konferencēs turpina pulcēties vadošie pētnieki, lai apspriestu jaunākos pētījumus un tendences saistībā ar patērētāju privātumu un datu drošību. Esam arī palielinājuši savas aģentūras spējas sekot līdzi tehnoloģiju attīstībai, kas lielā mērā ir uzmanības centrā mūsu darbam privātuma jomā, veidojot aizvien pieaugošu tehnologu un starpdisciplināru pētnieku komandu. Kā jau zināt, mēs arī paziņojām par kopīgu dialogu ar jums un jūsu kolēģiem Eiropas Komisijā, kas ietver tādu ar privātumu saistītu jautājumu risināšanu kā maldinošās saskarnes un darījumdarbības modeļi, kurus raksturo visaptveroša datu vākšana ([5]). Nesen mēs arī publicējām ziņojumu Kongresam, kurā brīdinājām par kaitējumu, kas saistīts ar mākslīgā intelekta izmantošanu, nolūkā novērst Kongresa konstatētos kaitējuma aspektus tiešsaistē. Šajā ziņojumā tika paustas bažas par neprecizitāti, neobjektivitāti, diskrimināciju un patvaļīgu komerciālu novērošanu ([6]).

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

ES un ASV DPR darbojas plašāka ASV privātuma regulējuma kontekstā, kas arī dažādos veidos aizsargā patērētājus no ES. *FTC* likumā noteiktais aizliegums attiecībā uz negodīgām vai maldinošām darbībām vai praksi neaprobežojas tikai ar ASV patērētāju aizsardzību no ASV uzņēmumiem, jo tas attiecas arī uz tādu praksi, kas 1) rada vai var radīt pamatoti paredzamu kaitējumu Amerikas Savienotajās Valstīs vai 2) ietver būtiskas darbības Amerikas Savienotajās Valstīs. Turklāt *FTC*, aizsargājot ārvalstu patērētājus, var izmantot visus koriģējošos pasākumus, kas ir pieejami vietējo patērētāju aizsardzībai ([7]).

*FTC* īsteno arī citus mērķtiecīgus tiesību aktus, ar kuriem nodrošinātā aizsardzība attiecas arī uz patērētājiem ārpus ASV, piemēram, Bērnu privātuma aizsardzības tiešsaistē likumu ("*COPPA*"). *COPPA* cita starpā ir noteikts, ka uz bērniem vērstu tīmekļa vietņu un tiešsaistes pakalpojumu vai vispārīgai auditorijai paredzētu vietņu operatoriem, kuri apzināti vāc personas datus 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 personas datus no ārvalstu

([2]) 15 U.S.C. § 45(a). *FTC* jurisdikcijā neietilpst krimināltiesību aizsardzības vai nacionālās drošības jautājumi. *FTC* arī nav kompetenta vairumā pārējo valdības darbību. Turklāt *FTC* jurisdikcija attiecībā uz komercdarbībām (cita starpā saistībā ar banku, aviosabiedrību, apdrošināšanas nozares un telekomunikāciju pakalpojumu sniedzēju nodrošinātām pārvadājumu darbībām) ir ierobežota. *FTC* pilnvaras neattiecas arī uz vairumu bezpeļņas organizāciju, taču tai ir jurisdikcija attiecībā uz fiktīvām labdarības vai citām bezpeļņas struktūrām, kas faktiski strādā, lai gūtu peļņu. Tā ir kompetenta arī saistībā ar bezpeļņas organizācijām, kas darbojas, lai nodrošinātu peļņu to locekļiem, kuru mērķis ir peļņa, tajā skaitā sniedzot tiem ievērojamus ekonomiskos ieguvumus. Dažos gadījumos *FTC* jurisdikcija sakrīt ar citu tiesībaizsardzības iestāžu jurisdikciju. Mums ir izveidojušās ciešas darba attiecības ar federālajām un štata iestādēm, un mēs cieši sadarbojamies ar tām, lai koordinētu izmeklēšanu vai vajadzības gadījumā nosūtītu lietas izskatīšanai.

([3]) Sk. *FTC, Privacy and Security*, https://www.ftc.gov/business-guidance/privacy-security.

([4]) *Sk.* paziņojumu presei *Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022)*, https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) *Sk.* Eiropas Komisijas tieslietu komisāra *Didier Reynders* un ASV Federālās tirdzniecības komisijas priekšsēdētājas *Lina Khan*kopīgo paziņojumu presei (2022. gada 30. marts), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) Sk.*Press Release, Fed. Trade Comm'n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (June 16, 2022)*, https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) 15 U.S.C. § 45(a)(4)(B). Turklāt "negodīgas vai maldinošas darbības vai prakse" ietver tādas darbības vai praksi, kas saistīta ar ārējo tirdzniecību un i) rada vai var radīt pamatoti paredzamu kaitējumu Amerikas Savienotajās Valstīs vai ii) ietver būtiskas darbības Amerikas Savienotajās Valstīs. 15 U.S.C. § 45(a)(4)(A).

bērniem, ir jāatbilst *COPPA* prasībām. *COPPA* prasībām ir jāatbilst arī ārvalstīs bāzētām vietnēm un tiešsaistes pakalpojumiem, ja tie ir vērsti uz bērniem Amerikas Savienotajās Valstīs vai ar tiem apzināti vāc personas datus no bērniem, kuri dzīvo Amerikas Savienotajās Valstīs. Turklāt papildus ASV federālajiem tiesību aktiem, kuru izpildi panāk *FTC*, ES patērētājus var aizsargāt arī citi federālie un štatu patērētāju tiesību aizsardzības, datu aizsardzības pārkāpumu un privātuma tiesību akti.

c. ***FTC* veiktās izpildes panākšanas darbības**

*FTC* ierosināja lietas gan saskaņā ar ASV un ES "drošības zonas", gan ES un ASV privātuma vairoga regulējumiem un turpināja īstenot ES un ASV privātuma vairoga regulējumu pat pēc tam, kad Eiropas Savienības Tiesa atzina par spēkā neesošu lēmumu par ES un ASV privātuma vairoga regulējuma nodrošinātā aizsardzības līmeņa pietiekamību ([8]). Vairākās no *FTC* nesen iesniegtajām sūdzībām ir iekļauti apgalvojumi par to, ka uzņēmumi ir pārkāpuši ES un ASV privātuma vairoga noteikumus, tajā skaitā procesos pret *Twitter,* ([9]) *CafePress* ([10]) un *Flo* ([11]). *FTC* izpildes panākšanas prasībā pret *Twitter* no *Twitter* piedzina 150 miljonus USD par iepriekšēja *FTC* rīkojuma pārkāpšanu, jo tā prakse ietekmēja vairāk nekā 140 miljonus klientu, tostarp pārkāpa ES un ASV privātuma vairoga 5. principu (datu integritāte un nolūka ierobežojumi). Turklāt aģentūras rīkojumā ir noteikts, ka *Twitter* ir jāļauj lietotājiem izmantot drošas daudzfaktoru autentifikācijas metodes, kas neprasa lietotājiem norādīt savu tālruņa numuru.

*CafePress* lietā *FTC* apgalvoja, ka uzņēmums nespēja aizsargāt patērētāju sensitīvo informāciju, slēpa lielu datu aizsardzības pārkāpumu un pārkāpa ES un ASV privātuma vairoga 2. (izvēle), 4. (drošība) un 6. (piekļuve) principu. *FTC* rīkojumā noteikts, ka uzņēmumam jāaizstāj nepiemēroti autentifikācijas pasākumi ar daudzfaktoru autentifikāciju, būtiski jāierobežo tā savākto un paturēto datu apjoms, jāšifrē sociālā nodrošinājuma numuri, kā arī jāpanāk, lai trešā persona novērtē uzņēmuma informācijas drošības programmas un iesniedz *FTC* to publiskojamu kopiju.

*Flo* lietā *FTC* apgalvoja, ka auglības sekošanas lietotne atklāja lietotāju veselības informāciju trešajām personām – datu analīzes pakalpojumu sniedzējiem – pēc tam, kad uzņēmums bija paudis solījumu saglabāt šīs informācijas privātumu. *FTC* sūdzībā konkrēti norādīts uz uzņēmuma mijiedarbību ar ES patērētājiem un to, ka *Flo* ir pārkāpis ES un ASV privātuma vairoga 1. (paziņošana), 2. (izvēle), 3. (atbildība par tālāku nosūtīšanu) un 5. (datu integritāte un nolūka ierobežojumi) principu. Aģentūras rīkojumā cita starpā noteikts, ka *Flo* ir jāinformē skartie lietotāji par viņu personas datu izpaušanu un jāuzdod visām trešajām personām, kas ir saņēmušas lietotāju veselības informāciju, iznīcināt šos datus. Jāuzsver, ka *FTC* rīkojumi nodrošina aizsardzību visiem attiecīgā ASV uzņēmuma klientiem neatkarīgi no to atrašanās vietas, nevis tikai tiem, kuri ir iesnieguši sūdzības.

Daudzās iepriekšējās ASV un ES "drošības zonas" un ES un ASV privātuma vairoga izpildes panākšanas lietās bija iesaistītas organizācijas, kas bija pabeigušas sākotnējo pašsertifikāciju Tirdzniecības ministrijā, bet neveica ikgadējo atkārtoto pašsertifikāciju, lai gan turpināja norādīt, ka joprojām ir attiecīgā regulējuma dalībnieki. Citas lietas bija saistītas ar nepatiesiem apgalvojumiem par dalību, ko sniedza organizācijas, kuras nekad nebija veikušas sākotnējo pašsertifikāciju Tirdzniecības ministrijā. Raugoties nākotnē, mēs plānojam arī turpmāk koncentrēt savus proaktīvos izpildes panākšanas centienus uz apgalvojumiem par būtiskiem ES un ASV DPR principu pārkāpumiem, kas minēti tādās lietās kā *Twitter, CafePress* un *Flo*. Tikmēr Tirdzniecības ministrija pārvaldīs un uzraudzīs pašsertifikācijas procesu, uzturēs ES un ASV DPR dalībnieku autoritatīvu sarakstu un risinās citus jautājumus, kas saistīti ar pretendēšanu uz dalību programmā ([12]). Svarīgi ir tas, ka uz organizācijām, kas pretendē uz dalību ES un ASV DPR, var attiecināt ES un ASV DPR principu materiāltiesisko izpildi pat tad, ja tās nav veikušas vai neuztur to pašsertifikāciju Tirdzniecības ministrijā.

([8]) *FTC* "drošības zonas" un privātuma vairoga jautājumu sarakstu sk. A pielikumā.

([9]) Sk. *Press Release, Fed. Trade Comm'n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (May 25, 2022)*, https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) Sk. *Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (March 15, 2022)*, https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) Sk. *Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021)*, https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Tirdzniecības ministra vietnieces starptautiskās tirdzniecības jautājumos *Marisa Lago* vēstule Eiropas Komisijas tieslietu komisāram *Didier Reynders*.

## II. **Pieprasījumu prioritāra izskatīšana un izmeklēšana**

Gluži kā tas tika darīts saskaņā ar ASV un ES "drošības zonas" regulējumu un ES un ASV privātuma vairoga regulējumu, *FTC* apņemas no Tirdzniecības ministrijas un ES dalībvalstīm saņemtos pieprasījumus par atbilstību ES un ASV DPR principiem izskatīt prioritārā kārtā. Mēs arī piešķirsim prioritāti ar privātumu saistītu pašregulējuma struktūru un citu neatkarīgu strīdu izšķiršanas struktūru iesniegtajiem pieprasījumiem par ES un ASV DPR principu neievērošanu.

Lai sekmētu ES dalībvalstu iesniegto ar ES un ASV DPR saistīto pieprasījumu izskatīšanu, *FTC* ir izveidojusi standartizētu pieprasījumu procesu un sniegusi ES dalībvalstīm norādes par to, kāda informācija *FTC* visvairāk noderētu pieprasījuma izpētē. Īstenojot šos centienus, *FTC* ir iecēlusi aģentūras kontaktpunktu, pie kura ES dalībvalstis varēs vērsties saistībā ar pieprasījumiem. Ir ļoti noderīgi, ja pieprasījuma iesniedzēja iestāde ir veikusi sākotnēju iespējamā pārkāpuma izpēti un var sadarboties ar *FTC* izmeklēšanā.

Saņemot šādu pieprasījumu no Tirdzniecības ministrijas, ES dalībvalsts vai pašregulējuma organizācijas, vai citām neatkarīgām strīdu izšķiršanas struktūrām, *FTC* var īstenot dažādas izvirzīto jautājumu risināšanas darbības. Mēs varam, piemēram, pārskatīt organizācijas privātuma politiku, iegūt papildu informāciju tieši no organizācijas 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 būtu lietderīgi veikt papildu pasākumus, lai informētu tirgus dalībniekus, un vajadzības gadījumā uzsākt izpildes procedūru.

Papildus prioritāšu piešķiršanai tādiem pieprasījumiem par neatbilstību ES un ASV DPR principiem, kas saņemti Tirdzniecības ministrijas, ES dalībvalstīm un privātuma pašregulējuma organizācijām vai citām neatkarīgām strīdu izšķiršanas struktūrām ([13]), *FTC* turpinās izmeklēt būtiskus ES un ASV DPR principu pārkāpumus pēc savas iniciatīvas un vajadzības gadījumā izmantos dažādus instrumentus. Īstenojot *FTC* programmu tādu privātuma un drošības jautājumu izmeklēšanai, kas saistīti ar komerciālām organizācijām, aģentūra regulāri pārbauda, vai attiecīgā struktūra ir sniegusi ES un ASV privātuma vairoga apliecinājumus. Ja uzņēmums bija sniedzis šādus apliecinājumus un izmeklēšanā tika atklāti acīmredzami ES un ASV privātuma vairoga principu pārkāpumi, *FTC* savās izpildes panākšanas darbībās iekļāva pieņēmumus par ES un ASV privātuma vairoga principu pārkāpumiem. Mēs turpināsim šo proaktīvo pieeju arī attiecībā uz ES un ASV DPR principiem.

## III. **Rīkojumu pieprasīšana un uzraudzība**

*FTC* arī apstiprina savu apņemšanos turpināt pieprasīt izpildes rīkojumus un uzraudzīt to īstenošanu, lai nodrošinātu atbilstību ES un ASV DPR principiem. Mēs pieprasīsim ES un ASV DPR principu ievērošanu, izmantojot dažādus atbilstošus aizliedzošus noteikumus turpmākajos *FTC* rīkojumos saistībā ar ES un ASV DPR principu ievērošanu. Par *FTC* administratīvo rīkojumu pārkāpšanu var piespriest civiltiesisku sodu līdz 50 120 USD par pārkāpumu vai līdz 50 120 USD par pārkāpuma turpināšanas dienu ([14]) – ja attiecīgā prakse ietekmē lielu skaitu patērētāju, 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. Rīkojumi jāizplata arī darbiniekiem, kas ir atbildīgi par rīkojumu izpildes nodrošināšanu.

*FTC*, tāpat kā saistībā ar visiem tās rīkojumiem, sistemātiski uzrauga, kā tiek ievēroti arī spēkā esošie rīkojumi par ES un ASV privātuma vairoga principu ievērošanu, un, ja nepieciešams, ierosina prasības par to izpildi ([15]). Jāuzsver, ka *FTC* rīkojumi arī turpmāk nodrošinās aizsardzību visiem attiecīgā uzņēmuma klientiem neatkarīgi no to atrašanās vietas, nevis tikai tiem, kuri ir iesnieguši sūdzības. Visbeidzot, *FTC* tiešsaistē uzturēs to uzņēmumu sarakstu, uz kuriem attiecas rīkojumi, kas saņemti saistībā ar ES un ASV DPR principu izpildi ([16]).

([13]) Lai gan *FTC* nerisina individuālas patērētāju sūdzības un nedarbojas kā šādu sūdzību izskatīšanas vidutājs, tā apstiprina, ka prioritāri izskatīs ar ES un ASV DPR principiem saistītos ES DAI pieprasījumus. Turklāt *FTC*, 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. Fiziskas personas no ES, izmantojot to pašu sūdzību sistēmu, kas ir pieejama patērētājiem ASV, var iesniegt sūdzību *FTC* tīmekļa vietnē https://reportfraud.ftc.gov/. Tomēr, ja fiziskām personām no ES ir individuālas ar ES un ASV DPR saistītas sūdzības, iespējams, visnoderīgāk būtu iesniegt tās savas dalībvalsts DAI vai neatkarīgai strīdu izšķiršanas struktūrai.

([14]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Šo summu periodiski koriģē atbilstoši inflācijai.

([15]) Pagājušajā gadā *FTC* nobalsoja par atkārtotu pārkāpumu izmeklēšanas procesa racionalizēšanu. Sk.*Press Release, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (Jul. 1, 2021)*, https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) Sal. ar *FTC, Privacy Shield* , https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Sadarbība izpildes jomā ar ES DAI**

*FTC* atzīst, ka ES DAI var būt liela nozīme attiecībā uz ES un ASV DPR principu ievērošanu, un mudina paplašināt apspriešanos un sadarbību izpildes jomā. Patiešām – koordinēta pieeja pašreizējās digitālā tirgus attīstības un datu ziņā ietilpīgu darījumdarbības modeļu radīto problēmu risināšanai kļūst arvien svarīgāka. *FTC*, ievērojot konfidencialitātes tiesību aktus un ierobežojumus, apmainīsies ar pieprasījuma iesniedzējām izpildes iestādēm ar attiecīgu informāciju, arī par pieprasījumu statusu. Ciktāl praksē iespējams un atkarībā no saņemto pieprasījumu skaita un veida, sniegtajā informācijā tiks iekļauts pieprasījumā norādīto aspektu novērtējums, tajā skaitā aprakstīti būtiski izvirzītie jautājumi un visas darbības, kas veiktas, lai reaģētu uz tiesību aktu pārkāpumiem, kuri ir *FTC* jurisdikcijā. Lai palielinātu nelikumīgas rīcības apkarošanas centienu rezultativitāti, *FTC* arī sniegs pieprasījuma iesniedzējai iestādei atsauksmes par saņemto pieprasījumu veidiem. Ja pieprasījuma iesniedzēja izpildes iestāde vēlas saņemt informāciju par konkrēta pieprasījuma statusu, lai izpildes procesu īstenotu pati, *FTC* atbildēs, ņemot vērā izskatīto pieprasījumu daudzumu un ievērojot konfidencialitātes un citas juridiskās prasības.

*FTC* arī cieši sadarbosies ar ES DAI ar mērķi sniegt tām ar izpildes panākšanu saistītu palīdzību. Attiecīgos gadījumos tas varētu ietvert informācijas apmaiņu un palīdzību izmeklēšanā atbilstīgi ASV Tīmekļa drošības likumam (*SAFE WEB Act*), kurā *FTC* ir atļauts palīdzēt citu valstu tiesībaizsardzības aģentūrām tādu tiesību aktu izpildes panākšanā, kuros aizliegtā prakse būtiski līdzinās *FTC* īstenotajos tiesību aktos aizliegtajām darbībām ([17]). Šīs palīdzības satvarā *FTC* var sniegt informāciju, kas iegūta saistībā ar *FTC* 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. *FTC* regulāri izmanto šīs pilnvaras, lai palīdzētu citu pasaules valstu iestādēm privātuma un patērētāju aizsardzības lietu īstenošanā.

Papildus visām apspriedēm ar pieprasījuma iesniedzējām ES DAI par konkrētas lietas aspektiem *FTC* piedalīsies periodiskās sanāksmēs ar norīkotiem Eiropas Datu aizsardzības kolēģijas ("EDAK") pārstāvjiem, lai vispārīgi pārspriestu, kā uzlabot sadarbību izpildes panākšanas jomā. *FTC* arī kopā ar Tirdzniecības ministrijas, Eiropas Komisijas un EDAK pārstāvjiem piedalīsies ES un ASV DPR periodiskā pārskatīšanā, lai apspriestu tā īstenošanu. *FTC* arī mudina izstrādāt instrumentus, kas uzlabotu sadarbību izpildes jomā gan ar ES DAI, gan citām privātuma aizsardzības iestādēm no visas pasaules. *FTC* ar gandarījumu apstiprina savu apņemšanos īstenot ES un ASV DPR komerciālā sektora aspektus. Mēs uzskatām, ka mūsu partnerība ar ES kolēģiem ir ļoti svarīga, lai nodrošinātu privātuma aizsardzību gan mūsu, gan jūsu pilsoņiem.

Ar cieņu

Lina M. KHAN
Federālās tirdzniecības komisijas priekšsēdētāja

([17]) Nosakot, vai īstenot savas pilnvaras, kas izriet no ASV Tīmekļa drošības likuma, *FTC* citustarp izvērtē: "A) vai pieprasījuma iesniedzēja aģentūra ir piekritusi sniegt vai sniegs savstarpēju palīdzību Komisijai; B) vai pieprasījuma izpilde neapdraudētu Amerikas Savienoto Valstu sabiedrības intereses; un C) vai pieprasījuma iesniedzējas 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.

***A papildinājums***

**Privātuma vairoga un "drošības zonas" izpildes pasākumi**

| | **Reģistra/*FTC* dokumenta Nr.** | **Lieta** | **Saite** |
|---|---|---|---|
| | | | |
| 1 | *FTC* dokumenta Nr. 2023062<br>Lieta Nr. 3:22-cv-03070 (N.D. Cal.) | ASV / **Twitter, Inc.** | Twitter |
| 2 | *FTC* dokumenta Nr. 192 3209 | Saistībā ar *Residual Pumpkin Entity, LLC*, iepriekš: **CafePress**, un *PlanetArt, LLC*, iepriekš: **CafePress** | CafePress |
| 3 | *FTC* dokumenta Nr. 192 3133<br>Reģistra dokumenta Nr. C-4747 | Saistībā ar **Flo Health, Inc.** | Flo Health |
| 4 | *FTC* dokumenta Nr. 192 3050<br>Reģistra dokumenta Nr. C-4723 | Saistībā ar **Ortho-Clinical Diagnostics, Inc.** | Ortho-Clinical |
| 5 | *FTC* dokumenta Nr. 192 3092<br>Reģistra dokumenta Nr. C-4709 | Saistībā ar **T&M Protection, LLC** | T&M Protection |
| 6 | *FTC* dokumenta Nr. 192 3084<br>Reģistra dokumenta Nr. C-4704 | Saistībā ar **TDARX, Inc.** | TDARX |
| 7 | *FTC* dokumenta Nr. 192 3093<br>Reģistra dokumenta Nr. C-4706 | Saistībā ar **Global Data Vault, LLC** | Global Data |
| 8 | *FTC* dokumenta Nr. 192 3078<br>Reģistra dokumenta Nr. C-4703 | Saistībā ar **Incentive Services, Inc.** | Incentive Services |
| 9 | *FTC* dokumenta Nr. 192 3090<br>Reģistra dokumenta Nr. C-4705 | Saistībā ar **Click Labs, Inc.** | Click Labs |
| 10 | *FTC* dokumenta Nr. 182 3192<br>Reģistra dokumenta Nr. C-4697 | Saistībā ar **Medable, Inc.** | Medable |
| 11 | *FTC* dokumenta Nr. 182 3189<br>Reģistra dokumenta Nr. 9386 | Saistībā ar *NTT Global Data Centers Americas, Inc.* kā **RagingWire Data Centers, Inc.** tiesību pārņēmēju. | RagingWire |
| 12 | *FTC* dokumenta Nr. 182 3196<br>Reģistra dokumenta Nr. C-4702 | Saistībā ar **Thru, Inc.** | Thru |
| 13 | *FTC* dokumenta Nr. 182 3188<br>Reģistra dokumenta Nr. C-4698 | Saistībā ar **DCR Workforce, Inc.** | DCR Workforce |
| 14 | *FTC* dokumenta Nr. 182 3194<br>Reģistra dokumenta Nr. C-4700 | Saistībā ar **LotaData, Inc.** | LotaData |
| 15 | *FTC* dokumenta Nr. 182 3195<br>Reģistra dokumenta Nr. C-4701 | Saistībā ar **EmpiriStat, Inc.** | EmpiriStat |

| | | | |
|---|---|---|---|
| 16 | *FTC* dokumenta Nr. 182 3193<br>Reģistra dokumenta Nr. C-4699 | Saistībā ar *214 Technologies, Inc.*; darbojas arī kā **Trueface.ai** | Trueface.ai |
| 17 | *FTC* dokumenta Nr. 182 3107<br>Reģistra dokumenta Nr. 9383 | Saistībā ar **Cambridge Analytica, LLC** | Cambridge Analytica |
| 18 | *FTC* dokumenta Nr. 182 3152<br>Reģistra dokumenta Nr. C-4685 | Saistībā ar **SecureTest, Inc.** | SecurTest |
| 19 | *FTC* dokumenta Nr. 182 3144<br>Reģistra dokumenta Nr. C-4664 | Saistībā ar **VenPath, Inc.** | VenPath |
| 20 | *FTC* dokumenta Nr. 182 3154<br>Reģistra dokumenta Nr. C-4666 | Saistībā ar **SmartStart Employment Screening, Inc.** | SmartStart |
| 21 | *FTC* dokumenta Nr. 182 3143<br>Reģistra dokumenta Nr. C-4663 | Saistībā ar **mResourceLLC**; darbojas arī kā *Loop Works LLC* | mResource |
| 22 | *FTC* dokumenta Nr. 182 3150<br>Reģistra dokumenta Nr. C-4665 | Saistībā ar **Idmission LLC** | IDmission |
| 23 | *FTC* dokumenta Nr. 182 3100<br>Reģistra dokumenta Nr. C-4659 | Saistībā ar **ReadyTech Corporation** | ReadyTech |
| 24 | *FTC* dokumenta Nr. 172 3173<br>Reģistra dokumenta Nr. C-4630 | Saistībā ar **Decusoft, LLC** | Decusoft |
| 25 | *FTC* dokumenta Nr. 172 3171<br>Reģistra dokumenta Nr. C-4628 | Saistībā ar **Tru Communication, Inc.** | Tru |
| 26 | *FTC* dokumenta Nr. 172 3172<br>Reģistra dokumenta Nr. C-4629 | Saistībā ar **Md7, LLC** | Md7 |
| 30 | *FTC* dokumenta Nr. 152 3198<br>Reģistra dokumenta Nr. C-4543 | Saistībā ar ***Jhayrmaine Daniels*** **(darbojas arī kā *California Skate-Line*)** | Jhayrmaine Daniels |
| 31 | *FTC* dokumenta Nr. 152 3190<br>Reģistra dokumenta Nr. C-4545 | Saistībā ar **Dale Jarrett Racing Adventure, Inc.** | Dale Jarrett |
| 32 | *FTC* dokumenta Nr. 152 3141<br>Reģistra dokumenta Nr. C-4540 | Saistībā ar **Golf Connect, LLC** | Golf Connect |
| 33 | *FTC* dokumenta Nr. 152 3202<br>Reģistra dokumenta Nr. C-4546 | Saistībā ar **Inbox Group, LLC** | Inbox Group |
| 34 | Dokumenta Nr. 152-3187<br>Reģistra dokumenta Nr. C-4542 | Saistībā ar **IOActive, Inc.** | IOActive |
| 35 | *FTC* dokumenta Nr. 152 3140<br>Reģistra dokumenta Nr. C-4549 | Saistībā ar **Jubilant Clinsys, Inc.** | Jubilant |
| 36 | *FTC* dokumenta Nr. 152 3199<br>Reģistra dokumenta Nr. C-4547 | Saistībā ar **Just Bagels Manufacturing, Inc.** | Just Bagels |

| | | | |
|---|---|---|---|
| 37 | *FTC* dokumenta Nr. 152 3138<br>Reģistra dokumenta Nr. C-4548 | Saistībā ar **NAICS Association, LLC** | NAICS |
| 38 | *FTC* dokumenta Nr. 152 3201<br>Reģistra dokumenta Nr. C-4544 | Saistībā ar **One Industries Corp.** | One Industries |
| 39 | *FTC* dokumenta Nr. 152 3137<br>Reģistra dokumenta Nr. C-4550 | Saistībā ar **Pinger, Inc.** | Pinger |
| 40 | *FTC* dokumenta Nr. 152 3193<br>Reģistra dokumenta Nr. C-4552 | Saistībā ar **SteriMed Medical Waste Solutions** | SteriMed |
| 41 | *FTC* dokumenta Nr. 152 3184<br>Reģistra dokumenta Nr. C-4541 | Saistībā ar **Contract Logix, LLC** | Contract Logix |
| 42 | *FTC* dokumenta Nr. 152 3185<br>Reģistra dokumenta Nr. C-4551 | Saistībā ar **Forensics Consulting Solutions, LLC** | Forensics Consulting |
| 43 | *FTC* dokumenta Nr. 152 3051<br>Reģistra dokumenta Nr. C-4526 | Saistībā ar **American Int'l Mailing, Inc.** | AIM |
| 44 | *FTC* dokumenta Nr. 152 3015<br>Reģistra dokumenta Nr. C-4525 | Saistībā ar **TES Franchising, LLC** | TES |
| 45 | *FTC* dokumenta Nr. 142 3036<br>Reģistra dokumenta Nr. C-4459 | Saistībā ar **American Apparel, Inc.** | American Apparel |
| 46 | *FTC* dokumenta Nr. 142 3026<br>Reģistra dokumenta Nr. C-4469 | Saistībā ar **Fantage.com, Inc.** | Fantage |
| 47 | *FTC* dokumenta Nr. 142 3017<br>Reģistra dokumenta Nr. C-4461 | Saistībā ar **Apperian, Inc.** | Apperian |
| 48 | *FTC* dokumenta Nr. 142 3018<br>Reģistra dokumenta Nr. C-4462 | Saistībā ar **Atlanta Falcons Football Club, LLC** | Atlanta Falcons |
| 49 | *FTC* dokumenta Nr. 142 3019<br>Reģistra dokumenta Nr. C-4463 | Saistībā ar **Baker Tilly Virchow Krause, LLP** | Baker Tilly |
| 50 | *FTC* dokumenta Nr. 142 3020<br>Reģistra dokumenta Nr. C-4464 | Saistībā ar **BitTorrent, Inc.** | BitTorrent |
| 51 | *FTC* dokumenta Nr. 142 3022<br>Reģistra dokumenta Nr. C-4465 | Saistībā ar **Charles River Laboratories, Int'l** | Charles River |
| 52 | *FTC* dokumenta Nr. 142 3023<br>Reģistra dokumenta Nr. C-4466 | Saistībā ar **DataMotion, Inc.** | DataMotion |
| 53 | *FTC* dokumenta Nr. 142 3024<br>Reģistra dokumenta Nr. C-4467 | Saistībā ar **DDC Laboratories, Inc.**; darbojas arī kā *DNA Diagnostics Center* | DDC |
| 54 | *FTC* dokumenta Nr. 142 3028<br>Reģistra dokumenta Nr. C-4470 | Saistībā ar **Level 3 Communications, LLC** | Level 3 |

| | | | |
|---|---|---|---|
| 55 | *FTC* dokumenta Nr. 142 3025<br>Reģistra dokumenta Nr. C-4468 | Saistībā ar **PDB Sports, Ltd.**; darbojas arī kā *Denver Broncos Football Club, LLP* | Broncos |
| 56 | *FTC* dokumenta Nr. 142 3030<br>Reģistra dokumenta Nr. C-4471 | Saistībā ar **Reynolds Consumer Products, Inc.** | Reynolds |
| 57 | *FTC* dokumenta Nr. 142 3031<br>Reģistra dokumenta Nr. C-4472 | Saistībā ar **Receivable Management Services Corporation** | Receivable Mgmt |
| 58 | *FTC* dokumenta Nr. 142 3032<br>Reģistra dokumenta Nr. C-4473 | Saistībā ar **Tennessee Football, Inc.** | Tennessee Football |
| 59 | *FTC* dokumenta Nr. 102 3058<br>Reģistra dokumenta Nr. C-4369 | Saistībā ar **Myspace LLC** | Myspace |
| 60 | *FTC* dokumenta Nr. 092 3184<br>Reģistra dokumenta Nr. C-4365 | Saistībā ar **Facebook, Inc.** | Facebook |
| 61 | *FTC* dokumenta Nr. 092 3081<br>Civilprasība Nr. 09-CV-5276 (C.D. Cal.) | *FTC* / *Javian Karnani* un **Balls of Kryptonite, LLC**, darbojas arī kā *Bite Size Deals, LLC*, un *Best Priced Brands, LLC* | Balls of Kryptonite |
| 62 | *FTC* dokumenta Nr. 102 3136<br>Reģistra dokumenta Nr. C-4336 | Saistībā ar **Google, Inc.** | Google |
| 63 | *FTC* dokumenta Nr. 092 3137<br>Reģistra dokumenta Nr. C-4282 | Saistībā ar **World Innovators, Inc.** | World Innovators |
| 64 | *FTC* dokumenta Nr. 092 3141<br>Reģistra dokumenta Nr. C-4271 | Saistībā ar **Progressive Gaitways LLC** | Progressive Gaitways |
| 65 | *FTC* dokumenta Nr. 092 3139<br>Reģistra dokumenta Nr. C-4270 | Saistībā ar **Onyx Graphics, Inc.** | Onyx Graphics |
| 66 | *FTC* dokumenta Nr. 092 3138<br>Reģistra dokumenta Nr. C-4269 | Saistībā ar **ExpatEdge Partners, LLC** | ExpatEdge |
| 67 | *FTC* dokumenta Nr. 092 3140<br>Reģistra dokumenta Nr. C-4281 | Saistībā ar **Directors Desk LLC** | Directors Desk |
| 68 | *FTC* dokumenta Nr. 092 3142<br>Reģistra dokumenta Nr. C-4272 | Saistībā ar **Collectify LLC** | Collectify |

*V PIELIKUMS*

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

2023. gada 6. jūlijā

Komisāram *Didier Reynders*
European Commission
Rue de la Loi / Wetstraat 200
1049 1049 Brussels
*Belgium*

Cien. komisār *Didier Reynders*!

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

*DoT* pirmo reizi publiski pauda apņemšanos īstenot ASV un ES "drošības zonas" regulējumu Eiropas Komisijai nosūtītā vēstulē pirms vairāk nekā 22 gadiem, un šī apņemšanās tika atkārtota un saistības paplašinātas 2016. gada vēstulē par ES un ASV privātuma vairoga regulējumu. Minētajās vēstulēs *DoT* apņēmās ievērot ASV un ES "drošības zonas" privātuma principus un pēc tam – ES un ASV privātuma vairoga principus. *DoT* šo apņemšanos tagad attiecina arī uz ES un ASV DPR principiem, apliecinot to ar šo vēstuli.

Jo īpaši *DoT* apliecina savu apņemšanos šādās galvenajās jomās: 1) apgalvojumu par ES un ASV DPR principu pārkāpumiem prioritāra izmeklēšana; 2) atbilstošas izpildes panākšanas darbības pret struktūrām, kas sniedz nepatiesus vai maldinošus apgalvojumus par dalību ES un ASV DPR; un 3) izpildes rīkojumu par ES un ASV DPR principu pārkāpumiem uzraudzība un publiskošana. Mēs sniedzam informāciju par katru saistību veidu un, lai ieskicētu kontekstu, attiecīgu pamatinformāciju par *DoT* nozīmi patērētāju privātuma aizsardzībā un ES un ASV DPR principu izpildes panākšanā.

1. **Konteksts**

A. DoT pilnvaras privātuma aizsardzības jomā

Ministrija ir stingri apņēmusies nodrošināt tās informācijas privātumu, ko

aviosabiedrībām un biļešu pārdevējiem sniedz patērētāji. *DoT* pilnvaras rīkoties šajā jomā ir paredzētas 49 U.S.C. 41712. iedaļā, kas aizliedz pārvadātājam vai biļešu pārdevējam iesaistīties "negodīgā vai maldinošā praksē" gaisa pārvadājumu nozarē vai gaisa pārvadājumu pakalpojumu pārdošanas jomā. 41712. iedaļa

ir formulēta, pamatojoties uz Federālās tirdzniecības komisijas likuma (*Federal Trade Commission Act*) 5. pantu (15 U.S.C. 45). Nesen *DoT* izdeva noteikumus, kuros definēta negodīga un maldinoša prakse, kas atbilst gan *DoT*, gan *FTC* precedentam (14 CFR § 399.79). Konkrētāk, rīcība ir "negodīga", ja tā rada vai var radīt būtisku kaitējumu, kas nav pamatoti novēršams un ko nepārsniedz

labums patērētājiem vai konkurencei. Prakse ir "maldinoša" attiecībā uz patērētājiem, ja tā attiecībā uz kādu būtisku jautājumu var maldināt patērētāju, kas rīkojas saprātīgi konkrētajos apstākļos. Jautājums ir būtisks, ja tas varētu būt ietekmējis patērētāja rīcību vai lēmumu attiecībā uz kādu produktu vai pakalpojumu. Papildus šiem vispārīgajiem principiem *DoT* jo īpaši interpretē 41712. iedaļu kā tādu, kas aizliedz pārvadātājiem un biļešu pārdevējiem: 1) pārkāpt to privātuma politikas noteikumus; 2) pārkāpt jebkādus ministrijas izdotus noteikumus, kuros konkrēta privātuma prakse ir atzīta par negodīgu vai maldinošu; vai 3) pārkāpt Bērnu privātuma aizsardzības tiešsaistē likumu (*COPPA*) vai *FTC* noteikumus, ar kuriem īsteno *COPPA*; vai 4) kā ES un ASV DPR dalībniekam neievērot ES un ASV DPR principus ([1]).

Kā jau norādīs iepriekš, saskaņā ar federālajiem tiesību aktiem *DoT* ir ekskluzīvas pilnvaras regulēt aviosabiedrību īstenoto privātuma aizsardzības praksi, un kopā ar *FTC* 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 ES un ASV DPR 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 ES un ASV DPR principus, tos neievērojot, pārvadātājs vai biļešu pārdevējs pārkāptu 41712. iedaļu.

B. Izpildes panākšanas prakse

Ministrijas Aviācijas patērētāju tiesību aizsardzības birojs (*OACP*) ([2]) izmeklē un uztur apsūdzību lietās saskaņā ar 49 U.S.C. 41712. iedaļu. Tas panāk 41712. iedaļā paredzētā negodīgas un maldinošas prakses likumiskā aizlieguma izpildi, galvenokārt ar sarunām, pieņem pretlikumīgas darbības pārtraukšanas rīkojumus, kā arī sagatavo rīkojumus ar civiltiesisku sodu novērtējumu. Par iespējamiem pārkāpumiem birojs lielākoties uzzina no tam iesniegtajām fizisku personu, ceļojumu aģentu, aviosabiedrību, kā arī ASV un ārvalstu valdības aģentūru sūdzībām. Patērētāji var iesniegt ar privātumu saistītas sūdzības par aviosabiedrībām un biļešu pārdevējiem, izmantojot DoT tīmekļa vietni ([3]).

Ja lietā neizdodas panākt saprātīgu un atbilstošu risinājumu, *OACP* ir pilnvaras sākt izpildes procesu ar pierādījumu izskatīšanu, ko veic *DoT* administratīvo tiesību tiesnesis ("ATT"). ATT ir pilnvarots pieņemt pretlikumīgas darbības pārtraukšanas rīkojumus un piespriest civiltiesiskus sodus. 41712. iedaļas pārkāpumu rezultātā var tikt pieņemti pretlikumīgas darbības pārtraukšanas rīkojumi un piemēroti civiltiesiski sodi līdz 37 377 USD apmērā par katru 41712. iedaļas pārkāpumu.

Ministrijai nav pilnvaru pieņemt lēmumu par kaitējuma atlīdzināšanu vai finansiālu kompensāciju individuāliem sūdzību iesniedzējiem. Tomēr tā var apstiprināt izlīgumus, kas izriet no *OACP* 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 ES un ASV DPR 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 *DoT* 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. DoT 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. *DoT* 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. *DoT* 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.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Iepriekš pazīstams kā Birojs aviācijas tiesībaizsardzības un procesuālajos jautājumos (*Office of Aviation Enforcement and Proceedings*).
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

*DoT* attiecībā uz aviosabiedrībām īsteno arī citus mērķtiecīgus tiesību aktus, ar kuriem nodrošinātā aizsardzība attiecas arī uz patērētājiem ārpus ASV, piemēram, Bērnu privātuma aizsardzības tiešsaistē likumu ("*COPPA*"). *COPPA* cita starpā ir noteikts, ka uz bērniem vērstu tīmekļa vietņu un tiešsaistes pakalpojumu vai vispārīgai auditorijai paredzētu vietņu operatoriem, kuri apzināti vāc personas datus 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 personas datus no ārvalstu bērniem, ir jāatbilst *COPPA* prasībām. *COPPA* prasībām ir jāatbilst arī ārvalstīs bāzētām vietnēm un tiešsaistes pakalpojumiem, ja tie ir vērsti uz bērniem Amerikas Savienotajās Valstīs vai ar tiem apzināti vāc personas datus no bērniem, kuri dzīvo Amerikas Savienotajās Valstīs. *DoT* ir pilnvarota veikt izpildes panākšanas darbības attiecībā uz *COPPA* pārkāpumiem, ko izdarījušas ASV vai ārvalstu aviosabiedrības, kuras veic uzņēmējdarbību Amerikas Savienotajās Valstīs.

## II. **ES un ASV DPR principu izpildes panākšana**

Ja aviosabiedrība vai biļešu pārdevējs ir nolēmis piedalīties ES un ASV DPR īstenošanā un ministrija saņem sūdzību, kurā apgalvots, ka attiecīgā aviosabiedrība vai biļešu pārdevējs ir pārkāpis ES un ASV DPR principus, ministrija, lai panāktu ES un ASV DPR principu stingru ievērošanu, veiks tālāk uzskaitītās darbības.

### A. Iespējamo pārkāpumu prioritāra izmeklēšana

Ministrijas *OACP* izmeklēs katru sūdzību, kas ietver apgalvojumus par ES un ASV DPR principu

pārkāpumiem, arī no ES datu aizsardzības iestādēm ("DAI") saņemtas sūdzības, un, ja konstatēs pārkāpumu pierādījumus, veiks izpildes panākšanas darbības. *OACP* arī sadarbosies ar *FTC* un Tirdzniecības ministriju un prioritārā kārtībā izskatīs apgalvojumus par regulētām struktūrām, kuras neievēro privātuma saistības, ko uzņēmušās attiecībā uz ES un ASV DPR.

Ja tiek saņemti apgalvojumi par ES un ASV DPR principu pārkāpumu, *OACP* 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 novērtēt, vai pastāv pārkāpumu pazīmes un vai ir ietekmēts liels patērētāju skaits. Turklāt birojs noteiktu, vai sūdzībā aplūkotie jautājumi nav Tirdzniecības ministrijas vai *FTC* kompetencē, novērtētu, vai noderētu patērētāju un uzņēmumu izglītošana, un attiecīgā gadījumā sāktu izpildes procesu.

Ja ministrija uzzinās par iespējamu ES un ASV DPR principu pārkāpumu, ko izdarījuši biļešu pārdevēji, tā saskaņos rīcību ar *FTC*. Mēs arī informēsim *FTC* un Tirdzniecības ministriju par visu ES un ASV DPR principu izpildes panākšanas darbību iznākumu.

### B. Reaģēšana uz nepatiesiem vai maldinošiem apgalvojumiem par dalību DPR

Ministrija joprojām ir apņēmusies izmeklēt ES un ASV DPR principu pārkāpumus, tajā skaitā nepatiesus vai maldinošus apgalvojumus par dalību ES un ASV DPR. Mēs prioritāri izskatīsim Tirdzniecības ministrijas pieprasījumus par organizācijām, kas, kā uzskata ministrija, nepamatoti uzdodas par ES un ASV DPR dalībniecēm vai bez atļaujas izmanto ES un ASV DPR sertifikācijas zīmi.

Turklāt jānorāda, ka, ja organizācijas privātuma politikā ir apgalvots, ka tā ievēro ES un ASV DPR principus, tomēr nav veikusi vai neuztur pašsertifikāciju Tirdzniecības ministrijā, šis fakts vien, visticamāk, neatbrīvos organizāciju no *DoT* centieniem panākt attiecīgo saistību izpildi.

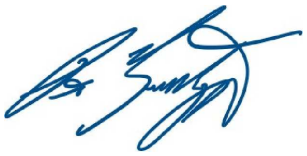
### C. Par ES un ASV DPR pārkāpumiem pieņemto izpildes rīkojumu uzraudzība un publiskošana

Lai nodrošinātu ES un ASV DPR ievērošanu, ministrijas *OACP* joprojām ir apņēmies vajadzības gadījumā uzraudzīt izpildes rīkojumu īstenošanu. Konkrētāk, ja birojs izdod rīkojumu, ar aviosabiedrībai vai biļešu pārdevējam liek izbeigt pretlikumīgu darbību un nepieļaut turpmākus ES un ASV DPR un 41712. iedaļas pārkāpumus, tas uzraudzīs, vai attiecīgā struktūra ievēro rīkojuma noteikumu par pretlikumīgās darbības izbeigšanu. Birojs arīdzan nodrošinās par lietām, kas saistītas ar ES un ASV DPR principu neievērošanu, pieņemto rīkojumu pieejamību tā tīmekļa vietnē.

Mēs labprāt turpināsim sadarboties ar mūsu federālajiem partneriem un ES ieinteresētajām personām ar ES un ASV DPR 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



Pete BUTTIGIEG

***VI PIELIKUMS***

U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General Washington, D.C. 20530

2023. gada 23. jūnijā

Ana Gallego Torres
Director-General for Justice and Consumers
European Commission
Rue Montoyer/Montoyerstraat 59
1049 Brussels
Belgium

Cien. ģenerāldirektore *Gallego Torres*!

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 reģistru informāciju, tajā skaitā izklāstīti ar šīm pilnvarām saistītie piekļuves ierobežojumi ([1]). Visi šajā vēstulē aprakstītie juridiskie procesi ir nediskriminējoši, proti, tos izmanto, lai no Amerikas Savienoto Valstu uzņēmumiem, arī tādiem, kas pašsertificēs ES un ASV datu privātuma regulējuma ievērošanu, iegūtu informāciju neatkarīgi no datu subjekta valstspiederības vai dzīvesvietas. Turklāt, kā aprakstīts tālāk, 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 grozījumu, 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 tad, ja ir pamatots iemesls, ko apstiprina zvērests vai svinīgs solījums. Šādā orderī jābūt kratīšanas vietas un arestējamās personas vai mantas sīkam aprakstam." U.S. Const. amend. IV. 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) (citējot spriedumu lietā *Camara | Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). Attiecībā uz iekšzemes krimināllizmeklēšanu Ceturtais grozījums parasti nozīmē to, ka tiesībaizsardzības darbiniekiem pirms kratīšanas ir jāsaņem tiesas izdots orderis. Sk. *Katz | United States*, 389 U.S. 347, 357 (1967). Ordera izdošanas standarti, piemēram, pamatota iemesla un konkrētības prasības, attiecas uz fiziskas kratīšanas un aresta orderiem, kā arī uz orderiem saistībā ar glabātu elektroniskās saziņas saturu, kas

([1]) Šajā pārskatā nav aprakstīti nacionālās drošības izmeklēšanas rīki, ko tiesībaizsardzības iestādes izmanto terorisma un citās nacionālās drošības izmeklēšanās, tostarp nacionālās drošības vēstules (*NSL*), kas ļauj iegūt konkrētu reģistru informāciju no kredītinformācijas, finanšu pārskatiem un elektroniskiem abonentu un darījumu reģistriem, 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, un attiecībā uz elektronisku novērošanu, kratīšanas orderiem, komercdarbības dokumentu un citas informācijas vākšanu, ko veic saskaņā ar Ārējās izlūkošanas uzraudzības likumu, 50 U.S.C. § 1801 et seq.

([2]) Šajā ir vēstulē aplūkotas federālās tiesībaizsardzības un regulatīvās iestādes. Štata tiesību aktu pārkāpumus izmeklē attiecīgie štata tiesībaizsardzības iestādes un iztiesā štata tiesās. Štata tiesībaizsardzības iestādes izmanto orderus un pavēstes, ko izdod saskaņā ar štata tiesību aktiem un lielākoties tādā pašā veidā, kā aprakstīts šajā dokumentā, taču pastāv iespēja, ka uz tiesas procesu štatā var attiekties štata konstitūcijā vai likumos piešķirta papildu aizsardzība, kas ir plašāka par ASV Konstitūcijā garantēto. Štatu tiesību aktos paredzētajai aizsardzībai jābūt vismaz līdzvērtīgai tai, kas paredzēta ASV konstitūcijā, tajā skaitā (bet neaprobežojoties) ar Ceturto grozījumu.

izsniegti saskaņā ar tālāk minēto Glabāta saziņas satura likumu (*Stored Communications Act*). Ja prasību par orderi nepiemēro, uz valdības darbību saskaņā ar Ceturto grozījumu joprojām attiecina "saprātīguma" kritēriju. Tādējādi jau saskaņā ar Konstitūciju vien ASV valdībai nav neierobežotu vai patvaļīgu pilnvaru konfiscēt privātu informāciju ([3]).

Krimināltiesību piemērošanas pilnvaras

Federālie prokurori, kas ir Tieslietu ministrijas (*DoJ*) amatpersonas, un federālie izmeklēšanas aģenti (arī Federālā izmeklēšanas biroja (FIB) – *DoJ* tiesībaizsardzības aģentūras – aģenti) var likt Amerikas Savienoto Valstu uzņēmumiem sagatavot dokumentus un citu reģistrētu informāciju krimināllizmeklēšanas vajadzībām, īstenojot dažādus obligātos juridiskos procesus, tajā skaitā iesniedzot zvērināto pavēstes, administratīvās pavēstes un kratīšanas orderus, kā arī iegūt citu sakaru informāciju, īstenojot federālās krimināllnoziedznieku tālruņa sarunu noklausīšanās un zvanīto numuru reģistrētāju izmantošanas pilnvaras.

Zvērināto vai tiesas pavēstes. Krimināllpavēstes izmanto, lai veicinātu mērķtiecīgas tiesībaizsardzības iestāžu izmeklēšanas. Zvērināto pavēste ir oficiāls zvērināto izdots pieprasījums (parasti to izdod pēc federālā prokurora pieprasījuma), kas palīdz zvērinātajiem veikt izmeklēšanu par konkrētu iespējamu krimināltiesību pārkāpumu. Zvērinātie ir tiesas izmeklēšanas daļa, un to sastāvu izvēlas tiesnesis vai miertiesnesis. Pavēstē var pieprasīt kādam liecināt tiesas procesā vai sagatavot vai darīt pieejamus komercdarbības dokuments, 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 zvērinātie 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 sagatavoti vai darīti pieejami komercdarbības dokumenti, elektroniski glabāta informācija vai citi materiāli vienumi, kas ir relevanti 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 saņēmējs tāpat kā zvērināto pavēstes gadījumā var iebilst, ka pavēste ir nesamērīga, jo ir pārāk vispārīga vai arī patvaļīga vai apgrūtinoša.

Tiesas rīkojumi par zvanīto numuru reģistrētāju un uztveršanas un izsekošanas (*trap and trace*) ierīču izmantošanu. Saskaņā ar krimināltiesību noteikumiem par zvanīto numuru reģistrētāja un uztveršanas un izsekošanas 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 notiekošā krimināllizmeklēšanā. Sk. 18 U.S.C. §§ 3121-3127. Šādas ierīces izmantošana vai uzstādīšana pretrunā tiesību aktiem ir federāls noziedzīgs nodarījuma.

Elektroniskās saziņas privātuma likums (*ECPA*). Valdības piekļuvi abonentu informācijai, datplūsmas datiem un interneta pakalpojumu sniedzēju (jeb IPS), tālruņu pakalpojumu uzņēmumu un citu pakalpojumu sniedzēju, kuri ir trešās personas, glabātajam saziņas saturam reglamentē papildu noteikumi, kas ir paredzēti *ECPA* – dēvētā arī par Glabāta saziņas satura likumu (*Stored Communications Act – SCA*), 18 U.S.C. §§ 2701-2712, II sadaļā. *SCA* ir noteikta likumisko privātuma tiesību aizsardzības sistēma, kas ierobežo tiesībaizsardzības iestāžu piekļuvi datiem, kas nav tie dati, kuri IPS 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, interneta protokola (IP) adreses un saistītos laika zīmogus un norēķinu informāciju, krimināltiesību

([3]) Attiecībā uz iepriekš aplūkotajiem Ceturtā grozījuma principiem par privātuma un drošības interešu aizsardzību ASV tiesas regulāri piemēro šos principus jauniem tiesībaizsardzības izmeklēšanas rīku veidiem, kas rodas kopā ar tehnoloģiju attīstību. Piemēram, 2018. gadā Augstākā tiesa nolēma, ka valdības veiktā vēsturiskās mobilo sakaru staciju atrašanās vietu informācijas iegūšana no kāda mobilo sakaru uzņēmuma tiesībaizsardzības izmeklēšanā ilgākā laikposmā ir "kratīšana", kurai piemērojama Ceturtā grozījuma ordera prasība. *Carpenter / United States*, 138 S. Ct. 2206 (2018).

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 kriminālizmeklēšanu un tajā būtiski nepieciešama. Lai iegūtu glabātās elektroniskās saziņas saturu, krimināltiesību piemērošanas iestādes parasti ir jāsaņem no tiesneša attiecīgs orderis, pamatojoties uz pamatotu iemeslu uzskatīt, ka konkrētajā kontā ir pierādījumi par noziedzīgu nodarījumu. *SCA* ir paredzēta arī civiltiesiskā atbildība un krimināLsodi ([4]).

Tiesu rīkojumi par novērošanu saskaņā ar Federālo Likumu par tālruņa sarunu noklausīšanos. Papildus iepriekš minētajam un atbilstīgi federālajiem tiesību aktiem par tālruņa sarunu noklausīšanos tiesībaizsardzības iestādes ar kriminālizmeklēšanu saistītos nolūkos var reāllaikā pārtvert tālruņa, mutisko vai elektronisko saziņu. Sk. 18 U.S.C. §§ 2510-2523. Šīs pilnvaras var izmantot vienīgi saskaņā ar tiesas rīkojumu, kurā tiesnesis citu starpā konstatē, ka pastāv pamatots iemesls uzskatīt, ka sarunu noklausīšanās vai elektroniskās saziņas pārtveršana nodrošinās federāla noziedzīga nodarījuma pierādījumus vai informāciju par tādas personas atrašanās vietu, kura izvairās no krimināLvajāšanas. Attiecīgajā likumā ir paredzēta civiltiesiskā atbildība un krimināLsodi par sarunu noklausīšanās noteikumu pārkāpumiem.

*Search Warrant-Fed. R. Crim. P. Rule 41:* Tiesībaizsardzības iestādes Amerikas Savienotajās Valstīs var fiziski pārmeklēt telpas, ja ir saņēmušas attiecīgu tiesneša atļauju. Tiesībaizsardzības iestādēm, norādot pamatotu iemeslu, ir jāpierāda tiesnesim, ka noziedzīgs nodarījums izdarīts vai varētu tik izdarīts un ka ar noziedzīgu nodarījumu 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. Persona, kas pakļauta kratīšanai vai kuras īpašums ir pakļauts kratīšanai, var pieprasīt neatklāt pierādījumus, kas iegūti nelikumīgas kratīšanas rezultātā vai izriet no šādas kratīšanas, ja šie pierādījumi tiek iesniegti pret šo personu krimināLprocesā. Sk. *Mapp/Ohio*, 367 U.S. 643 (1961). Ja datu turētājam saskaņā ar orderi tiek pieprasīts izpaust datus, personai, kurai tas pieprasīts, var apstrīdēt prasību izpaust datus kā pārmērīgi apgrūtinošu. Sk. *In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979)* (kurā tika uzskatīts, ka "pienācīgā procesā nepieciešama uzklausīšana jautājumā par apgrūtinājumu, pirms likt tālruņa sakaru uzņēmumu sniegt" palīdzību saistībā ar kratīšanas orderi); *In re Application of United States, 616 F.2d 1122 (9th Cir. 1980)* (pamatojoties uz tiesas uzraudzības pilnvarām, izdarīts tāds pats secinājums).

*DoJ pamatnostādnes un politika*. Papildus aprakstītajiem konstitucionālajiem, likumiskajiem un noteikumos pamatotajiem ierobežojumiem, kas valdībai jāievēro saistībā ar piekļuvi datiem, ģenerālprokurors ir izdevis pamatnostādnes, kurās ir paredzēti papildu ierobežojumi attiecībā uz tiesībaizsardzības iestāžu piekļuvi datiem un noteikti arī privātuma un pilsonisko brīvību aizsardzības pasākumi. Piemēram, ģenerālprokurora pamatnostādnēs par FIB iekšzemes operācijām (2008. gada septembris) (tālāk – ĢP FIB pamatnostādnes), kas pieejamas http://www.justice.gov/archive/opa/docs/guidelines.pdf, ir ierobežota izmeklēšanas līdzekļu izmantošana ar federālu noziedzīgu nodarījumu izmeklēšanu saistītas informācijas meklēšanai. Pamatnostādnēs ir noteikts, ka FIB jāizmanto iespējami maz invazīvu izmeklēšanas metožu, ņemot vērā to ietekmi uz privātumu un pilsoniskajām brīvībām un kaitējumu, ko tās var nodarīt reputācijai. Pamatnostādnēs arī norādīts, ka "ir pašsaprotami, ka FIB veic izmeklēšanas un citas darbības likumīgā un samērīgā veidā, ievērojot brīvību un privātumu un nepieļaujot nevajadzīgu iejaukšanos likumpaklausīgu cilvēku dzīvē." ĢP FIB pamatnostādnes, 5. punkts. FIB ir īstenojusi minētās pamatnostādnes, sagatavojot FIB iekšzemes izmeklēšanas un operāciju rokasgrāmatu (*DIOG*), kas pieejama https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29 , – tā ir visaptveroša rokasgrāmata, kurā ietverti sīki izstrādāti ierobežojumi izmeklēšanas rīku izmantošanai un norādījumi, kā nodrošināt, lai ikvienā izmeklēšanā tiktu aizsargātas pilsoniskās brīvības un privātums. Papildu noteikumi un politika, no kā izriet federālo prokuroru izmeklēšanas darbību ierobežojumi, ir izklāstīti tieslietu rokasgrāmatā, kas arī pieejama tiešsaistē https://www.justice.gov/jm/justicemanual.

Civiltiesiskās un regulatīvās pilnvaras (sabiedrības intereses).

([4]) Turklāt *SCA* 2705. panta b) punkts atļauj valdībai, pamatojoties uz pierādītu vajadzību aizsargāt no datu izpaušanas, saņemt tiesas rīkojumu, kas aizliedz sakaru pakalpojumu sniedzējam brīvprātīgi paziņot tā pakalpojumu lietotājiem par *SCA* paredzētā tiesvedības procesa uzsākšanu. 2017. gada oktobrī ģenerālprokurora vietnieks *Rod Rosenstein* izdeva memorandu DoJ advokātiem un pārstāvjiem, kurā izklāstīja norādījumus, kā nodrošināt, ka šādu aizsardzības rīkojumu pieteikumi ir pielāgoti konkrētiem izmeklēšanas faktiem un apsvērumiem, un noteica, ka parasti paziņošanas atlikšanas maksimālais termiņš, ko iespējams pieprasīt, ir viens gads. 2022. gada maijā ģenerālprokurora vietniece *Lisa Monaco* izdeva papildu norādījumus par šo tematu, kurās cita starpā tika noteiktas iekšējās *DoJ* apstiprināšanas prasības attiecībā uz pieteikumiem pagarināt aizsardzības rīkojuma termiņu pēc sākotnējā viena gada perioda un prasīts izbeigt aizsardzības rīkojumu darbību izmeklēšanas noslēgumā.

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 izdot uzņēmumiem pavēstes, kurās pieprasa komercdarbības dokumentus, 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 izpildes tiesas ceļā. 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. 31 U.S.C. § 5318; 31 C.F.R. *Chapter X*. Citi uzņēmumi var izmantot Likumu par godīgu kredītinformāciju, 15 U.S.C. § 1681b, vai vairākus citus nozaru likumus Aģentūras pavēstes pilnvaru ļaunprātīga izmantošana var būt par iemeslu aģentūras atbildībai vai aģentūras amatpersonu personiskajai atbildībai. Sk., piemēram, Likumu par tiesībām uz finanšu datu aizsardzību (*Right to Financial Privacy Act*), 12 U.S.C. §§ 3401-3423. 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 prasības saskaņā ar Konstitūcijas Ceturto grozījumu. Sk. *See | City of Seattle*, 387 U.S. 541(1967).

Secinājums

Visām Amerikas Savienotajās Valstīs īstenotajām tiesībaizsardzības un regulatīvajām darbībām ir jāatbilst piemērojamiem tiesību aktiem, tajā skaitā ASV Konstitūcijai, normatīvajiem aktiem un noteikumiem. Šīs darbības arī jāveic saskaņā ar piemērojamo politiku, arī jebkādām 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 personām vai ārvalstu pilsoņiem –, kā arī sniedz iespēju izskatīt tiesā visus datu pieprasījumus, ko valdība iesniegusi atbilstīgi šīm pilnvarām.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

*VII PIELIKUMS*

**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE OFFICE OF GENERAL COUNSEL**

**WASHINGTON, DC 20511**

2022. gada 9. decembrī

*Leslie B. Kiernan,*
galvenā juriskonsulte
U.S. Department of
Commerce 1401 Constitution
Ave., NW Washington, DC 20230

Cien. *Leslie B. Kiernan*!

2022. gada 7. oktobrī prezidents Baidens parakstīja Izpildrīkojumu Nr. 14086 "Drošības pasākumu uzlabošana Amerikas Savienoto Valstu sakaru izlūkošanas darbībās", kas pastiprina stingro privātuma un pilsonisko brīvību garantiju kopumu, kas attiecas uz ASV sakaru izlūkošanas darbībām. Šīs garantijas ir šādas: prasīt, lai sakaru izlūkošanas darbības atbilstu noteiktiem likumīgiem mērķiem; nepārprotami aizliegt šādas darbības konkrētu aizliegtu mērķu sasniegšanai; ieviest jaunas procedūras, ar kurām nodrošināt, ka sakaru izlūkošanas darbības veicina šo likumīgo mērķu sasniegšanu un neveicina aizliegtu mērķu sasniegšanu; prasīt, lai sakaru izlūkošanas darbības tiktu veiktas tikai pēc tam, kad, pamatojoties uz visu attiecīgo faktoru pamatotu novērtējumu, ir konstatēts, ka šīs darbības ir nepieciešamas, lai veicinātu apstiprinātas izlūkošanas prioritātes īstenošanu, un tikai tādā apjomā un veidā, kas ir samērīgs ar apstiprināto izlūkošanas prioritāti, kuras īstenošanai tās ir atļautas; un uzdot izlūkošanas struktūrām atjaunināt savu politiku un procedūras, lai atspoguļotu izpildrīkojumā noteiktās sakaru izlūkošanas garantijas. Svarīgākais ir tas, ka ar izpildrīkojumu tiek ieviests arī neatkarīgs un saistošs mehānisms, kas ļauj fiziskām personām no "kvalificētām valstīm", kuras atzītas saskaņā ar izpildrīkojumu, vērsties tiesā, ja tās uzskata, ka pret tām ir veiktas nelikumīgas ASV sakaru izlūkošanas darbības – arī darbības, kas pārkāpj izpildrīkojumā noteikto aizsardzību.

Prezidenta Baidena izdotais Izpildrīkojums Nr. 14086 ir kulminācija vairāk nekā gadu ilgušām detalizētām sarunām starp Eiropas Komisijas (EK) un Amerikas Savienoto Valstu pārstāvjiem, un tajā noteikti pasākumi, ko Amerikas Savienotās Valstis veiks, lai īstenotu savas saistības saskaņā ar ES un ASV datu privātuma regulējumu. Kā noprotu, atbilstīgi sadarbības principam, kura rezultātā regulējums izstrādāts, no EK esat saņēmusi divus jautājumu kopumus par to, kā izlūkošanas struktūras īstenos izpildrīkojumu. Es labprāt atbildēšu uz šiem jautājumiem šajā vēstulē.

*1978. gada Ārējās izlūkošanas uzraudzības likuma 702. pants (FISA 702. pants)*

Pirmais jautājumu kopums attiecas uz *FISA* 702. pantu, kas ļauj ar elektronisko sakaru pakalpojumu sniedzēju palīdzību, kura ir sniedzama obligāti, iegūt ārējās izlūkošanas informāciju, novērojot personas, kuras nav ASV personas un par kurām ir pamats uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām Valstīm. Konkrētāk, jautājumi attiecas uz šī noteikuma un Izpildrīkojumu Nr. 14086 mijiedarbību, kā arī uz citām garantijām, kas piemērojamas darbībām, kuras veic saskaņā ar *FISA* 702. pantu.

Pirmkārt, varam apstiprināt, ka izlūkošanas struktūras piemēros Izpildrīkojumā Nr. 14086 noteiktās garantijas darbībām, ko veic saskaņā ar *FISA* 702. pantu.

Turklāt uz *FISA* 702. panta izmantošanu, ko veic valdība, attiecas arī daudzas citas garantijas. Piemēram, visi *FISA* 702. pantā noteiktie apliecinājumi ir jāparaksta gan ģenerālprokuroram, gan nacionālās izlūkošanas direktoram (*DNI*), un valdībai visi šādi apliecinājumi ir jāiesniedz apstiprināšanai Ārējās izlūkošanas uzraudzības tiesā (*FISC*), kuras sastāvā ir neatkarīgi tiesneši ar mūža pilnvarām, kuru pilnvaru termiņš šajā tiesā ir septiņi gadi. Apliecinājumos ir noteiktas tās ārējās izlūkošanas informācijas kategorijas, kas ir jāvāc un kam jāatbilst likumā noteiktajai ārējās izlūkošanas informācijas definīcijai, mērķtiecīgi vēršoties pret personām, kuras nav ASV personas un par kurām ir pamats uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām Valstīm. Apliecinājumos ir iekļauta informācija par starptautisko terorismu un citiem jautājumiem, piemēram, par informācijas iegūšanu attiecībā uz masu iznīcināšanas ieročiem. Katrs ikgadējais apliecinājums ir jāiesniedz *FISC* apstiprināšanai apliecinājuma pieteikuma dokumentu paketē, kurā ir iekļauti ģenerālprokurora un *DNI* apliecinājumi, dažu izlūkošanas aģentūru vadītāju ar zvērestu apliecinātas liecības, kā arī aprakstītas valdībai saistošas mērķorientēšanas procedūras, minimizācijas procedūras un vaicājumu procedūras. Mērķorientēšanas procedūras cita starpā paredz, ka izlūkošanas struktūras, pamatojoties uz visu apstākļu kopumu, pamatoti novērtē, ka mērķorientēšanas rezultātā, visticamāk, tiks iegūta *PISA* 702. pantā minētajā apliecinājumā norādītā ārējās izlūkošanas informācija.

Turklāt, vācot informāciju saskaņā ar *FISA* 702. pantu, izlūkošanas struktūrām: jāsniedz rakstisks paskaidrojums par to, uz kāda pamata mērķorientēšanas laikā ir novērtēts, ka mērķa rīcībā varētu būt *PISA* 702. pantā minētā apliecinājumā norādītā ārējās izlūkošanas informācija vai ka tas varētu saņemt, vai, iespējams, nodot šādu informāciju; jāapstiprina, ka joprojām tiek ievērots *PISA* 702. pantā noteiktais mērķorientēšanas standarts; kā arī jāpārtrauc vākšana, ja standarts vairs netiek ievērots. *Sk.* ASV valdības iesniegto dokumentu Ārējās izlūkošanas uzraudzības tiesai "2015. gada kopsavilkums par nozīmīgām 702. panta prasībām", 2.–3. lpp. (2015. gada 15. jūlijs).

Prasība izlūkošanas struktūrām rakstiski reģistrēt un regulāri apstiprināt sava novērtējuma, ka *FISA* 702. panta mērķi atbilst piemērojamajiem mērķorientēšanas standartiem, pamatotību atvieglo *FISC* veikto izlūkošanas struktūru mērķorientēšanas darbību uzraudzību. Katru reģistrēto mērķorientēšanas novērtējumu un pamatojumu reizi divos mēnešos pārskata Tieslietu ministrijas (*DoJ*) izlūkošanas pārraudzības juristi, kas šo pārraudzības funkciju veic neatkarīgi no ārējās izlūkošanas operācijām. Saskaņā ar jau izsenis pieņemtu *FISC* noteikumu, kas paredz, ka par jebkādiem piemērojamo procedūru pārkāpumiem jāziņo *FISC*, atbildīga ir tā *DoJ* nodaļa, kas veic šo funkciju. Šī ziņošana, kā arī regulāras *FISC* un šīs *DoJ* nodaļas sanāksmes par *FISA* 702. pantā noteikto mērķorientēšanas darbību pārraudzību ļauj *FISC* nodrošināt atbilstību *FISA* 702. pantā noteiktajai mērķorientēšanai un citām procedūrām un arī citos veidos nodrošināt, ka valdības darbības ir likumīgas. Proti, *FISC* to var panākt vairākos veidos – arī izdodot saistošus lēmumus par koriģējošiem pasākumiem, lai izbeigtu valdības pilnvaras vākt datus pret konkrētu mērķi vai lai grozītu vai aizkavētu datu vākšanu saskaņā ar *FISA* 702. pantu. *FISC* var arī pieprasīt, lai valdība sniedz papildu ziņojumus vai informāciju par atbilstību mērķorientēšanas un citām procedūrām, vai pieprasīt izmaiņas šajās procedūrās.

*Sakaru izlūkdatu lielapjoma vākšana*

Otrais jautājumu kopums attiecas uz sakaru izlūkdatu lielapjoma vākšanu, kas Izpildrīkojumā Nr. 14086 ir definēta kā "atļauta liela daudzuma sakaru izlūkdatu vākšana, kas tehnisku vai operatīvu apsvērumu dēļ tiek iegūta, neizmantojot diskriminantus (piemēram, neizmantojot īpašus identifikatorus vai atlases nosacījumus)."

Attiecībā uz šiem jautājumiem vispirms jāatzīmē, ka ne *FISA*, ne nacionālās drošības vēstules neatļauj lielapjoma datu vākšanu. Attiecībā uz *FISA*:

— *FISA* I un III daļā, kurā ir atļauta attiecīgi elektroniska novērošana un fiziska pārmeklēšana, ir noteikts, ka ir vajadzīgs tiesas rīkojums (ar retiem izņēmumiem, piemēram, ārkārtas apstākļos) un vienmēr prasīts pamatots iemesls uzskatīt, ka mērķis ir sveša vara vai svešas varas aģents. *Sk.* 50 U.S.C. §§ 1805, 1824.

— Ar 2015. gada *USA FREEDOM Act* tika grozīta *FISA* IV sadaļa, kas atļauj izmantot zvanīto numuru reģistrētājus un uztveršanas un izsekošanas ierīces saskaņā ar tiesas rīkojumu (izņemot ārkārtas apstākļus), lai pieprasītu valdībai pamatot pieprasījumus ar "īpašu atlases noteikumu". *Sk.* 50 U.S.C. § 1842(c)(3).

— *FISA* V sadaļa, kas ļauj Federālajam izmeklēšanas birojam (FIB) iegūt noteiktu veidu komercdarbības dokumentus, paredz, ka nepieciešams tiesas rīkojums, pamatojoties uz pieteikumu, kurā norādīts, ka "pastāv konkrēti un skaidri formulēti fakti, kas dod pamatu uzskatīt, ka persona, uz kuru ieraksti attiecas, ir sveša vara vai svešas varas aģents." *Sk.* 50 U.S.C. § 1862(b)(2)(B) ([1]).

— Ar *FISA* 702. pantu ir atļauts "izsekot personas, attiecībā uz kurām ir pamats uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām Valstīm, lai iegūtu ārējās izlūkošanas informāciju." *Sk.* 50 U.S.C. § 188la(a). Tādējādi, kā norādījusi Privātuma un pilsonisko brīvību pārraudzības padome, valdības veikta datu vākšana saskaņā ar *FISA* 702. pantu "ietver vienīgi tādu atsevišķu fizisku personu mērķtiecīgu novērošanu un ar šīm personām saistīta saziņas satura iegūšanu, saistībā ar kurām valdībai ir pamats sagaidīt, ka tā iegūs noteikta veida ārējās izlūkošanas datus", proti, "programma neparedz saziņas satura vākšanu ar lielapjoma metodēm". Privātuma un pilsonisko brīvību pārraudzības padome, ziņojums *"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act"*, 103. punkts (2014. gada 2. jūlijs) ([2]).

Attiecībā uz nacionālās drošības vēstulēm 2015. gada *USA FREEDOM Act* šādu vēstuļu izmantošanai ir noteikta "īpaša atlases noteikuma" prasība. *Sk.* 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

Turklāt Izpildrīkojumā Nr. 14086 noteikts, ka "[p]rioritāte jāpiešķir mērķorientētai vākšanai" un ka gadījumos, kad izlūkošanas struktūras veic lielapjoma datu vākšanu, "lielapjoma sakaru izlūkdatu vākšana ir atļauta, tikai pamatojoties uz konstatējumu (..), ka informāciju, kas nepieciešama, lai veicinātu apstiprinātas izlūkošanas prioritātes īstenošanu, nevar pamatoti iegūt ar mērķorientētu vākšanu." Sk. Izpildrīkojumu Nr. 14086, § 2(c)(ii)(A).

Turklāt, ja izmeklēšanas struktūras konstatē, ka lielapjoma datu vākšana atbilst šiem standartiem, Izpildrīkojums Nr. 14086 paredz papildu garantijas. Konkrētāk, izpildrīkojumā noteikts, ka, veicot lielapjoma datu vākšanu, izmeklēšanas struktūrām "jāpiemēro saprātīgas metodes un tehniskie pasākumi, lai vāktu tikai tādus datus, kas nepieciešami apstiprinātās izlūkošanas prioritātes īstenošanai, vienlaikus samazinot nebūtiskas informācijas vākšanu." Sk. turpat. Rīkojumā ir arī noteikts, ka "sakaru izlūkošanas darbības", kas ietver vaicājumu veikšanu ar lielapjoma datu vākšanas metodēm iegūtiem sakaru izlūkdatiem, "veic tikai pēc tam, kad, pamatojoties uz visu attiecīgo faktoru pamatotu novērtējumu, ir konstatēts, ka šīs darbības ir nepieciešamas apstiprinātās izlūkošanas prioritātes īstenošanai." *Sk. turpat* § 2(a)(ii)(A). Ar rīkojumu šis princips ir īstenots plašāk – tajā noteikts, ka izmeklēšanas struktūras drīkst veikt vaicājumus tikai saistībā ar neminimizētiem sakaru izlūkdatiem, kas ar lielapjoma vākšanas metodēm iegūti, lai sasniegtu sešus pieļaujamus mērķus, un ka šādi vaicājumi jāveic saskaņā ar politiku un procedūrām, kurās "pienācīgi ņemta vērā [vaicājumu] ietekme uz visu personu privātumu un pilsoniskajām brīvībām neatkarīgi no to valstspiederības vai dzīvesvietas." *Sk. turpat* § 2(c)(iii)(D). Visbeidzot, rīkojumā ir paredzēta savākto datu apstrāde, drošība un piekļuves kontrole. *Sk. turpat* § 2(c)(iii)(A) and§ 2(c)(iii)(B).

* * * * *

Mēs ceram, ka šie precizējumi būs noderīgi. Lūdzam nevilcināties un sazināties ar mums, ja jums ir vēl kādi jautājumi par to, kā ASV Iekšlietu ministrija plāno īstenot Izpildrīkojumu Nr. 14086.

([1]) No 2001. līdz 2020. gadam *FISA* V sadaļa ļāva FIB lūgt *FISC* atļauju iegūt "materiālus vienumus", kas ir būtiski noteiktām atļautām izmeklēšanām. Sk. *USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001)*. Šis formulējums, kas ir zaudējis spēku un tādējādi vairs nav likums, nodrošināja pilnvaras, saskaņā ar kurām valdība savulaik lielā apjomā vāca telefonijas metadatus. Tomēr vēl pirms šā noteikuma darbības beigām ar *USA FREEDOM Act*, tas tika grozīts, lai pieprasītu valdībai pamatot pieteikumu *FISC* ar "īpašu atlases noteikumu". Sk. *USA FREEDOM Act*, Pub. L. No. 114-23, 129 Stat. 268, § I 03 (2015).

([2]) Saskaņā ar 703. un 704. pantu, kas pilnvaro izlūkošanas struktūras vērsties pret ASV personām, kuras atrodas ārvalstīs, ir nepieciešams tiesas rīkojums (izņemot ārkārtas apstākļos), un vienmēr tiek prasīts pamatots iemesls uzskatīt, ka izlūkošanas subjekts ir sveša vara vai svešas varas aģents, vai svešas varas struktūras amatpersona vai darbinieks. *Sk. 50U.S.C.*§§ 1881b, 1881c.

Sincerely,

Galvenais juriskonsults
Christopher C. FONZONE

*VIII PIELIKUMS*

**Saīsinājumu saraksts**

Šajā lēmumā ir lietoti šādi saīsinājumi.

| | |
|---|---|
| AAA | Amerikas Šķīrējtiesu asociācija (*American Arbitration Association*) |
| ĢP noteikumi | Ģenerālprokurora vispārīgie noteikumi par Datu aizsardzības pārskatīšanas tiesu |
| AGG DOM | Ģenerālprokurora vadlīnijas FIB iekšzemes operācijām (*Attorney General Guidelines for Domestic FBI Operations*) |
| APA | Administratīvā procesa likums (*Administrative Procedure Act*) |
| CIP | Centrālā izlūkošanas pārvalde |
| CNSS | Nacionālās drošības sistēmu komiteja (*Committee on National Security Systems*) |
| Tiesa | Eiropas Savienības Tiesa |
| Lēmums | Komisijas Īstenošanas lēmums, kas pieņemts, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, par personas datu pietiekamu aizsardzības līmeni ES un ASV datu privātuma regulējuma ietvaros |
| DHS | Iekšzemes drošības ministrija (*Department of Homeland Security*) |
| DNI | nacionālās izlūkošanas direktors (*Director of National Intelligence*) |
| DoC | ASV Tirdzniecības ministrija (*U.S. Department of Commerce*) |
| DoJ | ASV Tieslietu ministrija (*U.S. Department of Justice*) |
| DoT | ASV Satiksmes ministrija |
| DAI | datu aizsardzības iestāde |
| DPR saraksts | datu privātuma regulējuma saraksts |
| DPRC | Datu aizsardzības pārskatīšanas tiesa (*Data Protection Review Court*) |
| ECOA | Likums par vienlīdzīgām kreditēšanas iespējām (*Equal Credit Opportunity Act*) |
| ECPA | Elektroniskās saziņas privātuma likums (*Electronic Communications Privacy Act*) |
| EEZ | Eiropas Ekonomikas zona |
| IR Nr. 12333 | Izpildrīkojums Nr. 12333 "Amerikas Savienoto Valstu izlūkošanas darbības" (*Executive Order 12333 'United States Intelligence Activities'*) |
| IR Nr. 14086, IR | Izpildrīkojums Nr. 14086 "Drošības pasākumu uzlabošana ASV sakaru izlūkošanas darbībām" (*Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities'*) |
| ES un ASV DPR jeb DPR | ES un ASV datu privātuma regulējums |
| ES un ASV DPR kolēģija | ES un ASV datu privātuma regulējuma kolēģija |
| FIB | Federālais izmeklēšanas birojs |
| FCRA | Likums par godīgu kredītinformāciju (*Fair Credit Reporting Act*) |
| FISA | Ārējās izlūkošanas uzraudzības likums (*Foreign Intelligence Surveillance Act*) |
| FISC | Ārējās izlūkošanas uzraudzības tiesa (*Foreign Intelligence Surveillance Court*) |
| FISCR | Ārējās izlūkošanas uzraudzības pārskatīšanas tiesa (*Foreign Intelligence Surveillance Court of Review*) |
| FOIA | Informācijas brīvības likums (*Freedom of Information Act*) |
| FRA | Federālais reģistru likums (*Federal Records Act*) |

| | |
|---|---|
| FTC | ASV Federālā tirdzniecības komisija (*U.S. Federal Trade Commission*) |
| HIPAA | Likums par veselības apdrošināšanas datu pārnesamību un pārskatatbildību (*Health Insurance Portability and Accountability Act*) |
| ICDR | Starptautiskais strīdu izšķiršanas centrs (*International Centre for Dispute Resolution*) |
| IOB | Izlūkošanas pārraudzības padome (*Intelligence Oversight Board*) |
| NIST | Nacionālais standartu un tehnoloģiju institūts (*National Institute of Standards and Technology*) |
| NSA | Nacionālā drošības aģentūra (*National Security Agency*) |
| NSL | nacionālās drošības vēstule(-es) (*National Security Letter(s)*) |
| ODNI | nacionālās izlūkošanas direktora birojs (*Office of the Director of National Intelligence*) |
| *ODNI CLPO, CLPO* | nacionālās izlūkošanas direktora biroja pilsonisko brīvību aizsardzības amatpersona (*Civil Liberties Protection Officer of the Director of National Intelligence*) |
| OMB | Pārvaldības un budžeta birojs (*Office of Management and Budget*) |
| OPCL | Tieslietu ministrijas Privātuma un pilsonisko brīvību birojs (*Office of Privacy and Civil Liberties of the Department of Justice*) |
| PCLOB | Privātuma un pilsonisko brīvību pārraudzības padome (*Privacy and Civil Liberties Oversight Board*) |
| PIAB | Prezidenta Izlūkošanas konsultatīvā padome (*President's Intelligence Advisory Board*) |
| PPD 28 | Prezidenta politikas direktīva 28 (*Presidential Policy Directive 28*) |
| Regula (ES) 2016/679 | Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK |
| SAOP | aģentūras vecākā amatpersona privātuma jautājumos (*Senior Agency Official for Privacy*) |
| DPR principi | ES un ASV datu privātuma regulējuma principi |
| ASV | Amerikas Savienotās Valstis |
| Savienība | Eiropas Savienība |