II

(Aktai, kurių skelbti neprivaloma)

KOMISIJA

KOMISIJOS SPRENDIMAS

2004 m. gegužės 14 d.

dėl Jungtinių Amerikos Valstijų Muitinės ir pasienio apsaugos tarnybai perduodamų oro keleivių asmens duomenų, nurodytų Keleivio duomenų įraše (*Passenger Name Record*), tinkamos apsaugos

(pranešta dokumentu Nr. K(2004)1914)

(Tekstas svarbus EEE)

(2004/535/EB)

EUROPOS BENDRIJŲ KOMISIJA,

atsižvelgdama į Europos bendrijos steigimo sutartį,

atsižvelgdama į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo [1], ypač į jos 25 straipsnio 6 dalį,

kadangi:

(1) Remiantis Direktyva 95/46/EB valstybės narės numato, kad asmens duomenys trečiajai šaliai gali būti perduoti tik tuo atveju, jei pastaroji užtikrina tinkamą apsaugos lygį ir jei iki perdavimo laikomasi kitų direktyvos nuostatas įgyvendinančių valstybių narių įstatymų.

(2) Komisija gali nuspręsti, kad trečioji šalis užtikrina tinkamą apsaugos lygį. Tokiu atveju asmens duomenys gali būti perduodami iš valstybių narių nereikalaujant papildomų garantijų.

(3) Remiantis Direktyva 95/46/EB, duomenų apsaugos lygio tinkamumas turėtų būti įvertinamas atsižvelgiant į duomenų perdavimo operacijos ar operacijų grupės aplinkybes, ypatingą dėmesį skiriant keletui duomenų perdavimui svarbių ir 25 straipsnio 2 dalyje išvardytų elementų.

(4) Oro transporto sistemoje „Keleivio duomenų įrašas“ („*Passenger Name Record*“, toliau – PNR) – tai kiekvieno keleivio kelionės sąlygų įrašas, kuriame pateikiama visa reikalinga informacija, kad vietas užsakančiosios ir dalyvaujančiosios oro linijos galėtų tvarkyti ir kontroliuoti užsakymus. Šiame sprendime „keleivio“ ir „keleivių“ sąvokos apima įgulos narius. „Vietas užsakančiosios oro linijos“ yra oro linijos, kuriose keleivis atliko pirmąjį užsakymą, arba kuriose po įvykusios kelionės buvo atlikti papildomi užsakymai. „Dalyvaujančios oro linijos“ yra bet kurios oro linijos, kuriose vietas užsakančiosios oro linijos keleiviui užsakė vietas viename arba daugiau nei viename jos skrydžių.

(5) Jungtinių Amerikos Valstijų Krašto saugumo departamento (*Department of Homeland Security*, toliau – DHS) Muitinės ir pasienio apsaugos tarnyba (*United States Bureau of Customs and Border Protection*, toliau – CBP) reikalauja, kad kiekvienas tarptautinius keleivių pervežimus oro transportu į Jungtines Amerikos Valstijas arba iš jų vykdantis vežėjas suteiktų jai elektroninę prieigą prie vežėjo oro transportu surinktų ir jo kompiuterinėje užsakymų sistemoje laikomų PNR.

(6) Reikalavimai oro keleivių asmens duomenims, nurodytiems PNR ir perduotiniems CBP, yra grindžiami Jungtinėse Amerikos Valstijose 2001 m. lapkričio mėn. [2] priimtu įstatymu ir remiantis minėtu įstatymu CBP priimtomis įgyvendinimo taisyklėmis [3].

[1] OL L 281, 1995 11 23, p. 31; Direktyva su paskutiniais pakeitimais, padarytais Reglamentu (EB) Nr. 1882/2003 (OL L 284, 2003 10 31, p. 1).

[2] *Title 49, United States Code, section 44909(c)(3).*

[3] *Title 19, Code of Federal Regulations, section 122.49b.*

(7) Minėtieji Jungtinių Amerikos Valstijų teisės aktai apibrėžia saugumo stiprinimo bei atvykimo į šalį ir išvykimo iš jos reikalavimus, kuriuos Jungtinės Amerikos Valstijos turi suverenią galią nustatyti savo jurisdikcijos ribose. Be to, nustatyti reikalavimai yra suderinti su Jungtinių Amerikos Valstijų prisiimtais tarptautiniais įsipareigojimais. Jungtinės Amerikos Valstijos yra demokratinė šalis, kurioje viešpatauja įstatymų viršenybė ir stipri pilietinių laisvių tradicija. Jos teisėkūros proceso teisėtumu bei jos teismų stiprumu ir nepriklausomumu neabejojama. Spaudos laisvė yra dar viena stipri garantija, kad nebus piktnaudžiaujama pilietinėmis laisvėmis.

(8) Bendrijos teisės nustatytose ribose Bendrija visada įsipareigoja remti Jungtines Amerikos Valstijas kovoje su terorizmu. Bendrijos teisėje numatoma būtinybė išlaikyti saugumo ir privatumo interesų pusiausvyrą. Pavyzdžiui, Direktyvos 95/46/EB 13 straipsnis numato, kad valstybės narės gali priimti teisines priemones, apribojančias tam tikrų šios direktyvos reikalavimų taikymo sritį, kai tai reikalinga dėl nacionalinio saugumo, gynybos, visuomenės saugumo ir nusikaltimų prevencijos, tyrimo, išaiškinimo ir baudžiamojo persekiojimo.

(9) Duomenų perdavime dalyvauja konkretūs duomenų valdytojai: skrydžius tarp Bendrijos ir Jungtinių Amerikos Valstijų vykdančios oro linijos ir tik vienintelis jų gavėjas Jungtinėse Amerikos Valstijose – CBP.

(10) Turi būti apibrėžtas laikotarpis, kurį taikomos priemonės dėl PNR perdavimo Jungtinėms Amerikos Valstijoms teisinio pagrindo, ypač remiantis šiuo sprendimu. Buvo susitarta dėl trejų su puse metų laikotarpio. Per šį laikotarpį aplinkybės gali labai pasikeisti, todėl Bendrija ir Jungtinės Amerikos Valstijos susitaria, kad priemones reikės peržiūrėti.

(11) CBP gautų oro keleivių asmens duomenų, nurodytų PNR, tvarkymą reglamentuoja 2004 m. gegužės 11 d. Jungtinių Amerikos Valstijų Krašto saugumo departamento Muitinės ir pasienio apsaugos tarnybos (*Department of Homeland Security Bureau of Customs and Border Protection of 11 May 2004, CBP*) įsipareigojimuose (toliau – Įsipareigojimai) ir Įsipareigojimuose nurodytuose Jungtinių Amerikos Valstijų vidaus teisės aktuose nustatyti reikalavimai.

(12) Iš visų Jungtinių Amerikos Valstijų vidaus teisės aktų šiuo atveju svarbus yra Informacijos laisvės aktas (*Freedom of Information Act*, toliau – FOIA), nes jis numato sąlygas, kurioms esant CBP gali atmesti prašymus dėl informacijos atskleidimo, ir taip išlaikyti PNR paslaptyje. Aktas reglamentuoja PNR atskleidimą tiems asmenims, kuriems jis skirtas, ir yra glaudžiai susijęs su duomenų subjekto teise į prieigą. Jis taikomas tiek Jungtinių Amerikos Valstijų pilietybę turintiems, tiek jos neturintiems asmenims.

(13) Kaip nurodyta Įsipareigojimų 44 dalyje, jų nuostatos bus arba jau yra įtrauktos į įstatymus, taisykles, direktyvas arba kitas Jungtinių Amerikos Valstijų politikos priemones, ir dėl to jų teisinė galia skiriasi. Visas Įsipareigojimų tekstas skelbiamas DHS tvarkomame Federaliniame registre. Todėl tai yra rimti ir gerai apgalvoti politiniai DHS įsipareigojimai, o ar jų laikomasi, nustatoma per Jungtinių Amerikos Valstijų ir Bendrijos bendrą peržiūrą. Jų nesilaikymas prireikus galėtų būti apskųstas teisiniais, administraciniais ir politiniais būdais, o jei pažeidimai tęstųsi, šio sprendimo galiojimas galėtų būti laikinai sustabdomas.

(14) Standartai, kuriais remiantis CBP tvarko keleivių PNR duomenis pagal Jungtinių Amerikos Valstijų teisės aktus ir Įsipareigojimus, numato pagrindinius principus, kurių reikia užtikrinant tinkamą fizinių asmenų apsaugos lygį.

(15) Laikantis tikslo ribojimo principo, CBP gaunami oro keleivių asmens duomenys, nurodyti PNR, tvarkomi atsižvelgiant į konkretų tikslą, o tada panaudojami arba toliau perduodami tiktai tuo atveju, kai tai suderinama su perdavimo tikslu. PNR duomenys bus iš esmės naudojami tik užkertant kelią terorizmui ir susijusiems nusikaltimams, kitiems tarpvalstybinio pobūdžio sunkiems nusikaltimams, įskaitant organizuotą nusikalstamumą, slėpimuisi nuo arešto ar įkalinimo už minėtus nusikaltimus bei su jais kovojant.

(16) Laikydamasi duomenų kokybės ir proporcingumo principo dėl svarbių viešųjų interesų, kuriuos užtikrinant perduodami PNR duomenys, CBP vėliau nekeis gautų PNR duomenų. Perduodamos ne daugiau kaip 34 PNR duomenų kategorijos, o Jungtinių Amerikos Valstijų institucijos konsultuojasi su Komisija prieš nustatydamos naujus reikalavimus. Papildoma informacija apie asmenį, kuri tiesiogiai gaunama patikrinus PNR duomenis bus gaunama tik teisėtais būdais iš kitų nei valdžios institucijos šaltinių. Paprastai PNR ištrinami ne vėliau kaip po trejų metų ir šešių mėnesių, išskyrus duomenis, kurie buvo gauti konkretiems tyrimams arba kitaip rankiniu būdu surinkti;

(17) Laikydamasi skaidrumo principo, CBP teikia informaciją keleiviams apie perdavimo ir tvarkymo tikslą bei apie trečiosios šalies duomenų valdytojo tapatybę, taip pat ir kitą informaciją.

(18) Laikydamasi saugumo principo, CBP imasi techninių ir organizacinių saugumo priemonių, atsižvelgdama į tvarkymo sukeliamą pavojų.

(19) Prieigos ir ištaisymo teisės pripažįstamos tik tada, kai duomenų subjektas prašo PNR duomenų kopijos ir ištaisyti netikslius duomenis. Numatomos išimtys yra plačiai suderintos su apribojimais, kuriuos valstybės narės gali taikyti pagal Direktyvos 95/46/EB 13 straipsnį.

(20) Duomenys toliau perduodami kitoms vyriausybės institucijoms, taip pat ir užsienio vyriausybių institucijoms, vykdančioms kovos su terorizmu arba teisėsaugos funkcijas, kiekvienu atveju tais tikslais, kurie nustatyti tikslus apribojančiuose nuostatuose. Taip pat duomenys gali būti perduodami siekiant apsaugoti duomenų subjekto ar kitų asmenų gyvybiškai svarbius interesus, ypač iškilus dideliam pavojui sveikatai arba vykstant bet kokiam teisminiam baudžiamajam procesui, arba dėl kitų įstatymu nustatytų priežasčių. Gaunančiosios tarnybos pagal tiksliai apibrėžtas atskleidimo sąlygas privalo naudoti duomenis tik tiems tikslams ir negali perduoti duomenų toliau be CBP sutikimo. Jokia kita užsienio, federalinė, valstijos ar vietos tarnyba neturi tiesioginės elektroninės prieigos prie PNR duomenų per CBP duomenų bazes. CBP atsisako viešai atskleisti PNR remdamasi atitinkamų FOIA nuostatų išimtimis.

(21) CBP nenaudoja Direktyvos 95/46/EB 8 straipsnyje nurodytų ypatingų duomenų, ir kol nėra filtrų sistemos, neleidžiančios panaikinti tokius duomenis iš Jungtinėms Amerikos Valstijoms perduodamų PNR, įsipareigoja įdiegti priemones, kurios juos ištrintų ir tuo metu jais nesinaudoja.

(22) Kalbant apie įgyvendinimo mechanizmus, užtikrinančius, kad CBP laikysis šių principų, numatoma CBP darbuotojus mokyti ir informuoti, o atskiriems darbuotojams taikyti sankcijas. DHS vyriausiasis privatumo reikalų pareigūnas (*DHS Chief Privacy Officer*), kuris yra DHS pareigūnas, bet turi labai didelį organizacinį savarankiškumą ir privalo kasmet teikti ataskaitą Kongresui, prižiūri kaip CBP laikosi privatumo reikalavimų. Asmenys, kurių PNR duomenys buvo perduoti, gali teikti skundus CBP arba, jeigu skundai nepatenkinami, DHS vyriausiajam privatumo reikalų pareigūnui tiesiogiai arba tarpininkaujant valstybių narių duomenų apsaugos institucijoms. DHS Privatumo reikalų biuras (*DHS Privacy Office*) skubos tvarka nagrinėja Bendrijos gyventojų vardu valstybių narių duomenų apsaugos institucijų pateiktus skundus, jeigu gyventojas mano, kad jo skundą CBP arba DHS Privatumo reikalų biuras išnagrinėjo netinkamai. CBP kartu su DHS ir Komisijos vadovaujama grupe kasmet vykdo bendrą peržiūrą, kurios metu tikrina, kaip laikomasi Įsipareigojimų.

(23) Siekiant skaidrumo ir norint apsaugoti valstybių narių kompetentingų institucijų galimybes užtikrinti asmenų apsaugą, kai tvarkomi pastarųjų asmens duomenys, svarbu tiksliai apibrėžti išimtines aplinkybes, kuriomis gali būti pagrįstas konkrečių duomenų srauto laikinas sustabdymas, nepažeidžiant tinkamos apsaugos.

(24) Pagal Direktyvos 95/46/EB 29 straipsnį įsteigta Darbo grupė asmenų apsaugai tvarkant asmens duomenis pateikė nuomones apie Jungtinių Amerikos Valstijų institucijų teikiamą keleivių duomenų apsaugos lygį, kurios tapo Komisijos gairėmis derybose su DHS. Komisija atsižvelgė į šias nuomones rengdama šį sprendimą [1].

(25) Šiame sprendime numatytos priemonės atitinka Direktyvos 95/46/EB 31 straipsnio 1 dalimi įkurto Komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Pagal Direktyvos 95/46/EB 25 straipsnio 2 dalį Jungtinių Amerikos Valstijų Muitinės ir pasienio apsaugos tarnyba (*United States' Bureau of Customs and Border Protection*, toliau – CBP) yra laikoma institucija, užtikrinančia tinkamą iš Bendrijos gaunamų PNR duomenų dėl skrydžių į Jungtines Amerikos Valstijas ir iš jų apsaugos lygį pagal priede nustatytus Įsipareigojimus.

2 straipsnis

Šis sprendimas yra susijęs su CBP teikiamos apsaugos tinkamumu, atsižvelgiant į Direktyvos 95/46/EB 25 straipsnio 1 dalies reikalavimus, ir neturi įtakos kitoms sąlygoms arba apribojimams, įgyvendinant kitas tos direktyvos, kuri siejasi su asmens duomenų tvarkymu valstybėse narėse, nuostatas.

[1] 2002 m. spalio 24 d. Darbo grupės priimta Nuomonė 6/2002 dėl keleivio deklaruojamos informacijos ir kitų oro linijų duomenų perdavimo Jungtinėms Amerikos Valstijoms, skelbiama: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf
2003 m. birželio 13 d. Darbo grupės priimta Nuomonė 4/2003 dėl Jungtinių Amerikos Valstijų užtikrinamo keleivių duomenų perdavimo apsaugos lygio, skelbiama: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf
2004 m. sausio 29 d. Darbo grupės priimta Nuomonė 2/2004 dėl oro keleivių asmens duomenų, nurodytų PNR ir perduodamų Jungtinių Amerikos Valstijų Muitinės ir pasienio apsaugos tarnybai (CBP), tinkamos apsaugos, skelbiama: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf

3 straipsnis

1. Nepažeisdamos savo galių imtis veiksmų, užtikrinančių nacionalinių nuostatų, priimtų pagal kitų nei Direktyvos 95/46/EB 25 straipsnio nuostatas, laikymąsi, valstybių narių kompetentingos institucijos gali pasinaudoti savo turimomis galiomis ir laikinai sustabdyti duomenų srautus į CBP, kad apsaugotų asmenis, kai tvarkomi jų asmens duomenys šiais atvejais:

a) jeigu kompetentinga Jungtinių Amerikos Valstijų institucija nustatė, kad CBP pažeidė taikomus apsaugos standartus, arba

b) jeigu yra reali tikimybė, kad pažeidinėjami priede nustatyti apsaugos standartai, yra pagrįstų priežasčių manyti, kad CBP nesiima arba nesiims tinkamų ir savalaikių priemonių konkrečiam atvejui išspręsti, tolesnis perdavimas sukels tiesioginį didelės žalos duomenų subjektams pavojų, ir tomis aplinkybėmis valstybių narių kompetentingos institucijos dėjo tinkamas pastangas, pateikdamos CBP pranešimą ir suteikdamos galimybę atsakyti į jį.

2. Laikinas sustabdymas galios tol, kol bus užtikrinti apsaugos standartai, ir apie tai bus pranešta atitinkamų valstybių narių kompetentingoms institucijoms.

4 straipsnis

1. Valstybės narės nedelsdamos praneša Komisijai, kada buvo priimtos 3 straipsnyje numatytos priemonės.

2. Valstybės narės ir Komisija praneša viena kitai apie bet kokius apsaugos standartų pasikeitimus ir apie atvejus, kuriais institucijų, atsakingų už tai, kad CBP laikytųsi apsaugos standartų, veiksmai, kaip nurodyta priede, neužtikrina tokio laikymosi.

3. Jeigu pagal 3 straipsnį ir pagal šio straipsnio 1 ir 2 dalis surinkta informacija įrodo, kad nebesilaikoma pagrindinių principų, kurie būtini užtikrinant fizinių asmenų tinkamą apsaugos lygį, arba kad institucija, kuri yra atsakinga už tai, kad CBP laikytųsi priede nustatytų apsaugos standartų, neefektyviai atliko savo vaidmenį, būtina apie tai pranešti CBP, o prireikus, siekiant šį sprendimą panaikinti arba laikinai sustabdyti jo galiojimą, taikyti Direktyvos 95/46/EB 31 straipsnio 2 dalyje numatytą tvarką.

5 straipsnis

Šio sprendimo veikimas yra prižiūrimas, ir apie bet kokius susijusius duomenis pranešama pagal Direktyvos 95/46/EB 31 straipsnį įsteigtam Komitetui, įskaitant visus patvirtinančius faktus, kurie gali daryti poveikį šio sprendimo 1 straipsnyje nurodytiems duomenims, kad CBP gaunamų oro keleivių asmens duomenų, nurodytų PNR, apsauga atitinka Direktyvos 95/46/EB 25 straipsnio reikalavimus.

6 straipsnis

Per keturis mėnesius nuo pranešimo dienos valstybės narės imasi visų priemonių, kurių reikia užtikrinant sprendimo laikymąsi.

7 straipsnis

Šis sprendimas galioja trejus metus ir šešis mėnesius nuo jo pranešimo dienos, nebent galiojimas pratęsiamas Direktyvos 95/46/EB 31 straipsnio 2 dalyje nustatyta tvarka.

8 straipsnis

Šis sprendimas skirtas valstybėms narėms.

Priimta Briuselyje, 2004 m. gegužės 14 d.

Komisijos vardu

Frederik BOLKESTEIN

Komisijos narys

PRIEDAS

KRAŠTO SAUGUMO DEPARTAMENTO MUITINĖS IR PASIENIO APSAUGOS TARNYBOS (*DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION*, TOLIAU – CBP) – ĮSIPAREIGOJIMAI

Remdama Europos Komisijos (toliau – Komisija) planą vykdyti jai Direktyvos 95/46/EB (toliau – Direktyva) 25 straipsnio 6 dalimi suteiktas galias ir priimti sprendimą, pripažįstantį, kad Krašto saugumo departamento Muitinės ir pasienio apsaugos tarnyba (CBP) gali suteikti tinkamą Keleivio ([1]) duomenų įrašo (PNR) informacijos, kurią perduoda vežėjai oro transportu ir kuriai gali būti taikomos šios direktyvos nuostatos, apsaugą, CBP įsipareigoja:

Teisiniai įgaliojimai gauti PNR

1. Remiantis įstatymu (*title 49, United States Code, section 44909(c)(3)*) ir jo įgyvendinimo (laikinosiomis) taisyklėmis (*title 19, Code of Federal Regulations, section 122.49b*), visi užsienio oro transportu į Jungtines Amerikos Valstijas ir iš jų keleivių skrydžius vykdantys vežėjai turi leisti CBP (buvusiai Jungtinių Amerikos Valstijų Muitinės tarnybai (*United States Customs Service)* elektroniniu būdu susipažinti su visais vežėjo oro transportu kompiuterinėje užsakymų ir (arba) išvykimo kontrolės sistemose (toliau – užsakymų sistemos) renkamais ir laikomais PNR duomenimis.

CBP naudojimasis PNR duomenimis

2. Daugumą PNR duomenų elementų Muitinės ir pasienio apsaugos tarnyba gali gauti išanalizavusi duomenų subjekto oro bilieto informaciją ir kitus kelionės dokumentus, remdamasi savo įprastomis pasienio kontrolės teisėmis, bet gaudama šiuos duomenis elektroniniu būdu ji turi didesnes galimybes palengvinti *bona fide* keliones ir vykdyti efektyvų išankstinį keleivių rizikos įvertinimą.

3. CBP naudojasi PNR duomenimis tik siekdama užkirsti kelią: 1) terorizmui ir su juo susijusiems nusikaltimams; 2) kitiems tarpvalstybinio pobūdžio sunkiems nusikaltimams, įskaitant organizuotą nusikalstamumą, ir 3) slėpimuisi nuo arešto ar įkalinimo už anksčiau minėtus nusikaltimus, bei su jais kovoti. Šiems tikslams naudojami PNR duomenys leidžia CBP sutelkti išteklius ypač didelį pavojų keliantiems dalykams, ir taip palengvinti bei apsaugoti *bona fide* keliones.

Duomenų reikalavimai

4. CBP reikalaujami duomenų elementai yra išvardinti A priedėlyje. (Šiuose Įsipareigojimuose tokie nustatyti elementai yra vadinami PNR). Nors CBP reikalauja galimybės susipažinti su visais trisdešimt keturiais (34) A priedėlyje išvardintais duomenų elementais, CBP mano, kad labai retai PNR turės visus nustatytus duomenų elementus. Tokiais atvejais, kai PNR neturės visų nustatytų duomenų, CBP nebandys tiesiogiai iš vežėjo oro transportu užsakymų sistemos susipažinti su kitais, A priedėlyje nenurodytais, PNR duomenimis.

5. „OSI“ ir „SSI/SSR“ duomenų elementų (kurie paprastai vadinami bendrosiomis pastabomis ir tuščiais laukais) atveju CBP kompiuterinė sistema tuose laukuose ieškos A priedėlyje išvardytų informacijos elementų. CBP darbuotojai turės teisę rankiniu būdu peržiūrėti visus OSI ir SSI/SSR laukus tik tada, jei CBP nustatys, kad asmuo, kuris yra PNR subjektas, kelia didelį pavojų kuriam nors iš šio dokumento 3 dalyje nurodytų tikslų.

6. Papildoma informacija apie asmenį, kurios ieškoma patikrinus PNR duomenis, bus tiesiogiai gaunama tik teisėtais būdais iš kitų nei valdžios institucijos šaltinių, o prireikus, pasinaudojant abipusės teisinės pagalbos kanalais, ir tik šio dokumento 3 dalyje nurodytais tikslais. Pavyzdžiui, jei PNR yra nurodytas kreditinės kortelės numeris, gali būti ieškoma informacijos apie su ta sąskaita siejamą sandorį, vadovaujantis teisėtu procesu, pavyzdžiui, didžiajai prisiekusiųjų žiuri (*Grand Jury*) išduodant šaukimą į teismą arba teismui priimant nutartį, arba remiantis kitomis teisėtomis priemonėmis. Be to, norint susipažinti su įrašais, susijusiais su elektroninio pašto sąskaitomis, apie kurias buvo sužinota iš PNR, reikės, atsižvelgiant į ieškomos informacijos pobūdį, laikytis Jungtinių Amerikos Valstijų teisės aktų reikalavimų dėl šaukimo į teismą, teismo nutarčių, orderių ir kitų teisėtų procesų.

7. Jei CBP sužinos apie papildomus PNR laukus, kuriuos oro linijos galėjo įdiegti į savo sistemas, ir kurie žymiai pagerintų CBP gebėjimus atlikti keleivio rizikos įvertinimą, arba, jei aplinkybės rodytų, kad anksčiau nereikalaujamo PNR lauko reikės vykdant šių Įsipareigojimų 3 dalyje nurodytus ribotus tikslus, prieš atlikdama tokią reikalaujamų PNR duomenų elementų (A priedėlis) peržiūrą, CBP dėl to konsultuosis su Europos Komisija.

([1]) Šiuose Įsipareigojimuose „keleivio“ ir „keleivių“ sąvokos apima įgulos narius.

8. CBP gali perduoti didelį kiekį PNR tuo pat metu Pervežimų saugos administracijai (TSA), kad ji galėtų patikrinti savo kompiuterizuotą Keleivių pirminio patikrinimo sistemą II (CAPPS II). Tokia informacija bus perduodama tik gavus leidimą tikrinti Jungtinų Amerikos Valstijų vidaus skrydžių PNR duomenis. Pagal šią nuostatą TSA ar kitos tiesiogiai tikrinimuose dalyvaujančios šalys perduotus PNR duomenis laikys tik tikrinimui reikalingą laikotarpį ir neperduos jų jokiai kitai trečiajai šaliai [2]. Duomenis galima naudoti tik CAPPS II sistemos ir sąsajų tikrinimui, toks naudojimasis jais negali turėti jokių praktinių pasekmių, išskyrus ypatingas situacijas, kai iš tikrųjų atpažįstamas žinomas teroristas arba nustatytų ryšių su terorizmu turintis asmuo. Laikydamasi 10 dalyje apibūdinto kompiuterinio filtravimo metodo reikalaujančios nuostatos, CBP, prieš perduodama TSA dideliais kiekiais pagal šios dalies reikalavimus keleivių duomenų įrašus, turės juos perfiltruoti ir panaikinti visus „jautrius“ duomenis.

Darbas su „jautriais“ duomenimis

9. CBP nesinaudos „jautriais“ iš PNR gaunamais duomenimis (t. y. duomenimis, atspindinčiais asmens rasinę ar etninę kilmę, politinę orientaciją, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose, ir duomenimis apie jo sveikatą ar lytinį gyvenimą), kaip nurodyta toliau.

10. Kaip galėdama greičiau CBP įdiegs kompiuterinę sistemą, kuri filtruoja ir ištrina tam tikrus „jautrius“ PNR kodus ir sąvokas, kuriuos CBP nustatė konsultuodamasi su Europos Komisija.

11. Laukdama, kol tokie kompiuteriniai filtrai bus įdiegti, CBP įsipareigoja nei dabar, nei ateityje nenaudoti „jautrių“ PNR duomenų ir, remiantis 28–34 dalimis, ištrinti „jautrius“ duomenis iš savo nuožiūra atskleidžiamų PNR duomenų [3].

PNR duomenų saugojimas

12. Nustatydami potencialius subjektus pasienio patikrinimui, CBP darbuotojai tikrins (arba gaus) tiesiogiai iš vežėjų oro transportu užsakymų sistemų PNR duomenis tik apie į Jungtines Amerikos Valstijas arba iš jų skrendančius asmenis, ir jais naudosi [4].

13. Kol vežėjai oro transportu nebus įdiegę sistemos, sugebančios perduoti duomenis CBP, CBP pati „išgaus“ informaciją apie keleivius iš vežėjų oro transportu užsakymų sistemų.

14. Siekdama nustatyti galimus informacijos pokyčius, CBP išgaus konkretaus skrydžio PNR duomenis ne anksčiau nei 72 valandos iki lėktuvo išskridimo ir pakartotinai patikrins sistemas daugiausiai tris (3) kartus nuo pirmojo duomenų gavimo iki lėktuvo išskridimo iš užsienyje esančios vietos ir atskridimo į Jungtines Amerikos Valstijas arba nuo pirmojo informacijos gavimo ir lėktuvo išskridimo iš Jungtinių Amerikos Valstijų. Jei vežėjai oro transportu tampa pajėgūs perduoti PNR duomenis, reikia, kad CBP [5] juos gautų likus 72 valandoms iki lėktuvo išskridimo, su sąlyga, kad ji gaus informaciją apie visus PNR duomenų pokyčius, įvykusius nuo to laiko iki lėktuvo atskridimo arba išskridimo iš Jungtinių Amerikos Valstijų. Neįprastu atveju, jei CBP iš anksto gaus informaciją, kad lėktuvu į, iš arba per Jungtines Amerikos Valstijas keliauja ypatingą susirūpinimą keliantis asmuo arba asmenys, ji gali gauti (arba pareikalauti perduoti) PNR duomenis likus daugiau nei 72 valandoms iki lėktuvo išskridimo, kad būtų galima užtikrinti būtinus teisėsaugos veiksmus, jei to reikėtų siekiant išvengti šio dokumento 3 dalyje nurodyto nusikaltimo ar su juo kovoti. Kai CBP turi gauti PNR duomenis likus daugiau kaip 72 valandoms iki lėktuvo išskridimo, tiek, kiek praktiškai įmanoma, ji naudosis įprastais teisėsaugos kanalais.

---

[2] Šioje nuostatoje CBP nelaikoma nei tiesiogiai CAPPS II tikrinime dalyvaujančia šalimi, nei „trečiąja šalimi“.

[3] Kol CBP nebus įdiegusi kompiuterinių filtrų (kaip nurodyta šio dokumento 10 dalyje), jei PNR nurodyti „jautrūs“ duomenys, kuriuos, kaip tai nurodyta 35 dalyje, CBP atskleidė ne savo nuožiūra, ji dės visas pastangas riboti „jautrių“ PNR duomenų perdavimą laikydamasi JAV teisės nuostatų.

[4] Čia turėtų būti įtraukti ir per Jungtines Valstijas tranzitu keliaujantys asmenys.

[5] Jei vežėjai oro transportu sutinka CBP perduoti PNR duomenis, tarnyba aptars su vežėjais oro transportu galimybę perduoti PNR duomenis, priklausomai nuo situacijos, arba periodiškai per 72 valandas iki lėktuvo išskridimo iš užsienyje esančios vietos ir atskridimo į Jungtines Amerikos Valstijas, arba per 72 valandas likusias iki lėktuvo išskridimo iš Jungtinių Amerikos Valstijų. CBP siekia naudotis PNR duomenų perdavimo metodu, kuris atitinka tarnybos veiksmingo rizikos įvertinimo poreikius, tuo pat metu mažindama ekonominį poveikį vežėjams oro transportu.

PNR duomenų saugojimas

15. Gavus Nacionalinių archyvų ir registrų administracijos (*National Archives and Records Administration*) leidimą (44 U.S. C. 2101, *et seq*.), CBP leis įgaliotiems CBP vartotojams [6] septynias (7) dienas naudotis elektroniniais PNR duomenimis, tam laikotarpiui pasibaigus, bus dar labiau sumažintas pareigūnų, galinčių susipažinti su PNR duomenimis skaičius, tokią teisę jiems suteikiant trejiems metams ir 6 mėnesiams (3,5 metų) skaičiuojant nuo prieigos prie vežėjo oro transportu užsakymų sistemos duomenų (arba jų gavimo) dienos. Po 3,5 metų bus sunaikinti per tą laikotarpį rankiniu būdu neieškoti PNR duomenys. CBP perkels į ištrintų įrašų rinkmeną, joje aštuonerius (8) metus laikys ir tik po to sunaikins per pradinį 3,5 metų laikotarpį rankiniu būdu išgautus PNR duomenis [7]. Tačiau toks tvarkaraštis nebus taikomas su konkrečiais teisėtvarkos įrašais susijusiems duomenims (tokiais duomenimis bus galima naudotis tik iki teisėtvarkos įrašų patalpinimo į archyvą). Nepaisant galimos Įsipareigojimų galiojimo pabaigos pagal šio dokumento 46 dalį, PNR duomenims, su kuriais šių Įsipareigojimų galiojimo metu buvo susipažinta, arba jie buvo tiesiogiai gauti iš vežėjo oro transportu užsakymų sistemos, CBP taikys šioje dalyje apibrėžtą duomenų laikymo politiką.

CBP kompiuterių sistemos saugumas

16. Įgalioti CBP darbuotojai prisijungia prie PNR per uždarą, nuo pradžios iki pabaigos koduotą CBP vidinio tinklo sistemą; prisijungimą kontroliuoja Muitinės duomenų centras. CBP duomenų bazėje saugomi PNR gali būti naudojami tik įgaliotų darbuotojų ir tik skaitymui, t. y. duomenų turinys gali būti programiškai performuotas, bet jokiu būdu nebus iš esmės pakeistas, CBP prisijungus prie vežėjo oro transportu užsakymų sistemos.

17. Jokia kita užsienio, federalinė, valstijos ar vietos tarnyba negali tiesiogiai elektroniniu būdu prisijungti prie PNR duomenų naudodamasi CBP duomenų bazėmis (įskaitant Tarpžinybinę pasienio tikrinimo sistemą (*Interagency Border Inspection System*, toliau – IBIS)).

18. Siekiant išvengti naudojimosi sistema be leidimo, Vidaus reikalų tarnyba (*Office of Internal Affairs*) automatiškai registruoja ir reguliariai tikrina informaciją apie prisijungimą prie CBP duomenų bazių informacijos (kas, kur, kada (data ir laikas) prisijungė, ir kokie duomenys buvo peržiūrimi).

19. PNR duomenimis gali naudotis tik tie CBP pareigūnai, darbuotojai arba informacijos technologijų rangovai [8] (prižiūrint CBP), kurių biografija buvo sėkmingai patikrinta ir kurie CBP kompiuterių sistemoje turi aktyvią, slaptažodžiu saugomą sąskaitą bei patvirtintą oficialų tikslą susipažinti su PNR duomenimis.

20. CBP pareigūnai, darbuotojai ir rangovai privalo išklausyti kas dvejus metus saugumo ir duomenų privatumo kursus, taip pat išlaikyti testus. CBP sistemos auditas atliekamas siekiant stebėti ir užtikrinti visų privatumo ir duomenų saugumo reikalavimų laikymąsi.

21. CBP darbuotojams, kurie be leidimo prisijungė prie vežėjo oro transportu užsakymų sistemų arba prie PNR saugojančios CBP kompiuterinės sistemos, taikomos griežtos drausminės nuobaudos (įskaitant pašalinimą iš darbo) ir galimos baudžiamosios sankcijos (baudos, įkalinimas iki vienerių metų arba tiek viena, tiek kita) (žr. *title 18, United States Code, section 1030*).

22. CBP politika ir taisyklės taip pat numato griežtas drausmines nuobaudas (įskaitant pašalinimą iš darbo), kurios gali būti taikomos kiekvienam CBP darbuotojui be oficialaus leidimo atskleidusiam CBP kompiuterinių sistemų informaciją (*title 19, Code of Federal Regulations, section 103.34*).

23. Baudžiamojo pobūdžio sankcijos (įskaitant baudas, įkalinimą iki vienerių metų arba tiek viena, tiek kita) gali būti taikomos kiekvienam Jungtinių Amerikos Valstijų pareigūnui arba darbuotojui, atskleidusiam PNR duomenis, gautus darbo metu, jei toks atskleidimas nėra leidžiamas įstatymu (žr. *title 18, United States Code, sections 641, 1030, 1905*).

---

[6] Tokiais įgaliotais CBP vartotojais būtų vietinių tarnybų analitinių skyrių darbuotojai bei Nacionalinio planavimo skyriaus darbuotojai. Kaip minėta anksčiau, už CBP duomenų bazės prižiūrėjimą, tobulinimą ar auditą atsakingi asmenys taip pat galės naudotis tokia informacija minėtais ribotais tikslais.

[7] Nors PNR įrašas nebuvo techniškai ištrintas jį patalpinant į Ištrintų įrašų rinkmeną, jis saugomas kaip neapdoroti duomenys (paieškai neparuoštos formos ir todėl nenaudotinas vykdant „įprastinius“ teisėsaugos tyrimus) ir prieinamas tik esant poreikiui gauti informaciją („*need to know*“) įgaliotiems CBP Vidaus reikalų tarnybos darbuotojams (ir tam tikrais su auditu susijusiais atvejais – Generalinio inspektoriaus tarnybai (*Office of the Inspector General*)) bei darbuotojams, atsakingiems už CBP Informacijos technologijų tarnybos duomenų bazės palaikymą.

[8] „Rangovų“ teisė susipažinti su CBP kompiuterių sistemose laikomais PNR duomenimis turėtų būti patikėta asmenims, sudariusiems su CBP sutartį dėl pagalbos prižiūrint arba tobulinant CBP kompiuterių sistemą.

Kaip CBP elgiasi su PNR duomenimis ir kaip juos saugo

24. CBP laiko PNR duomenis bet kokios pilietybės ar šalies gyventojų atžvilgiu jautria teisėsaugos požiūriu, konfidencialia asmenine duomenų subjekto informacija ir konfidencialia komercine vežėjo oro transportu informacija, ir todėl neatskleis tokios informacijos visuomenei, išskyrus taip, kaip nurodyta šiuose Įsipareigojimuose, arba kitu būdu, kai to reikalauja įstatymas.

25. Viešą PNR duomenų atskleidimą paprastai reglamentuoja Informacijos laisvės aktas (*Freedom of Information Act*, toliau – FOIA) (*title 5, United States Code, section 552*), kuris leidžia kiekvienam asmeniui (nepaisant jo pilietybės ar šalies, kurioje jis gyvena) susipažinti su JAV federalinės tarnybos įrašais, išskyrus tokius įrašus (ar jų dalį), kurie yra neatskleidžiami viešai taikant FOIA numatytą išimtį. Tokioms FOIA nurodytoms išimtims priklauso tarnybai suteikiamas leidimas neatskleisti įrašo (arba jo dalies), jei tokia informacija yra konfidenciali komercinė informacija, jei tokios informacijos atskleidimas reikštų aiškų nesankcionuotą kišimąsi į privatumą arba, kai informacija renkama teisėsaugos tikslais, tiek, kiek toks atskleidimas gali pagrįstai būti laikomas nesankcionuotu kišimusi į privatumą (*title 5, United States Code, sections 552(b)(4), (6), (7)(C)*).

26. CBP taisyklės (*title 19, Code of Federal Regulations, section 103.12*), kurios reglamentuoja prašymų suteikti informaciją (pavyzdžiui, PNR duomenų) nagrinėjimą, remiantis FOIA, konkrečiai numato, kad (laikantis tam tikrų ribotų išimčių, kai duomenų subjektas pateikia prašymą) FOIA atskleidimo reikalavimai netaikomi CBP įrašams, susijusiems su: 1) konfidencialia komercine informacija; 2) medžiaga, kuri yra susijusi su privačia informacija, kurios atskleidimas reikštų aiškiai nesankcionuotą kišimąsi į privatumą, ir 3) teisėsaugos tikslais surinkta informacija, kurios atskleidimas reikštų nesankcionuotą kišimąsi į privatumą ([9]).

27. Bet kokių administracinių ar teisminių procesų dėl FOIA prašymo pateikti iš vežėjų oro transportu gautus PNR duomenis atžvilgiu CBP laikosi pozicijos, kad FOIA leidžia tokių įrašų neatskleisti.

PNR duomenų perdavimas kitoms vyriausybės institucijoms

28. Išskyrus CBP ir TSA tarpusavio perdavimus pagal šio dokumento 8 dalį, Krašto saugumo departamento (*Department of Homeland Security*, toliau – DHS) struktūriniai padaliniai bus laikomi „trečiosiomis tarnybomis“, kurioms bus taikomos tos pačios taisyklės ir sąlygos dėl dalinimosi PNR duomenimis kaip ir kitoms DHS nepriklausančioms vyriausybės įstaigoms.

29. Siekiant išvengti šio dokumento 3 dalyje nurodytų nusikaltimų ir su jais kovoti, CBP savo nuožiūra, atskirai atsižvelgdama į kiekvieną atvejį, suteiks PNR duomenis kitoms su terorizmu kovojančioms ir teisėsaugos funkcijas atliekančioms vyriausybės institucijoms, įskaitant užsienio vyriausybių institucijas. (Institucijos, su kuriomis CBP gali dalintis tokia informacija, toliau vadinamos „Paskirtosiomis institucijomis“).

30. CBP apgalvotai naudosis teise savo nuožiūra perduoti PNR duomenis nustatytais tikslais. CBP pirmiausiai išsiaiškins, ar PNR duomenų atskleidimo kitai Paskirtajai institucijai priežastis atitinka nustatytą tikslą (žr. šio dokumento 29 dalį). Jei taip, CBP nustatys, ar Paskirtoji institucija yra atsakinga už pažeidimų prevenciją, tyrimą, ar persekiojimą arba su tuo tikslu susijusių teisės aktų ar taisyklių vykdymą arba įgyvendinimą, kai CBP žino apie tokio teisės pažeidimo arba potencialaus pažeidimo požymius. Sprendimas atskleisti duomenis turės būti peržiūrimas atsižvelgiant į visas nurodytas aplinkybes.

31. PNR duomenų, kuriais gali būti dalinamasi su kitomis Paskirtosiomis institucijomis, požiūriu CBP yra laikoma duomenų „savininke“; aiškios atskleidimo sąlygos įpareigoja tokias Paskirtąsias institucijas: 1) naudoti PNR duomenis tik šio dokumento atitinkamai 29 ir 34 dalyse nurodytais tikslais; 2) užtikrinti gautų PNR duomenų tinkamą sunaikinimą, laikantis Paskirtosios institucijos įrašų laikymo procedūrų, ir 3) skleisti informaciją toliau tik gavus aiškų CBP leidimą. Sąlygų dėl perdavimo nesilaikymo atvejai gali būti tiriami ir apie juos pranešama DHS vyriausiajam privatumo reikalų pareigūnui, ir todėl Paskirtajai institucijai gali būti atimta teisė iš CBP toliau gauti PNR duomenis.

([9]) CBP taikytų šias išimtis vienodai, neatsižvelgdama į tikrinamojo asmens pilietybę ar šalį, kurioje jis gyvena.

32. Kiekvienam CBP PNR duomenų atskleidimui bus taikoma tokia sąlyga, kad gaunančioji tarnyba turės laikyti šiuos duomenis konfidencialia komercine informacija ir jautria teisėsaugos požiūriu, konfidencialia asmenine duomenų subjekto informacija, kaip tai nurodyta šio dokumento 25 ir 26 dalyse, kurios atskleidimo negalima reikalauti remiantis Informacijos laisvės aktu (5 U.S.C. 552). Be to, gaunančioji tarnyba bus informuota, kad tokią informaciją toliau skleisti leidžiama tik gavus aiškų išankstinį CBP pritarimą. CBP leis toliau perduoti PNR duomenis tik šio dokumento 29, 34 arba 35 dalyse nurodytais tikslais.

33. Tokiose Paskirtosiose institucijose dirbantiems asmenims, be tinkamo leidimo atskleidusiems PNR duomenis, gali būti taikomos baudžiamojo pobūdžio sankcijos (*title 18, United States Code, sections 641, 1030, 1905*).

34. Jokia šio dokumento nuostata negali trukdyti susijusioms vyriausybės institucijoms naudotis PNR duomenimis arba juos atskleisti, kai toks atskleidimas reikalingas duomenų subjekto arba kitų asmenų gyvybiškai svarbių interesų apsaugai, ypač iškilus dideliam pavojui sveikatai. Informacijos atskleidimui tokiais tikslais bus taikomos šių Įsipareigojimų 31 ir 32 dalyse nurodytos sąlygos.

35. Jokia šių Įsipareigojimų nuostata negali trukdyti naudotis PNR duomenimis arba juos atskleisti baudžiamajame procese ar kitais teisės numatytais atvejais. CBP informuos Europos Komisiją apie visus išleistus Jungtinių Amerikos Valstijų teisės aktus, kurie iš esmės įtakos šių Įsipareigojimų nuostatas.

PNR duomenų subjektų informavimas, galimybė gauti informaciją ir pareikšti prieštaravimus

36. CBP supažindins keliaujančius asmenis su PNR duomenims keliamais reikalavimais ir su jų naudojimu susijusiais klausimais (pvz., bendra informacija apie įgaliojimus, kuriais remiantis renkami duomenys, rinkimo tikslas, duomenų apsauga, dalijimasis duomenimis, atsakingojo pareigūno tapatybė, prieštaravimų pareiškimo procedūros ir kontaktinė informacija asmenims, turintiems klausimų ar rūpesčių, ir t. t., kurią bus galima gauti tinklalapyje, kelionės lankstinukuose ir t. t.).

37. Duomenų subjekto (taip pat vadinamo „pirmojo lygmens prašytoju“) prašymas gauti CBP duomenų bazėje laikomo PNR apie jį kopiją nagrinėjamas vadovaujantis Informacijos laisvės aktu. Tokie prašymai turi būti siunčiami paštu šiuo adresu: *Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229* arba pristatomi asmeniškai Informacijos atskleidimo pareigūnui Jungtinių Amerikos Valstijų Muitinės ir pasienio apsaugos būstinėje (*Disclosure Law Officer, U.S. Customs and Border Protection, Headquarters*) Vašingtone, Kolumbijos apygardoje. Papildomą informaciją apie prašymų pateikimo pagal FOIA procedūras rasite *section 103.5 of title 19 of the U.S. Code of Federal Regulations*. Kai pateikiamas pirmojo lygmens prašymas, CBP nesirems tuo faktu, kad CBP paprastai laiko PNR duomenis konfidencialia duomenų subjekto asmens informacija ir konfidencialia vežėjo oro transportu komercine informacija, t. y. pagrindu pagal FOIA neišduoti duomenų subjektui PNR duomenų.

38. Kai kuriais išskirtiniais atvejais CBP gali pasinaudoti FOIA nurodyta teise atsisakyti arba atidėti atskleidimą viso (arba, dažniau, dalies) PNR įrašo pirmojo lygmens prašytojui pagal *title 5, United States Code, section 552(b)* (pvz. jei, kaip nurodyta FOIA, duomenų atskleidimas „galėtų pagrįstai sutrukdyti teisėsaugos procesams“ arba „atskleistų teisėsaugos tyrimų techniką ir procedūras… (kas) pagrįstai reikštų įstatymo pažeidimą“). FOIA teigiama, kad kiekvienas prašytojas turi teisę administraciniu arba teisiniu būdu užginčyti CBP sprendimą nesuteikti informacijos (žr. *5 U.S.C. 552a)4)B); 19 CFR 103.7–103.9*).

39. CBP įsipareigoja keisti ([10]) informaciją keleivių, įgulos narių, vežėjų oro transportu arba Duomenų apsaugos institucijų (DAI) ES valstybėse narėse prašymu (tiek, kiek konkrečiai leidžia duomenų subjektas), kai CBP nustato, jog tokie duomenys yra jos duomenų bazėje, ir toks ištaisymas yra pateisinamas ir tinkamai pagrįstas. CBP praneš tokiai PNR duomenų gavusiai Paskirtajai institucijai apie visus tokių PNR duomenų esminius pakeitimus.

([10]) CBP nori pareikšti, kad terminas „keisti“ nesuteikia jai teisės keisti tuos PNR duomenis, kuriuos ji gauna iš vežėjų oro transportu sistemų. Atvirkščiai, bus sukurtas atskiras, su konkrečiais PNR duomenimis susijęs, įrašas, kuriame bus pažymėta, kad paaiškėjo, jog informacija yra netiksli, taip pat atliktas atitinkamas ištaisymas. Konkrečiai, CBP pateiks keleivio antrinio patikrinimo įraše komentarus apie tai, kad dalis PNR duomenų yra arba gali būti netikslūs.

40. Prašymai dėl PNR, esančių CBP duomenų bazėje, pakeitimų ir privačių asmenų skundai dėl to, kaip CBP tvarko jų PNR duomenis, gali būti pateikiami tiesiogiai arba per atitinkamą DAI (jei ją konkrečiai nurodo duomenų subjektas) komisaro pavaduotojui: *Assistant Commissioner, Office of Field Operations, U.S. Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229*.

41. Jei CBP negali patenkinti skundo, jis gali būti persiunčiamas vyriausiajam privatumo reikalų pareigūnui: *Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528*, kuris apsvarstys situaciją ir stengsis skundą patenkinti ([11]).

42. Be to, DHS Privatumo reikalų tarnyba (*DHS Privacy Office*) skubos tvarka peržiūrės Europos Sąjungos (ES) valstybių narių DAI persiųstus ES gyventojų skundus, jei tokie gyventojai įgaliojo DAI atlikti veiksmus jų vardu, ir mano, kad jų skundą dėl jų PNR duomenų apsaugos CBP arba DAI Privatumo reikalų tarnyba neišnagrinėjo tinkamai (kaip nurodyta šių Įsipareigojimų 37–41 dalyse). Privatumo reikalų tarnyba praneš apie savo išvadas ir įvertins suinteresuotų DAI arba DAI-ų atliktus veiksmus, jei tokių buvo. DHS vyriausiasis privatumo reikalų pareigūnas įtrauks į savo ataskaitą Kongresui medžiagą apie tai, kiek ir kokių skundų dėl asmeninio pobūdžio informacijos, pvz., PNR duomenų, buvo pateikta, ir kaip jie buvo patenkinti ([12]).

Įsipareigojimų laikymasis

43. CBP, kartu su DHS įsipareigoja kartą per metus arba dažniau, jei šalys taip sutars, atlikti bendrą su Europos Komisija peržiūrą, prireikus padedant Europos teisėtvarkos institucijoms ir (arba) Europos Sąjungos ([13]) valstybių narių institucijoms, išsiaiškinant, kaip įgyvendinami šie Įsipareigojimai, siekiant abipusiai prisidėti prie šiuose Įsipareigojimuose apibūdintų procesų efektyvaus veikimo.

44. CBP paskelbs taisykles, direktyvas arba kitus politikos dokumentus su šiame dokumente paminėtomis nuostatomis, taip siekdama, kad šių Įsipareigojimų laikytųsi CBP pareigūnai, darbuotojai ir rangovai. Kaip nurodyta šiame dokumente, jei CBP pareigūnai, darbuotojai arba rangovai nesilaikys minėtuose dokumentuose nurodytos politikos, jiems gali būti taikomos griežtos drausminės nuobaudos, o prireikus baudžiamojo pobūdžio sankcijos.

Abipusiškumas

45. Jei Europos Sąjungoje įgyvendinama tokia oro linijų keleivių atpažinimo sistema, pagal kurią reikalaujama, kad vežėjai oro transportu suteiktų institucijoms galimybę susipažinti su PNR duomenimis apie asmenis, kurių galiojantį kelionės maršrutą sudaro skrydis į Europos Sąjungą ar iš jos, CBP privalo griežtai laikydamasi abipusiškumo principo, skatinti Jungtinių Amerikos Valstijų oro linijas bendradarbiauti.

Įsipareigojimų peržiūra ir nutraukimas

46. Šie Įsipareigojimai taikomi trejus metus ir šešis mėnesius (3,5 metų) nuo Jungtinių Amerikos Valstijų ir Europos bendrijos susitarimo įsigaliojimo datos, leisdami vežėjams oro transportu tvarkyti PNR duomenis siekiant juos perduoti CBP pagal Direktyvos reikalavimus. Praėjus dvejiems metams ir šešiems mėnesiams (2,5 metų) nuo tokių Įsipareigojimų įsigaliojimo, CBP kartu su DHS pradės diskusijas su Komisija siekdamos pratęsti Įsipareigojimų ir kitų papildomų susitarimų galiojimo laiką abipusiai priimtinomis sąlygomis. Jei iki šių Įsipareigojimų galiojimo pabaigos nerandama abipusiai priimtinos tvarkos, nuo tos datos jie tampa negaliojančiais.

([11]) DAI vyriausiasis privatumo reikalų pareigūnas (*Chief Privacy Office*) yra nepriklausomas nuo jokio Krašto saugumo departamento. Remiantis įstatymu jis yra įpareigotas užtikrinti, kad asmeninė informacija būtų naudojama laikantis atitinkamų įstatymų (žr. 13 išnašą). Departamentas turi paklusti vyriausiojo privatumo reikalų pareigūno sprendimams, jie negali būti panaikinti dėl politinių priežasčių.

([12]) Pagal 2002 m. Krašto saugumo akto (*Homeland Security Act*, toliau – Aktas) 222 skirsnį (2002 m. lapkričio 25 d. *Public Law 107–296*), DHS privatumo reikalų pareigūnas yra įpareigotas atlikti Departamento pateiktų taisyklių dėl „asmeninės informacijos privatumo, įskaitant surinktos asmeninės informacijos rūšį ir paveiktų žmonių skaičių“ „įtakos privatumui įvertinimą“, ir kasmet atsiskaityti Kongresui apie „Departamento veiklą, kuri daro įtaką privatumui …“. Akto 222 skirsnio 5 dalis taip pat aiškiai nurodo DHS privatumo reikalų pareigūnui susipažinti ir pranešti Kongresui apie visus „skundus dėl privatumo pažeidimo.“

([13]) Abiem šalims iš anksto bus pranešta apie grupių, kurias gali sudaryti atitinkamos institucijos, susijusios su privatumo ir duomenų apsauga, muitinės kontrole ir kitomis teisėsaugos formomis, pasienio apsauga ir (arba) aviacijos saugumu, sudėtį. Dalyvaujančios institucijos turės atlikti reikalaujamus saugumo patikrinimus ir įsipareigos neatskleisti pokalbių ir dokumentų, kuriais joms gali būti leista naudotis, turinio. Tačiau konfidencialumas netaps kliūtimi nei vienai iš šalių pateikiant atitinkamą pranešimą apie bendros peržiūros rezultatus jų kompetentingoms institucijoms, įskaitant Jungtinių Amerikos Valstijų Kongresą ir Europos Parlamentą. Tačiau jokiomis aplinkybėmis dalyvaujančios institucijos negalės atskleisti jokios asmeninės informacijos apie duomenų subjektą; dalyvaujančios institucijos taip pat neturės teisės atskleisti jokios ne viešos informacijos, gautos iš dokumentų, kuriais joms buvo leista naudotis, ar iš bendros peržiūros metu gautos tarnybos operatyvinės ar vidaus informacijos. Abi šalys kartu nustatys išsamią bendros peržiūros tvarką.

Privačios teisės ir precedento nebuvimas

47. Šie Įsipareigojimai nesukuria ir nesuteikia jokios teisės ar privilegijos jokiam privačiam ar viešam asmeniui ar šaliai.

48. Šių Įsipareigojimų nuostatos nesukuria precedento jokioms būsimoms diskusijoms su Europos Komisija, Europos Sąjunga ar kokiu kitu susijusiu subjektu arba trečiąja valstybe dėl duomenų perdavimo bet kokia forma.

2004 m. gegužės 11 d.

A PRIEDĖLIS

PNR duomenų elementai, kurių CBP reikalauja iš vežėjų oro transportu

1. PNR įrašų aptikimo kodas
2. Užsakymo data
3. Planuotos kelionės data (datos)
4. Vardas, pavardė
5. Kiti vardai, pavardės PNR
6. Adresas
7. Informacija apie visas mokėjimo formas
8. Sąskaitos pateikimo adresas
9. Kontaktiniai telefono numeriai
10. Konkretaus keleivio PNR kelionės tvarkaraštis
11. Keleivio, dažnai keliaujančio lėktuvais, informacija (apsiribojama nukeliautomis myliomis ir adresu (adresais))
12. Kelionių agentūra
13. Kelionių agentas
14. Dalijimosi PNR informacija kodas
15. Keleivio kelionės statusas
16. Dalis (arba padalinta) PNR informacija
17. Elektroninio pašto adresas
18. Informacija apie bilietą
19. Bendros pastabos
20 Bilieto numeris
21. Vietos numeris
22. Bilieto išdavimo data
23. Informacija apie neatvykimą (*no show*)
24. Bagažo registracijos numeriai
25. Informacija apie bilietus, nupirktus jų nerezervavus (*go show*)
26. OSI informacija
27. SSI/SSR informacija
28. Gauta iš informacijos
29. Visa PNR keitimo istorija
30. PNR nurodytas keleivių skaičius
31. Informacija apie keleivio vietą
32. Bilietai į vieną pusę
33. Visa surinkta APIS informacija
34. ATFQ laukai