EUROPOS
KOMISIJA

Briuselis, 2016 04 06
COM(2016) 205 final

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI

Patikimesnės ir pažangesnės sienų ir saugumo informacinės sistemos

1. ĮVADAS

Europa yra mobili visuomenė. Kas dieną milijonai ES ir trečiųjų šalių piliečių kerta vidaus ir išorės sienas. 2015 m. Europos Sąjungoje lankėsi daugiau kaip 50 milijonų ne ES piliečių – jie daugiau kaip 200 mln. kartų kirto Šengeno erdvės išorės sienas.

Be šių teisėtų keliaujančių asmenų srautų vien tik 2015 m. dėl konflikto Sirijoje ir dėl kitur kilusių krizių nustatyta 1,8 mln. neteisėtų Europos išorės sienos kirtimo atvejų. ES piliečiai tikisi, kad išorės sienas kertančių asmenų kontrolė yra veiksminga siekiant užtikrinti veiksmingą migracijos valdymą ir didinti vidaus saugumą. 2015 m. Paryžiuje ir 2016 m. kovo mėn. Briuselyje įvykdyti skaudūs teroristiniai išpuoliai parodė, kad Europos vidaus saugumui ir toliau iškilusi grėsmė.

Abu šie elementai privertė atidžiau pažvelgti į būtinybę visapusiškai suvienyti ir sustiprinti ES bendradarbiavimo sienų valdymo, migracijos ir saugumo srityje sistemas bei informacines priemones. Sienų valdymas, teisėsauga ir migracijos kontrolė yra dinamiškai tarpusavyje susieti. Yra žinoma, kad ES piliečiai yra kirtę išorės sienas, kad galėtų nuvykti į konfliktų zonas teroristiniais tikslais – sugrįžę jie kelia pavojų. Esama įrodymų, kad teroristai pasinaudojo neteisėtos migracijos į ES maršrutais, kad patektų į ES, o vėliau nepastebėti keliavo Šengeno erdvės viduje.

Siekiant spręsti susijusias migracijos valdymo ir kovos su terorizmu bei organizuotu nusikalstamumu problemas Europos saugumo ir migracijos darbotvarkėse buvo nustatytos ES politikos plėtros ir įgyvendinimo gairės. Šis komunikatas grindžiamas šių abiejų darbotvarkių sąveika ir skirtas pradėti diskusiją apie tai, kaip esamomis ir būsimomis informacinėmis sistemomis būtų galima sustiprinti tiek ES išorės sienų valdymą, tiek vidaus saugumą. Jis papildo 2015 m. gruodžio mėn. pasiūlymą įsteigti Europos sienų ir pakrančių apsaugos pajėgas ir gerinti krizių prevenciją bei intervenciją prie išorės sienų.

Esama kelių ES lygmens informacinių sistemų, kuriomis sienos apsaugos pareigūnams ir policijos pareigūnams teikiama atitinkama informacija apie asmenis, tačiau ES duomenų valdymo struktūra nėra tobula. Šiame komunikate nurodomos kelios galimybės, kaip kuo labiau padidinti esamų informacinių sistemų naudingumą ir, jei reikia, parengti naujus papildomus veiksmus spragoms šalinti. Jame taip pat pabrėžiamas ilgalaikis tikslas – būtinybė pagerinti informacinių sistemų sąveikumą (šį tikslą taip pat nustatė Europos Vadovų Taryba ir Taryba[1]), ir pateikiamos idėjos, kaip informacinės sistemos galėtų būti kuriamos ateityje siekiant užtikrinti, kad sienos apsaugos pareigūnai, muitinės, policijos pareigūnai ir teisminės institucijos galėtų gauti joms reikalingos informacijos.

Bet kokia būsima iniciatyva būtų rengiama remiantis geresnio reglamentavimo principais, viešomis konsultacijomis ir poveikio vertinimu, ir atsižvelgiant į pagrindines teises, ypač teisę į asmens duomenų apsaugą.

[1] 2015 m. gruodžio 17–18 d. Europos Vadovų Tarybos susitikimo išvados; ES teisingumo ir vidaus reikalų ministrų ir ES institucijų atstovų bendras pareiškimas dėl 2016 m. kovo 22 d. Briuselyje įvykdytų teroristinių išpuolių (2016 m. kovo 24 d.); ES Tarybos ir Taryboje posėdžiavusių valstybių narių išvados dėl kovos su terorizmu (2015 m. lapkričio 20 d.).

2. SPRĘSTINOS PROBLEMOS

Kadangi Šengeno erdvėje nėra vidaus sienų, būtina geriau ir patikimiau valdyti išorės sienas kertančių asmenų judėjimą. Tai būtina sąlyga siekiant šioje erdvėje užtikrinti aukšto lygio vidaus saugumą ir laisvą asmenų judėjimą. Taip pat tai, kad nėra vidaus sienų, reiškia, kad valstybių narių teisėsaugos institucijos irgi turi prieigą prie atitinkamų duomenų apie asmenis. Yra keletas ES lygmens informacinių sistemų ir duomenų bazių, kuriomis sienos apsaugos pareigūnams, policijos pareigūnams ir kitoms institucijoms teikiama atitinkama informacija apie asmenis atsižvelgiant į jų atitinkamus tikslus[2].

Tačiau informacinės sistemos turi ir trūkumų, kurie apsunkina šių nacionalinių institucijų darbą. Todėl Europos saugumo darbotvarkėje geresnis keitimasis informacija buvo išskirtas kaip svarbus prioritetas. Pagrindiniai trūkumai: a) nepakankamas esamų informacinių sistemų funkcionalumas, b) ES duomenų valdymo struktūros spragos, c) sudėtinga skirtingai reglamentuojamų informacinių sistemų įvairovė ir d) suskaidyta sienų kontrolės ir saugumo srities duomenų valdymo struktūra.

Esamos ES sienų valdymui ir vidaus saugumui skirtos informacinės sistemos atlieka labai įvairias funkcijas. Nepaisant to, **esamų sistemų funkcijos tebeturi trūkumų**. Vertinant sienų kontrolės procesus, taikomus skirtingų kategorijų keliautojams, paaiškėja, kad kai kurie iš šių procesų turi trūkumų, taip pat esama trūkumų atitinkamose sienų kontrolei skirtose informacinėse sistemose. Be to, būtina optimizuoti esamų teisėsaugos priemonių veiksmingumą. Todėl reikia apsvarstyti, kokių veiksmų reikėtų imtis siekiant patobulinti esamas informacines sistemas (5 skirsnis).

Be to, **ES duomenų valdymo struktūroje esama spragų**. Vis dar esama probleminių klausimų dėl tam tikrų kategorijų sieną kertančių keliautojų, pvz., trečiųjų šalių piliečių, turinčių ilgalaikę vizą, kontrolės. Taip pat neturima informacijos apie trečiųjų šalių piliečius, kuriems taikomas bevizis režimas, prieš jiems atvykstant prie sienos. Reikėtų apsvarstyti, ar būtina šiuos trūkumus šalinti reikiamais atvejais sukuriant papildomą informacinę sistemą (6 skirsnis).

Sienos apsaugos pareigūnai, ypač policijos pareigūnai, ES lygmeniu susiduria su **sudėtinga skirtingai reglamentuojamų informacinių sistemų įvairove**. Dėl tokios sudėtingos įvairovės iškyla praktinių sunkumų, ypač kiekvienu konkrečiu atveju sunku nuspręsti, kuriose duomenų bazėse turi būti tikrinama informacija. Be to, ne visos valstybės narės yra prisijungusios prie visų esamų sistemų[3]. Dabartinė problema, kai sunku gauti prieigą prie ES lygmens informacinių sistemų, galėtų būti iš dalies išspręsta sukūrus bendrą nacionalinio lygmens paieškos sąsają, kuri atitiktų skirtingus prieigos tikslus (7.1 skirsnis).

Dabartinė ES sienų kontrolės ir saugumo srities duomenų valdymo struktūra yra **suskaidyta**. Taip yra dėl įvairių institucinių, teisinių ir politinių aplinkybių, kurioms esant buvo sukurtos šios sistemos. Informacija yra saugoma atskirai įvairiose sistemose, kurios retai būna tarpusavyje sujungtos. Esama neatitikimų tarp duomenų bazių, o atitinkamos institucijos turi nevienodą prieigą prie duomenų. Dėl to gali atsirasti visų pirma teisėsaugos institucijoms nematomų pilkųjų zonų, nes gali būti labai sunku atpažinti ryšį tarp duomenų fragmentų. Todėl būtina skubiai kurti integruotus sprendimus, kad būtų pagerinta prieiga prie duomenų sienų valdymo ir saugumo tikslais

[2] Žr. 4 skirsnį, kuriame pateikta sienų ir saugumo srities informacinių sistemų apžvalga, ir 2 priedą, kuriame pateikta išsamesnės informacijos.

[3] Vadovaujantis 22 protokolo dėl Danijos ir 21 bei 36 protokolų dėl Jungtinės Karalystės ir Airijos konkrečiomis sąlygomis ir atitinkamais Stojimo aktais.

visapusiškai laikantis pagrindinių teisių. Tam reikia inicijuoti procesą, kuriuo būtų siekiama esamų informacinių sistemų sąveikumo (7 skirsnis).

3. PAGRINDINĖS TEISĖS

Visapusiška pagarba pagrindinėms teisėms ir visapusiškas duomenų apsaugos taisyklių laikymasis yra svarbi išankstinė sąlyga siekiant spręsti bet kurias iš minėtų problemų.

Kad būtų užtikrintas pagrindinių teisių laikymasis, būtinos tinkamai sukurtos ir teisingai naudojamos technologijos ir informacinės sistemos. Technologijos ir informacinės sistemos gali padėti viešosioms institucijoms apsaugoti pagrindines piliečių teises. Biometrinės technologijos gali sumažinti riziką, kad tapatybė bus nustatyta neteisingai, bus diskriminuojama arba taikomas rasinis skirstymas. Jos taip pat gali padėti spręsti vaikų apsaugai kylančios rizikos klausimus (pvz., dingusių vaikų arba nuo prekybos žmonėmis nukentėjusių vaikų), jeigu šios technologijos naudojamos kartu su pagrindinių teisių apsaugos priemonėmis ir kitomis apsaugos priemonėmis. Jos gali sumažinti riziką, kad žmonės bus neteisingai sulaikyti ir suimti. Jos taip pat padės kovoti su terorizmu ir sunkiais nusikaltimais ir taip galės padėti didinti Šengeno erdvėje gyvenančių piliečių saugumą.

Sukūrus didelės apimties informacines sistemas taip pat gali iškilti rizika privatumui – tokią riziką reikia numatyti ir imtis atitinkamų veiksmų. Asmens duomenų rinkimas ir naudojimas šiose sistemose turi įtakos teisei į privatumą ir asmens duomenų apsaugą, kuri įtvirtinta Europos Sąjungos pagrindinių teisių chartijoje. Visos sistemos turi atitikti duomenų apsaugos principus ir būtinumo, proporcingumo, tikslų apribojimo bei duomenų kokybės reikalavimus. Turi būti įdiegtos apsaugos priemonės, galinčios užtikrinti duomenų subjektų teises, susijusias su jų privataus gyvenimo ir asmens duomenų apsauga. Duomenys turėtų būti saugomi tik tiek laiko, kiek to reikia pasiekti tikslui, dėl kurio jie buvo surinkti. Turi būti numatyti mechanizmai, užtikrinantys kruopštų rizikos valdymą ir veiksmingą duomenų subjektų teisių apsaugą.

2015 m. gruodžio mėn. teisėkūros institucijos pasiekė politinį susitarimą dėl duomenų apsaugos reformos. Priėmus naują Bendrąjį duomenų apsaugos reglamentą ir Duomenų apsaugos direktyvą, skirtus policijai ir baudžiamosios teisenos institucijoms[4], jie bus pradėti taikyti 2018 m. ir jais bus sukurta suderinta asmens duomenų tvarkymo sistema.

Tikslų apribojimas yra pagrindinis duomenų apsaugos principas, įtvirtintas Pagrindinių teisių chartijoje. Dėl skirtingų institucinių, teisinių ir politinių aplinkybių, kurioms esant buvo sukurtos ES lygmens informacinės sistemos, tikslų apribojimo principas buvo įgyvendintas suskaidžius informacijos valdymo struktūrą[5]. Tai yra viena iš priežasčių, dėl kurios ES sienų kontrolės ir vidaus saugumo srities duomenų valdymo struktūra yra suskaidyta. ES įdiegus naują visapusišką asmens duomenų apsaugos sistemą ir atlikus svarbius technologijų ir IT saugumo pakeitimus, galima lengviau įgyvendinti tikslų apribojimo principą prieigos prie saugomų duomenų ir jų naudojimo lygmeniu, visapusiškai laikantis Pagrindinių teisių chartijos ir naujausios Europos Teisingumo Teismo praktikos. Tokios apsaugos priemonės, kaip antai vienos sistemos duomenų suskaidymas ir specialios prieigos ir naudojimo taisyklės, skirtos kiekvienos kategorijos duomenims ir naudotojams, turėtų užtikrinti būtiną tikslų apribojimą įgyvendinant integruotus duomenų tvarkymo sprendimus. Tai sudaro sąlygas užtikrinti informacinių

[4] Žr. http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
[5] COM(2010) 385 final.

sistemų sąveikumą ir nustatyti būtinas griežtas prieigos ir naudojimo taisykles, nepažeidžiant esamo tikslų apribojimo principo.

ES duomenų apsaugos taisyklės šiuo metu grindžiamos pritaikytosios duomenų apsaugos ir standartizuotosios duomenų apsaugos principais. Komisija sieks vadovautis šia koncepcija rengdama naujas priemones, kurias įgyvendinant reikia naudoti informacines technologijas. Tai reiškia, kad asmens duomenų apsauga būtų integruota į siūlomos priemonės technologinį pagrindą, būtų tvarkomi tik konkrečiam tikslui būtini duomenys, o prieiga prie duomenų būtų suteikiama tik tiems subjektams, kuriems tokią informaciją būtina žinoti[6].

Komisija, spręsdama ES sienų kontrolės ir saugumo srities duomenų valdymo struktūros spragų ir trūkumų problemas, vadovausis Pagrindinių teisių chartijos reikalavimais, ypač naujos duomenų apsaugos reformos priemonėmis. Taip bus užtikrinta, kad informacinės sistemos šiose srityse toliau bus plėtojamos laikantis griežčiausių duomenų apsaugos standartų ir informacinės sistemos atitiks ir papildys pagrindines teises, įtvirtintas Pagrindinių teisių chartijoje.

4. SIENOMS IR SAUGUMUI SKIRTŲ INFORMACINIŲ SISTEMŲ APŽVALGA[7]

Visos esamos ES informacinės sistemos, skirtos sienų valdymui ir vidaus saugumui, turi savo atskirus tikslus, naudojimo paskirtis, teisinius pagrindus[8], naudotojų grupes ir institucinį kontekstą. Visos kartu jos sudaro sudėtingą susijusių duomenų bazių sistemą.

Trys pagrindinės ES sukurtos **centralizuotos informacinės sistemos** – tai i) Šengeno informacinė sistema (SIS), teikianti plataus spektro perspėjimus apie asmenis ir daiktus, ii) Vizų informacinė sistema (VIS), skirta duomenims apie trumpalaikes vizas, ir iii) sistema EURODAC, kurioje laikomi prieglobsčio prašytojų ir trečiųjų šalių piliečių, kurie neteisėtai kirto išorės sienas, pirštų atspaudų duomenys. Šios trys sistemos viena kitą papildo ir (išskyrus SIS) pirmiausia skirtos trečiųjų šalių piliečiams. Šios sistemos taip pat padeda nacionalinėms institucijoms kovoti su nusikalstamumu ir terorizmu[9]. Tai visų pirma pasakytina apie SIS – šiuo metu tai plačiausiai naudojama dalijimosi informacija priemonė. Šiose sistemose duomenimis keičiamasi naudojant saugią tikslinę komunikacijos infrastruktūrą, vadinamą sTESTA[10].

Be šių esamų sistemų, Komisija siūlo sukurti ketvirtą centralizuotą sienų valdymo sistemą – **atvykimo ir išvykimo sistemą** (EES)[11], kurią tikimasi įgyvendinti iki 2020 m. Ji irgi būtų skirta trečiųjų šalių piliečiams.

---

[6] Privatumo užtikrinimas projektuojant išsamiai aprašytas Europos duomenų apsaugos priežiūros pareigūno nuomonėje dėl pasitikėjimo informacinėje visuomenėje skatinimo, stiprinant duomenų apsaugą ir privatumą, Europos duomenų apsaugos priežiūros pareigūnas, 2010 03 18.

[7] Žr. 2 priedą, kuriame aprašomos esamos sienų valdymui ir teisėsaugai skirtos informacinės sistemos.

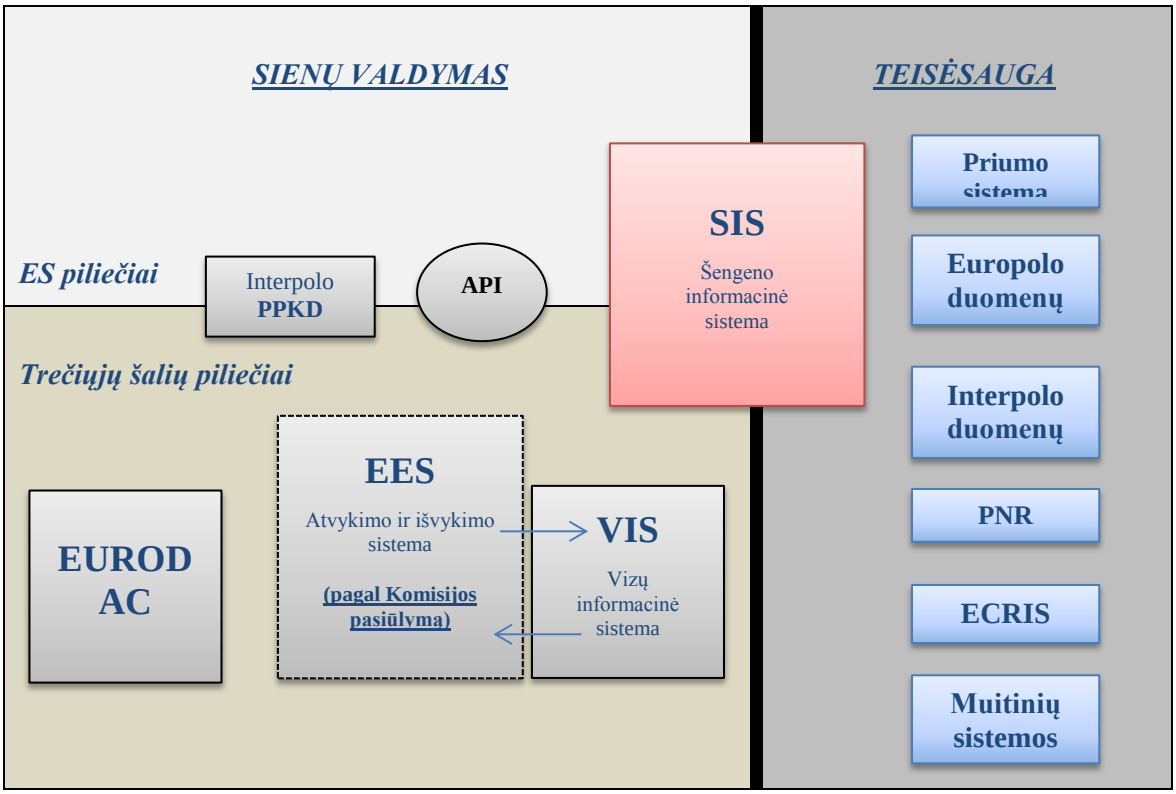
[8] Vadovaujantis 22 protokolo dėl Danijos ir 21 bei 36 protokolų dėl Jungtinės Karalystės ir Airijos konkrečiomis sąlygomis.

[9] Teisėsaugos institucijų prieiga prie VIS ir EURODAC gali būti suteikiama ribotai – tik įvykdžius tam tikras sąlygas, nes teisėsauga yra papildomas šių sistemų tikslas. Valstybės narės, norėdamos gauti prieigą prie VIS, turi paskirti instituciją, atsakingą už teisėsaugos institucijų prieigos kontrolę, o policija privalo pateikti įrodymų, kad prieiga yra būtina nusikalstamų veikų tyrimų tikslais. Dėl EURODAC – tyrimą atliekanti institucija, prieš jai suteikiant prieigą prie EURODAC, turi atlikti paiešką nacionalinėje AFIS, Priumo sistemoje ir VIS.

[10] Netrukus ją pakeis TESTA-NG.

[11] COM(2016) 194 final.

1 paveikslas. *Pagrindinių informacinių sistemų, skirtų sienų valdymui ir teisėsaugai, scheminė apžvalga*



Esamos papildomos sienų valdymo priemonės – tai Interpolo pavogtų ir pamestų kelionės dokumentų (PPKD) duomenų bazė ir išankstinė informacija apie keleivius (API), kuriomis renkama informacija apie keleivius, ketinančius skristi į ES. Šios priemonės yra susijusios tiek su ES piliečiais, tiek su trečiųjų šalių piliečiais.

Teisėsaugos, nusikalstamų veikų tyrimų ir teisminio bendradarbiavimo tikslais ES sukūrė specialias **decentralizuotas keitimosi informacija priemones** – tai i) Priumo sistema, skirta keistis DNR, pirštų atspaudų ir transporto priemonių registracijos duomenimis, ir ii) Europos nuosprendžių registrų informacinė sistema (ECRIS), skirta keistis nacionalinių nuosprendžių registrų informacija. ECRIS sudaro galimybę per saugų tinklą keistis informacija apie Europos Sąjungos baudžiamųjų bylų teismų paskelbtus ankstesnius apkaltinamuosius nuosprendžius dėl konkretaus asmens. Užklausos daugiausia grindžiamos raidiniais skaitmeninis asmens tapatybės duomenimis, nors galima keistis ir biometriniais duomenimis.

Europolas kaip ES kriminalinės informacijos centras remia informacijos mainus tarp nacionalinių policijos institucijų. Europolo informacinė sistema (EIS) yra centralizuota kriminalinės informacijos duomenų bazė, kurioje valstybės narės kaupia duomenis apie sunkius nusikaltimus ir terorizmą ir vykdo tokių duomenų paiešką. Europolo ryšių punktai teikia analizei skirtas darbo bylas, į kurias įtraukta informacija apie valstybėse narėse tebevykdomas operacijas. Europolo saugaus keitimosi informacija tinklo programa (SIENA) suteikia galimybę valstybėms narėms greitai, saugiai ir patogiu būdu keistis informacija tarpusavyje, su Europolu arba su trečiosiomis šalimis, sudariusiomis bendradarbiavimo susitarimą su Europolu. Be to, programoje SIENA didelės svarbos teikiama sąveikumui su kitomis Europolo sistemomis siekiant, pvz., tiesiogiai keistis duomenimis su ryšių punktais. Ji suteikia galimybę į Europolo duomenų bazes įtraukti informaciją, kuria valstybės narės keičiasi tarpusavyje. Todėl valstybės narės turėtų

rinktis programą SIENA kaip pirminį dalijimosi teisėsaugos informacija visoje ES kanalą.

Keleivio duomenų įrašų (PNR)[12] sistema – tai papildomų asmens duomenų tvarkymo sistemų, kurios bus sukurtos įvairiose valstybėse narėse, grupė. PNR duomenys – tai bilietų rezervavimo metu ir registruojantis skrydžiui pateikta informacija.

Galiausiai, vykdant tarpžinybinį bendradarbiavimą prie išorės sienų svarbus vaidmuo taip pat tenka **muitinėms**. Jos turi įvairių sistemų[13] ir duomenų bazių, kuriose yra duomenų apie prekių judėjimą, ekonominės veiklos vykdytojų identifikavimą ir su rizika susijusios informacijos, kuri galėtų būti panaudota siekiant padidinti vidaus saugumą. Šios sistemos taip pat turi savo kontroliuojamą ir saugią ribotos prieigos infrastruktūrą (bendrąjį ryšių tinklą), kurios efektyvumas jau pasitvirtino. Turėtų būti toliau siekiama didesnės informacinių sistemų ir atitinkamos jų infrastruktūros, skirtos ES sienų valdymui ir muitinių operacijoms, sąveikos ir konvergencijos.

5. ESAMŲ INFORMACINIŲ SISTEMŲ GERINIMAS

Esamos ES sienų valdymo ir vidaus saugumo informacinės sistemos atlieka labai įvairias funkcijas. Vis dėlto sistemos tebeturi **trūkumų**, kuriuos reikia šalinti siekiant optimizuoti jų veikimą.

Šengeno informacinė sistema (SIS)

Šiuo metu patikrinimai kertant sieną naudojant **Šengeno informacinę sistemą** (SIS) vykdomi pagal raidinę skaitmeninę paiešką (t. y. vardas, pavardė ir gimimo data). Pirštų atspaudai gali būti naudojami tik siekiant patikrinti ir patvirtinti asmenų, kurie jau buvo identifikuoti pagal jų vardą ir pavardę, tapatybę. Ši saugumo spraga suteikia asmenims, dėl kurių paskelbtas perspėjimas, galimybę naudoti suklastotus dokumentus, kad SIS sistemoje nebūtų galima rasti su jais susijusios tikslios atitikties.

Šis esminis trūkumas bus pašalintas į SIS įtraukiant pirštų atspaudų paieškos funkciją įdiegus **automatinę pirštų atspaudų identifikavimo sistemą (AFIS)**, kaip numatyta pagal esamą teisinę sistemą[14]. AFIS turėtų pradėti veikti nuo 2017 m. vidurio[15]. Sukurta AFIS galės naudotis Europolas – taip ji papildys Europolo nusikalstamų veikų tyrimų ir kovos su terorizmu sistemas ir padės keistis pirštų antspaudų duomenimis pagal Priumo sistemą. Komisija ir „eu-LISA“ išnagrinės tokias platesnio būsimos AFIS panaudojimo galimybes.

---

[12] Žr. 6.2 skirsnį.

[13] Muitinių informacinės sistemos – tai visos sistemos, sukurtos pagal Bendrijos muitinės kodeksą (Reglamentas (EEB) Nr. 2913/92), būsimą Sąjungos muitinės kodeksą (Reglamentas (ES) Nr. 952/2013) ir Sprendimą dėl nepopierinės muitinės ir verslo aplinkos (Sprendimas 70/2008/EB), ir Muitinės informacinė sistema, sukurta pagal 1995 m. Konvenciją dėl informacijos technologijų naudojimo muitinės tikslais. Jų tikslas – palengvinti Europos muitinių bendradarbiavimą ir taip padėti kovoti su nusikalstama veika, susijusia su muitinės veikla.

[14] 2006 m. gruodžio 20 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1987/2006 dėl antrosios kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo 22 straipsnio c punktas ir 2007 m. birželio 12 d. Tarybos sprendimo 533/2007/TVR dėl antrosios kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo 22 straipsnio c punktas (OL L 381, 2006 12 28, p. 4 ir OL L 2015, 2007 8 7, p. 63).

[15] 2016 m. kovo mėn. Komisija pateikė ataskaitą Europos Parlamentui ir Tarybai apie technologinį prieinamumą ir parengtį siekiant nustatyti asmenų tapatybę pagal pirštų atspaudus, saugomus antrosios kartos Šengeno informacinėje sistemoje (SIS II).

Komisija, remdamasi tebeatliekamu vertinimu ir techniniu tyrimu, šiuo metu nagrinėja **galimas papildomas SIS funkcijas** siekdama pateikti pasiūlymus, kaip pakeisti SIS teisinį pagrindą. Svarstomi aspektai:

- sukurti SIS perspėjimus apie neteisėtus migrantus, dėl kurių priimtas sprendimas juos grąžinti;
- biometrinio identifikavimo tikslu be pirštų atspaudų naudoti ir veido atvaizdus;
- automatiškai perduoti informaciją apie nustatytus atitikties atvejus atlikus patikrinimą;
- SIS centrinėje sistemoje saugoti informaciją apie paieškos rezultatus apie nustatytus perspėjimo dėl slapto ar specialiojo patikrinimo atvejus;
- sukurti naują perspėjimų kategoriją „Ieškomi nežinomi asmenys“, su kuria susiję teismo ekspertizės duomenys gali būti nacionalinėse duomenų bazėse (pvz., nusikaltimo vietoje palikti latentiniai atspaudai)[16].

Komisija ES lėšomis toliau rems įgyvendinamus projektus, kurie sudaro galimybę tuo pačiu metu vykdyti paieškas SIS ir Interpolo pavogtų ir pamestų kelionės dokumentų (PPKD) bei ieškomų nusikaltėlių, transporto priemonių arba šaunamųjų ginklų (iARMS) duomenų bazėse, papildančiose ES informacines sistemas[17].

Interpolo pavogtų ir pamestų kelionės dokumentų (PPKD) duomenų bazė

Siekiant užtikrinti veiksmingą sienų valdymą, itin svarbu visų trečiųjų šalių piliečių ir ES piliečių kelionės dokumentus patikrinti **PPKD duomenų bazėje**. Teisėsaugos institucijos taip pat turėtų naudoti **PPKD duomenų bazę** vykdydamos užklausas Šengeno erdvėje. Po 2015 m. lapkričio 13 d. Paryžiuje įvykdytų teroristinių išpuolių Taryba paragino iki 2016 m. kovo mėn. visuose išorės sienos perėjimo punktuose įdiegti elektroninę prieigą prie atitinkamų Interpolo duomenų bazių ir automatizuotą kelionės dokumentų tikrinimą[18]. Visos valstybės narės turėtų įdiegti atitinkamą elektroninę prieigą ir sistemas, kurios leistų PPKD duomenų bazėje automatiškai atnaujinti duomenis apie pavogtus arba pamestus kelionės dokumentus.

Išankstinė informacija apie keleivius (API)

Atsižvelgdamos į taikomą geriausią praktiką, valstybės narės taip pat turėtų įdiegti automatinę kryžminę šių duomenų patikrą SIS ir Interpolo PPKD duomenų bazėje ir taip padidinti papildomą **išankstinės informacijos apie keleivius** (API) naudą. Komisija įvertins būtinybę persvarstyti API duomenų tvarkymo teisinį pagrindą siekiant užtikrinti platesnį taikymą ir nustatyti valstybių narių įpareigojimą reikalauti API duomenų apie visus atvykstamuosius ir išvykstamuosius skrydžius ir tokius duomenis naudoti. Tai ypač svarbu atsižvelgiant į būsimos Keleivio duomenų įrašo direktyvos įgyvendinimą, nes kartu naudojant PNR ir API duomenis PNR duomenys leidžia veiksmingiau kovoti su terorizmu ir sunkiais nusikaltimais[19].

---

[16] Galimybė nustatyti šį naują perspėjimą bus vertinama siekiant užtikrinti papildomumą ir išvengti dubliavimosi su esama Priumo sistema, skirta ieškoti pirštų atspaudų įvairiose ES valstybių narių nacionalinėse duomenų bazėse.

[17] Interpolo sukurtos informacijos paieškos priemonės, kaip antai Fiksuotojo ryšio tinklo Interpolo duomenų bazė (FIND) ir Judriojo ryšio tinklo Interpolo duomenų bazė (MIND), leidžia paprasčiau tuo pačiu metu vykdyti paieškas Interpolo sistemose ir SIS.

[18] 2015 m. lapkričio 20 d. ES Tarybos ir Taryboje posėdžiavusių valstybių narių išvados dėl kovos su terorizmu.

[19] Žr. 6.2 skirsnį dėl siūlomos Keleivio duomenų įrašo direktyvos.

Vizų informacinė sistema (VIS)

Šiuo metu Komisija taip pat atlieka bendrą **Vizų informacinės sistemos** (VIS) įvertinimą, kuris turėtų būti užbaigtas 2016 m. Be kitų dalykų vertinime nagrinėjama, kaip VIS naudojama atliekant patikrinimus prie išorės sienų ir valstybių narių teritorijoje ir kaip ji padeda kovoti su tapatybės ir vizų klastojimu. Tuo remdamasi Komisija išnagrinės galimybes tobulinti VIS funkcijas imantis šių veiksmų:

- gerinti veido atvaizdų kokybę, kad būtų galima patikrinti biometrinių duomenų atitiktį;
- naudoti vizų prašytojų biometrinius duomenis siekiant vykdyti paieškas būsimoje automatinėje pirštų atspaudų identifikavimo sistemoje (AFIS), kuri bus sukurta kaip SIS dalis;
- sumažinti 6–12 metų vaikų pirštų atspaudų ėmimo tikslais nustatytą amžiaus ribą, numatant patikimas pagrindinių teisių apsaugos priemones ir kitas apsaugos priemones[20];
- sudaryti sąlygas nagrinėjant prašymus išduoti vizą paprasčiau atlikti paiešką Interpolo PPKD duomenų bazėje.

Dėl galimybės pagal galiojančią teisinę sistemą **teisėsaugos tikslais** gauti prieigą prie VIS duomenų – valstybės narės tokią galimybę suteikia nenuosekliai. Šiuo atveju valstybės narės pranešė, kad prieigos prie VIS procedūrų metu teisėsaugos institucijos susidūrė su praktinėmis problemomis. Be to, teisėsaugos tikslais prieiga prie EURODAC sistemos suteikiama vis dar labai ribotai. Komisija apsvarstys, ar reikia persvarstyti teisėsaugos institucijų prieigos prie VIS ir EURODAC teisinę sistemą.

Sistema EURODAC

Kaip nurodyta komunikate „Bendros Europos prieglobsčio sistemos reformavimas ir teisėtų kelių į Europą tiesimas“[21], Komisija pateiks pasiūlymą dėl sistemos **EURODAC** reformos siekiant labiau patobulinti jos funkcijas, susijusias su neteisėta migracija ir grąžinimu. Tai padės pašalinti dabartinę spragą, susijusią su galimybe atsekti neteisėtų migrantų antrinį judėjimą tarp valstybių narių. Be to, pasiūlymu bus siekiama sustiprinti grąžinimo ir readmisijos procedūras – bus numatytos neteisėtų migrantų tapatybės nustatymo ir naujų dokumentų išdavimo priemonės grąžinimo tikslais. Taigi pasiūlymas taip pat aprėps keitimąsi EURODAC saugoma informacija su trečiosiomis šalimis, atsižvelgiant į būtinas duomenų apsaugos priemones.

Europolas

ES suteikė **Europolui** prieigą prie pagrindinių centrinių duomenų bazių, tačiau agentūra dar visapusiškai nepasinaudojo šia galimybe. Europolas turi teisę susipažinti su į SIS įvestais duomenimis areštų, slaptų ar specialiųjų patikrinimų ir konfiskuotinų daiktų paieškos tikslais, ir tiesiogiai jų ieškoti. Ligi šiol Europolas SIS sistemoje atliko palyginti mažai paieškų. Nuo 2013 m. rugsėjo mėn. Europolui teisiškai įmanoma gauti prieigą prie VIS susipažinimo tikslais. Nuo 2015 m. liepos mėn. pagal sistemos EURODAC teisinį pagrindą Europolui suteikiama prieiga prie šios sistemos. Agentūra turėtų paspartinti tebevykdomus prisijungimo prie VIS ir EURODAC darbus. Apskritai Komisija įvertins, ar kitoms ES vidaus reikalų srities agentūroms (visų pirma, būsimoms Europos sienų ir pakrančių apsaugos pajėgoms) būtina suteikti didesnę prieigą prie informacinių sistemų.

Priumo sistema

[20] JRC tyrime *Fingerprint Recognition for children* (EUR 26193 EN; ISBN 978-92-79-33390-3Children', 2013 m.) nurodyta, kad tai yra techniškai įmanoma.

[21] COM(2016) 197 final.

Šiuo metu nėra išnaudojamos visos **Priumo sistemos** galimybės. Taip yra dėl to, kad ne visos valstybės narės įvykdė savo teisinius įsipareigojimus integruoti tinklą į savo sistemas. Valstybės narės gavo didelę finansinę ir techninę paramą Priumo sistemos įdiegimui, tad dabar turėtų visiškai ją įdiegti. Komisija naudojasi jai suteiktais įgaliojimais, siekdama užtikrinti, kad valstybės narės visiškai įgyvendintų savo teisinius įsipareigojimus – 2016 m. sausio mėn. ji pradėjo struktūrinį dialogą (sistema „EU Pilot“) su atitinkamomis valstybėmis narėmis. Jeigu valstybių narių pateikti atsakymai Komisijos netenkins, ji nedvejodama pradės pažeidimo nagrinėjimo procedūrą.

Europos nuosprendžių registrų informacinė sistema (ECRIS)

Europos nuosprendžių registrų informacinė sistema **ECRIS** leidžia keistis informacija apie apkaltinamuosius nuosprendžius dėl trečiųjų šalių piliečių ir asmenų be pilietybės, tačiau nėra procedūros, pagal kurią tai būtų galima daryti veiksmingai. 2016 m. sausio mėn. Komisija priėmė teisės akto pasiūlymą siekdama pašalinti šią spragą[22]. Todėl Komisija pasiūlė nacionalinėms institucijoms suteikti galimybę ieškoti trečiųjų šalių piliečių pagal pirštų atspaudus, kad jos galėtų saugiau nustatyti jų tapatybę. 2016 m. Europos Parlamentas ir Taryba turėtų priimti šio teisės akto tekstą.

Horizontalieji klausimai

Bendra su informacinėmis sistemomis susijusi problema – tai jų **įdiegimo lygis** valstybėse narėse. Ryškiausi pavyzdžiai – Priumo sistema įdiegta nevienodai, nesukurta elektroninė prieiga prie PPKD duomenų bazės. Komisija, siekdama padidinti informacinių sistemų įdiegimo lygį, atidžiai stebės kiekvienos valstybės narės veiklos rezultatus[23]. Atliekant stebėseną bus ne tik nagrinėjama, ar valstybės narės vykdo su informacinėmis sistemomis susijusius teisinius įsipareigojimus, bet ir kaip jos naudojasi esamomis priemonėmis ir ar jos laikosi gerosios praktikos. Vykdydama įdiegimo lygio stebėseną ir skatindama šį lygį didinti, Komisija remsis įvairiais šaltiniais, įskaitant valstybių narių pranešimus ir vizitus, surengtus pagal Šengeno vertinimo ir stebėjimo mechanizmą.

Kita bendra su informacinėmis sistemomis susijusi problema – tai **įvestų duomenų kokybė**. Jeigu valstybės narės nesilaiko minimalių kokybės reikalavimų, saugomų duomenų patikimumas ir vertė smarkiai sumažėja, o klaidingos atitikties atvejų arba atvejų, kai paieška neduoda rezultatų, rizika verčia abejoti pačių sistemų vertingumu. Siekiant pagerinti įvestų duomenų kokybę, „eu-LISA“ sukurs **centrinius** visų jos kompetencijai priskiriamų sistemų **duomenų kokybės stebėjimo pajėgumus**.

Daugelyje sienų kontrolės ir saugumo srities informacinių sistemų tvarkomi tapatybės duomenys, gauti iš kelionės ir asmens tapatybės dokumentų. Siekiant stiprinti sienas ir saugumą gerai veikiančių sistemų neužtenka – turi būti įmanoma lengvai ir saugiai patikrinti kelionės ir tapatybės dokumentų autentiškumą. Šiuo tikslu Komisija pasiūlys priemones, skirtas pagerinti elektroninių **dokumentų saugumą** bei tapatybės duomenų valdymą ir sustiprinti kovą su dokumentų klastojimu. Galimi būdai šiam tikslui pasiekti – tai saugios atpažinties sąveikumo lygiai, kuriuos galima įdiegti pagal eIDAS reglamentą[24].

---

[22] COM(2016) 7 final, 2016 1 19.

[23] Vadovaujantis 22 protokolo dėl Danijos ir 21 bei 36 protokolų dėl Jungtinės Karalystės ir Airijos konkrečiomis sąlygomis.

[24] 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

Veiksmai, skirti esamoms informacinėms sistemoms gerinti

Šengeno informacinė sistema (SIS)

- Komisija ir „eu-LISA“ iki 2017 m. vidurio turi sukurti ir įdiegti automatinę pirštų atspaudų identifikavimo sistemą (AFIS) kaip SIS funkciją.
- Komisija iki 2016 m. pabaigos turi pateikti pasiūlymus, skirtus persvarstyti SIS teisinį pagrindą, kad būtų labiau patobulintos jos funkcijos.
- Valstybės narės turi į SIS įvesti visą susijusią informaciją ir šioje sistemoje ją tikrinti visais būtinais atvejais siekiant maksimaliai išnaudoti SIS galimybes.

Interpolo pavogtų ir pamestų kelionės dokumentų (PPKD) duomenų bazė

- Valstybės narės visuose išorės sienos perėjimo punktuose turi įdiegti elektroninę prieigą prie Interpolo priemonių.
- Valstybės narės turi vykdyti įsipareigojimą tuo pačiu metu į SIS ir PPKD duomenų bazę įvesti duomenis apie pavogtus arba pamestus kelionės dokumentus ir jose tikrinti šiuos duomenis.

Išankstinė informacija apie keleivius (API)

- Valstybės narės, vadovaudamosi geriausia praktika, turi automatizuoti API duomenų naudojimą, kai jie tikrinami SIS ir Interpolo pavogtų ir pamestų kelionės dokumentų (PPKD) duomenų bazėje.
- Komisija turi įvertinti poreikį persvarstyti API duomenų tvarkymo teisinį pagrindą.

Vizų informacinė sistema (VIS)

- Komisija turi iki 2016 m. pabaigos išnagrinėti, kaip galima labiau patobulinti VIS.

EURODAC

- Komisija turi pateikti pasiūlymą persvarstyti sistemos EURODAC teisinį pagrindą, kad būtų labiau patobulintos jos funkcijos, susijusios su neteisėta migracija ir grąžinimu.

Europolas

- Europolas turi visokeriopai pasinaudoti turimomis prieigos prie SIS, VIS ir EURODAC teisėmis, kad galėtų jose tikrinti duomenis.
- Komisija ir Europolas turėtų siekti Europolo informacinės sistemos (EIS) ir kitų sistemų, visų pirma SIS, sąveikos ir ją skatinti.
- Komisija ir „eu-LISA“ turi išnagrinėti, ar automatinė pirštų atspaudų identifikavimo sistema (AFIS), kuri turi būti sukurta kaip SIS dalis, gali papildyti Europolo sistemas nusikalstamų veikų tyrimų ir kovos su terorizmu tikslais.

Priumo sistema

- Valstybės narės turi visapusiškai įgyvendinti ir naudoti Priumo sistemą.
- Prireikus Komisija turi pradėti pažeidimo nagrinėjimo procedūrą prieš tas valstybes nares, kurios nėra prisijungusios prie Priumo sistemos.
- Komisija ir „eu-LISA“ turi išnagrinėti, ar automatinė pirštų atspaudų identifikavimo sistema (AFIS), kuri turi būti sukurta kaip SIS dalis, gali papildyti pagal Priumo sistemą vykdomus pirštų atspaudų duomenų mainus.

Europos nuosprendžių registrų informacinė sistema (ECRIS)

- Europos Parlamentas ir Taryba 2016 m. turėtų priimti teisės akto pasiūlymą, kuriuo nacionalinėms valdžios institucijoms būtų suteikta galimybė sistemoje ECRIS ieškoti trečiųjų šalių piliečių pagal pirštų atspaudus.

Horizontalieji klausimai

- Komisija turi **stebėti ir skatinti** informacinių sistemų **įdiegimo lygį.**
- „eu-LISA“ turi sukurti **centrinius** visų jos kompetencijai priskiriamų sistemų **duomenų kokybės stebėjimo pajėgumus**.
- Komisija turi pasiūlyti priemones, skirtas pagerinti elektroninių **dokumentų saugumą bei tapatybės valdymą** ir sustiprinti kovą su dokumentų klastojimu.
- Komisija turi nagrinėti informacinių sistemų ir atitinkamos jų infrastruktūros, skirtos ES sienų valdymui ir **muitinių operacijoms**, didesnės sąveikos ir konvergencijos galimybes.

6. PAPILDOMŲ INFORMACINIŲ SISTEMŲ KŪRIMAS IR SPRAGŲ ŠALINIMAS

Esamos informacinės sistemos apima labai įvairius duomenis, kurie yra reikalingi sienų valdymo ir teisėsaugos sritims, tačiau jos taip pat turi ir didelių spragų. Kai kurias iš šių spragų Komisija pašalino pateikusi teisės aktų pasiūlymus, visų pirma pasiūlymus dėl atvykimo ir išvykimo sistemos ir dėl ES keleivio duomenų įrašo (PNR) sistemos. Kitas nustatytas spragas reikia kruopščiai įvertinti siekiant išsiaiškinti, ar reikalingos papildomos ES priemonės.

1. Atvykimo ir išvykimo sistema

Kartu su šiuo komunikatu Komisija pateikė persvarstytą teisės akto pasiūlymą dėl atvykimo ir išvykimo sistemos (EES) sukūrimo. Teisėkūros institucijoms jį priėmus „eu-LISA“, bendradarbiaudama su Šengeno valstybėmis narėmis, turės šią sistemą sukurti ir įdiegti.

EES registruos visų trečiųjų šalių piliečių, vykstančių į Šengeno erdvę trumpam laikotarpiui (ne daugiau kaip 90 dienų per bet kurį 180 dienų laikotarpį), kuriems nustatytas vizos reikalavimas ir kuriems toks reikalavimas netaikomas arba kurie atvyksta su nauja kelionių viza (iki vienerių metų), sienos kirtimus (atvykimą ir išvykimą). EES tikslai: a) gerinti išorės sienų valdymą, b) sumažinti neteisėtą migraciją, sprendžiant užsibuvusių asmenų klausimą ir c) padėti kovoti su terorizmu ir sunkiais nusikaltimais ir taip padėti užtikrinti aukštą vidaus saugumo lygį.

EES registruos trečiųjų šalių piliečių tapatybę (raidinius skaitmeninius duomenis, keturių pirštų atspaudus ir veido atvaizdus) ir jų kelionės dokumentų duomenis ir juos susies su elektroniniais atvykimo ir išvykimo įrašais. Dabartinė kelionės dokumentų antspaudavimo praktika bus taikoma toliau. EES leis veiksmingai valdyti teisėtą trumpalaikį buvimą, labiau automatizuoti sienų kontrolę ir geriau nustatyti dokumentų ir tapatybės klastojimo atvejus. Centrinė registracija leis nustatyti Šengeno erdvėje užsibuvusius asmenis ir dokumentų neturinčius asmenis. Todėl siūloma EES sistema pašalina svarbią esamų informacinių sistemų spragą.

2. Keleivio duomenų įrašai

Keleivio duomenų įrašo (PNR) duomenys yra bilietų rezervavimo duomenys, kontaktiniai duomenys, išsami informacija apie kelionės maršrutą ir rezervaciją, specialios pastabos, informacija apie sėdėjimo vietą, bagažą ir mokėjimo būdą. PNR duomenys yra naudingi ir reikalingi, kad būtų galima nustatyti didelę riziką keliančius

keliautojus kovojant su terorizmu, neteisėta prekyba narkotikais, prekyba žmonėmis, seksualiniu vaikų išnaudojimu ir kitais sunkiais nusikaltimais. Siūloma PNR direktyva bus užtikrintas geresnis nacionalinių sistemų bendradarbiavimas ir sumažės saugumo spragų valstybių narių tarpusavio veikloje. Todėl siūloma PNR direktyva panaikinama didelė spraga, susijusi su prieiga prie duomenų, kurie yra būtini siekiant kovoti su sunkiais nusikaltimais ir terorizmu. **PNR direktyva turėtų būti priimta kuo skubiau.**

Būsimoje direktyvoje bus nustatyta, kad valstybės narės turi įsteigti informacijos apie keleivius skyrius, kurie gaus PNR duomenis iš vežėjų. Šiuo tikslu nereikės kurti centrinės sistemos ar duomenų bazės, tačiau reikės šiek tiek suvienodinti nacionalinius techninius sprendimus ir procedūras. Tai sudarys palankesnes sąlygas informacijos apie keleivius skyriams keistis PNR duomenimis, kaip numatyta siūlomoje direktyvoje. Šiuo tikslu Komisija padės valstybėms narėms analizuoti įvairius informacijos apie keleivius skyrių tarpusavio sujungiamumo scenarijus, siekdama pasiūlyti standartizuotų sprendimų ir procedūrų. Priėmus direktyvą, Komisija paspartins bendrų protokolų ir tinkamų duomenų formatų, skirtų oro vežėjų PNR duomenims perduoti informacijos apie keleivius skyriams, rengimą. Per tris mėnesius nuo šios direktyvos priėmimo Komisija parengs įgyvendinimo akto projektą.

3. Informacijos trūkumas prieš trečiųjų šalių piliečių, kuriems netaikomas vizos reikalavimas, atvykimą

Vizų turėtojų tapatybė, ryšiai ir pagrindinė informacija yra įregistruoti VIS, tačiau informacija apie asmenis, kuriems netaikomas vizos reikalavimas, gaunama vien tik iš jų kelionės dokumento. Oro arba jūrų transportu atvykstantiems keliautojams iki jų atvykimo ją galima papildyti API duomenimis. Pagal siūlomą PNR direktyvą jų PNR duomenys taip pat bus renkami, jei asmenys atvyks į ES oro transportu. Apie asmenis, atvykstančius į ES per sausumos sienas, neturima informacijos iki jų atvykimo prie ES išorės sienos.

Teisėsaugos institucijos gali gauti informacijos apie vizų turėtojų tapatybę iš VIS, jei būtina siekiant kovoti su sunkiais nusikaltimais ir terorizmu, tačiau nėra palyginamų duomenų apie asmenis, kuriems netaikomas vizos reikalavimas. Šis informacijos trūkumas ypač turi poveikio ES sausumos sienų valdymui, tuo atveju, kai daug keliautojų, kuriems netaikomas vizos reikalavimas, atvyksta automobiliu, autobusu ar traukiniu. Kelioms ES kaimyninėms šalims jau netaikomas vizos reikalavimas, su kitomis kaimyninėmis šalimis ES vykdo dialogą dėl vizų režimo liberalizavimo. Dėl to artimiausioje ateityje gali labai padaugėti keliautojų, kuriems netaikomas vizos reikalavimas.

Komisija įvertins, ar nauja ES priemonė šiam klausimui spręsti yra būtina, įgyvendinama ir proporcinga. Galimybė, kurią būtų galima svarstyti, yra **ES kelionių informacijos ir leidimų sistema** (ETIAS), kurioje keliautojai, kuriems netaikomas vizos reikalavimas, registruotų atitinkamą informaciją, susijusią su savo numatyta kelione. Automatinis šios informacijos apdorojimas galėtų padėti sienos apsaugos pareigūnams vertinti trečiųjų šalių lankytojus, atvykstančius trumpalaikiam buvimui. JAV, Kanada ir Australija jau įdiegė panašias sistemas, kurios taikomos ir ES piliečiams.

Kelionės leidimo sistemos grindžiamos elektroninėmis paraiškomis, kuriose pareiškėjas prieš išvykimą pateikia išsamią informaciją apie savo tapatybę, kontaktinius duomenis, kelionės tikslą, maršrutą ir kt. Kai leidimas gaunamas, pasienio procedūros atvykus tampa greitesnės ir sklandesnės. Todėl be saugumo ir sienų valdymo privalumų, ir galimos svarbos įgyvendinant vizų režimo abipusiškumą, tokia sistema kaip ETIAS taip pat būtų kelionių supaprastinimo priemonė.

4. Europos policijos registrų informacinė sistema (EPRIS)

Kaip nurodyta Europos saugumo darbotvarkėje, ateityje keitimosi informacija srityje bus siekiama, kad turimi policijos duomenys būtų prieinami realiuoju laiku įvairiose valstybėse narėse. Siekdama palengvinti tarpvalstybinę prieigą prie informacijos, saugomos nacionalinėse teisėsaugos duomenų bazėse, Komisija įvertins Europos policijos registrų rodyklės sistemos (EPRIS) būtinybę, technines galimybes ir proporcingumą. Šioje srityje Komisija teikia ES finansavimą penkių valstybių narių grupės įgyvendinamam bandomajam projektui, kuriuo siekiama sukurti automatinės tarpvalstybinės paieškos nacionalinėse rodyklėse mechanizmus, remiantis principu „atitiktis nustatyta / atitikties nenustatyta“[25]. Atlikdama šį vertinimą, Komisija atsižvelgs į projekto rezultatus.

<u>Veiksmai, kuriais siekiama plėtoti papildomas informacines sistemas ir surinkti trūkstamą informaciją</u>

Atvykimo ir išvykimo sistema (EES)

- Europos Parlamentas ir Taryba teisės aktų dėl EES pasiūlymus turėtų laikyti vienu iš didžiausių prioritetų ir siekti juos priimti iki 2016 m. pabaigos.

Keleivio duomenų įrašai (PNR)

- Europos Parlamentas ir Taryba turėtų priimti PNR direktyvą iki 2016 m. balandžio mėn.
- Priėmus PNR direktyvą valstybės narės turi ją įgyvendinti skubos tvarka.
- Komisija turi remti duomenų mainus tarp informacijos apie keleivius skyrių, pasiūlydama standartizuotų sprendimų ir procedūrų.
- Komisija turi parengti Įgyvendinimo sprendimo dėl bendrų protokolų ir tinkamų duomenų formatų, skirtų oro vežėjų PNR duomenų perdavimui informacijos apie keleivius skyriams, projektą per tris mėnesius po PNR direktyvos priėmimo.

Informacijos trūkumas prieš trečiųjų šalių piliečių, kuriems netaikomas vizos reikalavimas, atvykimą

- 2016 m. Komisija turi įvertinti naujos ES priemonės, tokios kaip ES kelionių informacijos ir leidimų sistema, sukūrimo būtinybę, technines galimybes ir proporcingumą.

Europos policijos registrų informacinė sistema (EPRIS)

- Komisija 2016 m. įvertins EPRIS sukūrimo būtinybę, technines galimybes ir proporcingumą.

[25] Automatinio keitimosi duomenimis proceso (ADEP) bandomojo projekto tikslas – sukurti techninę sistemą, kuri sudarytų sąlygas, naudojantis rodykle, išsiaiškinti, ar vienoje ar keliose valstybėse narėse egzistuoja policijos įrašai apie asmenį arba nusikalstamos veikos policijos tyrimą. Automatiniame atsakyme į paiešką rodyklėje būtų nurodyta tik ar duomenų turima („atitiktis nustatyta“) ar ne („atitikties nenustatyta“). Nustačius atitiktį papildomų asmens duomenų turėtų būti prašoma antruoju etapu, naudojantis įprastais policijos bendradarbiavimo kanalais.

7. SIEKIANT INFORMACINIŲ SISTEMŲ SĄVEIKUMO

Sąveikumas – informacinių sistemų gebėjimas keistis duomenimis ir sudaryti sąlygas keistis informacija. Galima išskirti **keturis sąveikumo aspektus**, dėl kiekvieno iš kurių kyla teisinių[26], techninių ir veikimo problemų, įskaitant dėl duomenų apsaugos:

- bendra paieškos sąsaja, sudaranti sąlygas atlikti paiešką keliose informacinėse sistemose tuo pačiu metu ir pateikti bendrus rezultatus viename ekrane;
- informacinių sistemų tarpusavio sujungiamumas, kuomet vienoje sistemoje užregistruotus duomenis galima automatiškai tikrinti kitoje sistemoje;
- bendros biometrinių duomenų atitikties nustatymo paslaugos sukūrimas, sujungiant įvairias informacines sistemas;
- bendra duomenų saugykla skirtingoms informacinėms sistemoms (pagrindinis modulis).

Siekdama inicijuoti procesą, kuriuo siekiama informacinių sistemų sąveikumo ES lygmeniu, Komisija sudarys aukšto lygmens **informacinių sistemų ir sąveikumo ekspertų grupę** su ES agentūromis, nacionaliniais ekspertais ir kitais instituciniais suinteresuotaisiais subjektais. Ekspertų grupei bus pavesta išspręsti skirtingų galimybių teisinius, techninius ir veikimo aspektus, siekiant užtikrinti informacinių sistemų sąveikumą, įvertinant turimų galimybių būtinybę, technines galimybes bei proporcingumą ir jų poveikį duomenų apsaugai. Ji turėtų pašalinti esamus trūkumus ir žinių spragas, atsirandančius dėl informacinių sistemų sudėtingumo ir susiskaidymo Europos lygmeniu. Ekspertų grupė laikysis plataus ir visapusiško požiūrio į sienų valdymą ir teisėsaugą, taip pat atsižvelgdama į muitinių vaidmenis, atsakomybę ir sistemas šioje srityje. Grupės darbo metodais bus siekiama sujungti visą atitinkamą patirtį, kuri praeityje būdavo pernelyg dažnai kaupiama izoliuotai.

Šio proceso tikslas – nustatyti bendrą strateginę ES sienų kontrolės ir saugumo srities duomenų valdymo struktūros viziją, taip pat pasiūlyti sprendimų siekiant ją įgyvendinti.

Šiame konsultacijų procese **vadovaujamasi šiais tikslais**:

- Informacijos sistemos turėtų viena kitą papildyti. Reikėtų vengti dubliavimosi, o esamas dubliavimasis turėtų būti panaikintas. Spragos turi būti tinkamai pašalintos.
- Reikėtų taikyti modulinį metodą, visapusiškai pasinaudojant technologijų raida ir remiantis privatumo užtikrinimo projektuojant principais.
- Nuo pat pradžių reikėtų užtikrinti visas tiek ES piliečių, tiek trečiųjų šalių piliečių pagrindines teises, vadovaujantis Pagrindinių teisių chartija.
- Jei būtina ir įmanoma, informacinės sistemos turėtų būti tarpusavyje susietos ir sąveikios. Turėtų būti sudarytos geresnės galimybės tuo pačiu metu ieškoti keliose sistemose ir taip užtikrinta, kad sienos apsaugos ar policijos pareigūnai galėtų gauti visą reikiamą informaciją, kai tai būtina jų atitinkamoms pareigoms vykdyti, nekeičiant esamų prieigos teisių.

1. Bendra paieškos sąsaja

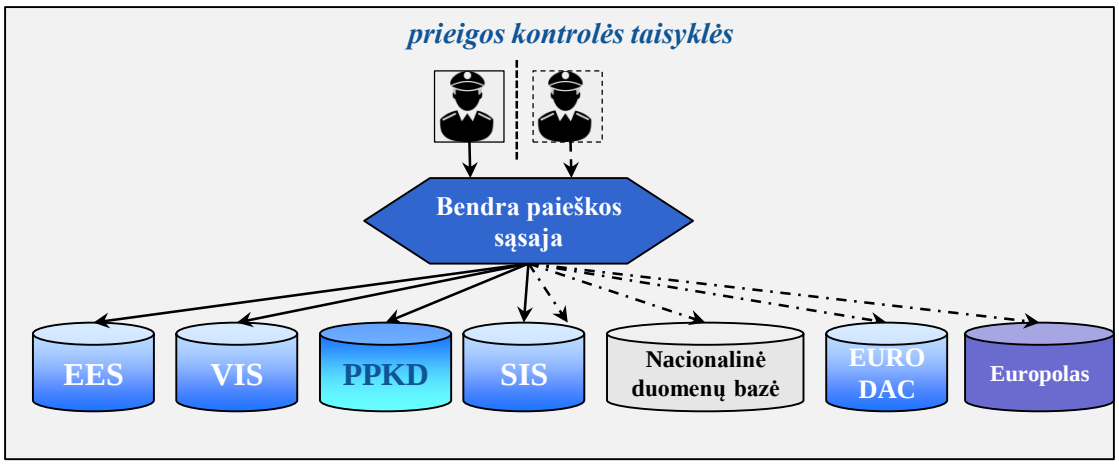
Pirmasis sąveikumo aspektas yra sienos apsaugos ar policijos pareigūnams suteikiama **galimybė atlikti paiešką keliose informacinėse sistemose tuo pačiu metu ir pateikti bendrus rezultatus viename ekrane**, visapusiškai gerbiant jų prieigos teises, laikantis

[26] Atsižvelgiant į 22 protokolo dėl Danijos ir 21 bei 36 protokolų dėl Jungtinės Karalystės ir Airijos konkrečias sąlygas.

atitinkamų tikslų. Tam reikia platformų su bendra paieškos sąsaja, kurios galėtų tikrinti informacines sistemas tuo pačiu metu, pateikus tik vieną užklausą. Pavyzdžiui, nuskaitydama kelionės dokumento lustą arba naudodama biometrinius duomenis, ši platforma galėtų vykdyti paiešką keliose skirtingose duomenų bazėse tuo pačiu metu. Bendros paieškos metodas taikomas visoms institucijoms, kurioms reikia susipažinti su duomenimis ir jais naudotis (pvz., sienos apsaugos pareigūnams, teisėsaugos institucijoms, prieglobsčio tarnyboms), laikantis tikslų apribojimo ir griežtų prieigos kontrolės taisyklių. Ji taip pat gali būti naudojama su mobiliąja įranga. Sukūrus bendrą paieškos sąsają sumažinamas informacinių sistemų Europos lygmeniu sudėtingumas, nes ji suteikia galimybę sienos apsaugos ir policijos pareigūnams atlikti paiešką keliose informacinėse sistemose tuo pačiu metu, taikant vieną procedūrą ir vadovaujantis jų prieigos teisėmis.

Kelios valstybės narės jau įdiegė tokias platformas su bendra paieškos sąsaja. Remdamasi šiuo turimu geriausios patirties pavyzdžiu, Komisija kartu su „eu-LISA“ sieks sukurti standartizuotą bendros paieškos sąsajos sprendimą. Tokiai funkcijai įdiegti valstybės narės turėtų pasinaudoti ES finansavimu pagal savo nacionalinę Vidaus saugumo fondo programą. Komisija atidžiai stebės, kaip valstybės narės naudojasi bendros paieškos sąsajos funkcija nacionaliniu lygmeniu.

***2 paveikslas**. Bendra paieškos sąsaja*



Vykdyti paiešką įvairiose centralizuotose arba nacionalinėse sistemose (kaip pavaizduota) yra lengviau nei vykdyti paiešką decentralizuotose sistemose. Komisija ir „eu-LISA“ ištirs, ar bendrą paieškos sąsają taip pat galima naudoti „vieno langelio“ paieškoms tuo pačiu metu vykdyti decentralizuotose sistemose, pavyzdžiui, Priumo sistemoje ir ECRIS. Komisija ir „eu-LISA“ šią analizę atliks kartu su informacinių sistemų ir sąveikumo ekspertų grupe, nekeičiant esamų prieigos teisių.

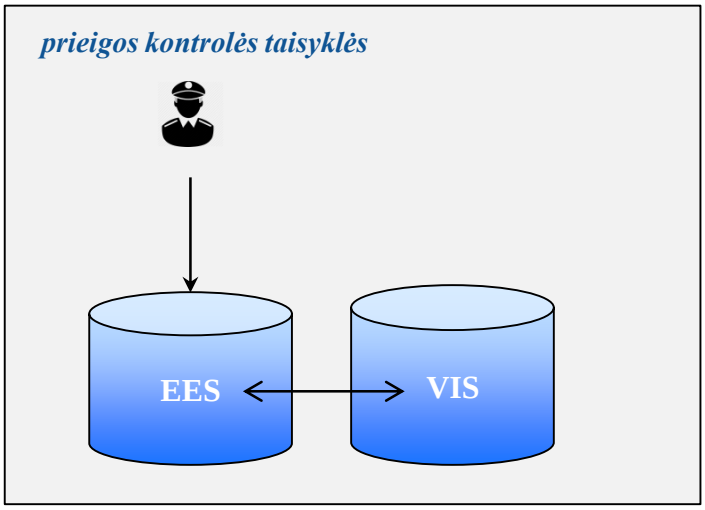
2. Informacinių sistemų tarpusavio sujungiamumas

Antrasis sąveikumo aspektas yra informacinių sistemų tarpusavio sujungiamumas. Tai reiškia, kad skirtingos sistemos ir duomenų bazės gali techniniu požiūriu „bendrauti“ tarpusavyje. **Vienoje sistemoje užregistruotus duomenis galima automatiškai tikrinti kitoje sistemoje centriniu lygmeniu**. Tam būtinas techninis sistemų suderinamumas, o šiose sistemose saugomi duomenų elementai (pvz., pirštų atspaudai) turi būti sąveikūs. Tarpusavio sujungiamumas gali sumažinti duomenų, kurie cirkuliuoja ryšių tinkluose ir yra perduodami per nacionalines sistemas, skaičių.

Tarpusavio sujungiamumui būtinos tinkamos duomenų apsaugos priemonės ir griežtos prieigos kontrolės taisyklės. 2015 m. gruodžio mėn. teisėkūros institucijų pasiektu politiniu susitarimu dėl duomenų apsaugos reformos visoje ES bus įdiegta moderni duomenų apsaugos sistema, kurioje bus numatytos šios apsaugos priemonės. Svarbu, kad teisėkūros institucijos nedelsiant priimtų Bendrąjį duomenų apsaugos reglamentą ir Duomenų apsaugos direktyvą.

Būsima EES sistema grindžiama tarpusavio sujungiamumo koncepcija. Būsima EES galės tiesiogiai susisiekti su VIS centriniu lygmeniu ir atvirkščiai. Tai svarbus žingsnis sprendžiant ES sienų kontrolės ir saugumo srities duomenų valdymo struktūros dabartinio susiskaidymo ir susijusias problemas. Nustačius automatinę kryžminę patikrą valstybėms narėms nebereikės vykdyti paieškos VIS atliekant patikrinimus kertant sieną, sumažės priežiūros reikalavimai ir pagerės sistemos veikimas.

***3 paveikslas**. Sistemų tarpusavio sujungiamumas. EES ir VIS pavyzdys*



Vėlesniu etapu Komisija ir „eu-LISA“ išnagrinės, ar centrinio lygmens būsimos EES ir VIS tarpusavio sujungiamumas gali būti išplėstas, kad apimtų SIS, ir ar galima tarpusavyje sujungti EURODAC ir SIS. Komisija ir „eu-LISA“ šią analizę atliks kartu su informacinių sistemų sąveikumo ekspertų grupe.

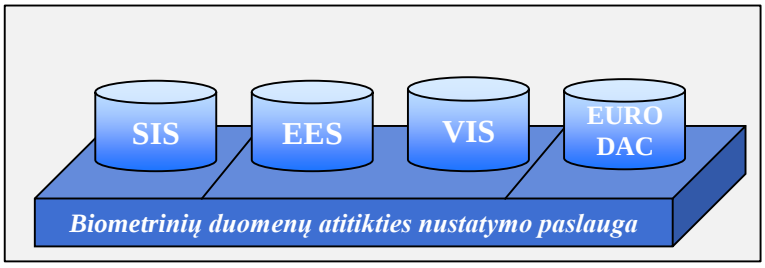
3. Bendra biometrinių duomenų atitikties nustatymo paslauga

Trečiasis sąveikumo aspektas yra susijęs su biometriniais identifikatoriais. Pavyzdžiui, kai vienos valstybės narės konsulate naudojantis tam tikra įranga paimami pirštų atspaudai, labai svarbu, kad šių atspaudų atitiktis galėtų būti patikrinta per VIS kitos valstybės narės pasienio poste, naudojant kito tipo įrangą. Toks pat reikalavimas taikomas ir pirštų atspaudų paieškai kitose sistemose – biometriniai pavyzdžiai turi atitikti būtiniausius kokybės ir formato reikalavimus, siekiant nesunkiai užtikrinti tokį sąveikumą.

Sistemos lygmeniu biometrinių identifikatorių sąveikumas leidžia naudoti bendrą biometrinių duomenų atitikties nustatymo paslaugą kelioms informacinėms sistemoms, laikantis asmens duomenų apsaugos taisyklių, suskaidžius duomenis, kiekvienos

kategorijos duomenims taikant atskiras prieigos kontrolės taisykles[27]. Tokios bendros paslaugos duoda didelės finansinės, priežiūros ir veikimo naudos.

4 paveikslas. *Bendra biometrinių duomenų atitikties nustatymo paslauga*



Komisija ir „eu-LISA“ išnagrinės, ar būtina ir techniškai įmanoma sukurti bendrą biometrinių duomenų atitikties nustatymo paslaugą visoms susijusioms informacinėms sistemoms. Komisija ir „eu-LISA“ šią analizę atliks kartu su informacinių sistemų ir sąveikumo ekspertų grupe.

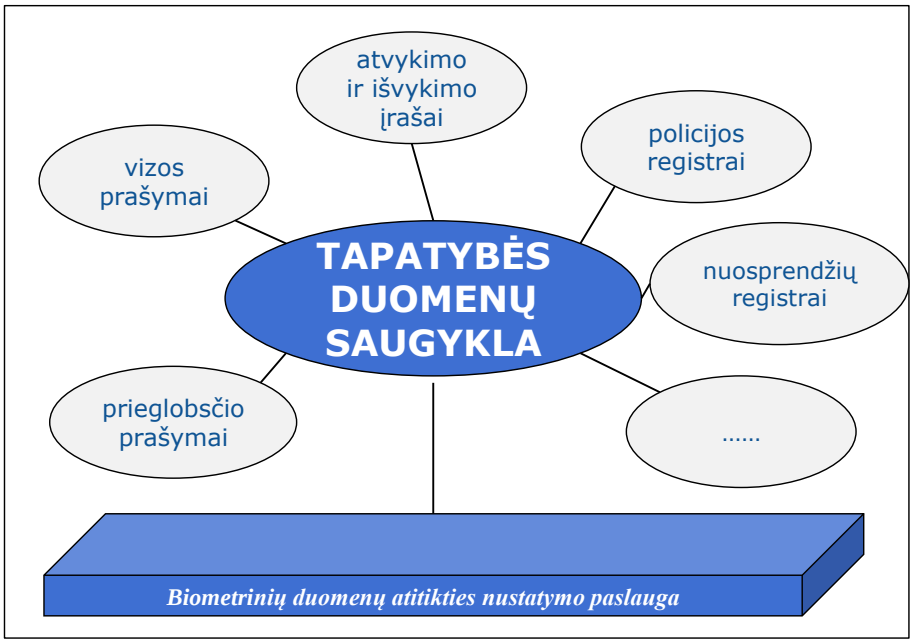
4. Bendra duomenų saugykla

Plačiausio užmojo ilgalaikis požiūris į sąveikumą būtų **bendra ES lygmens duomenų saugykla skirtingoms informacinėms sistemoms**. Bendrą duomenų saugyklą sudarytų pagrindinis modulis, kuriame būtų saugomi pagrindiniai duomenys (raidiniai skaitmeniniai ir biometriniai duomenys), o kiti duomenų elementai ir specifinės informacinių sistemų savybės (pvz., vizos duomenys) būtų saugomi konkrečiuose moduliuose. Pagrindinis modulis ir konkretūs moduliai būtų sujungti tarpusavyje, siekiant susieti atitinkamus duomenų rinkinius. Tai sukurtų **modulinį ir integruotą tapatybės valdymą sienų ir saugumo srityje**. Reikėtų užtikrinti, kad būtų laikomasi duomenų apsaugos taisyklių, pavyzdžiui, suskaidžius duomenis, kiekvienos kategorijos duomenims taikant atskiras prieigos kontrolės taisykles.

Sukūrus bendrą duomenų saugyklą būtų išspręsta dabartinio ES sienų kontrolės ir saugumo srities duomenų valdymo struktūros susiskaidymo problema. Šis susiskaidymas prieštarauja duomenų kiekio mažinimo principui, nes tie patys duomenys saugomi keletą kartų. Prireikus bendra saugykla sudarytų galimybę pripažinti ryšius ir susidaryti bendrą vaizdą, sujungiant skirtingose informacinėse sistemose saugomus atskirus duomenų elementus. Tokiu būdu būtų pašalintos esamos žinių spragos ir išaiškintos sienos apsaugos ir policijos pareigūnams nematomos pilkosios zonos.

[27] Panašiai vieną fizinį rinkmenų serverį dalijasi daugybė naudotojų, kurių kiekvienas turi konkrečias prieigos tik prie tam tikrų aplankų teises.

5 paveikslas. *Bendra duomenų saugykla*



Nagrinėjant bendros ES lygmens duomenų saugyklos sukūrimo galimybę kyla svarbūs susijusio duomenų apdorojimo tikslo, būtinumo, techninių galimybių ir proporcingumo apibrėžties klausimai. Tam reikėtų iš esmės persvarstyti teisinę sistemą, kuria sukuriamos įvairios informacinės sistemos ir šis tikslas galėtų būti pasiektas tik ilguoju laikotarpiu. Informacinių sistemų ir sąveikumo ekspertų grupė išnagrinės su bendra duomenų saugykla susijusius teisinius, techninius ir veikimo klausimus, taip pat duomenų apsaugos klausimus.

Visų minėtų keturių sąveikumo aspektų (bendra paieškos sąsaja, sistemų tarpusavio sujungiamumas, bendra biometrinių duomenų atitikties nustatymo paslauga ir bendra duomenų saugykla) atveju būtina užtikrinti, kad skirtingose informacinėse sistemose arba moduliuose saugomi duomenys būtų suderinami. Norint tai pasiekti, svarbu, kad būtų padaryta pažanga kuriant **vienodą pranešimų formatą** (UMF), siekiant sukurti visoms susijusioms informacinėms sistemoms taikomą bendrą standartą[28].

<u>Veiksmai, kuriais siekiama informacinių sistemų sąveikumo</u>

- Su ES agentūromis, nacionaliniais ekspertais ir susijusiais suinteresuotaisiais subjektais Komisija turi sudaryti **informacinių sistemų ir sąveikumo ekspertų grupę**, siekiant išnagrinėti informacinių sistemų sąveikumo didinimo teisinius, techninius ir veikimo aspektus, įskaitant turimų sprendimų būtinybę, technines galimybes bei proporcingumą ir jų poveikį duomenų apsaugai.

Bendra paieškos sąsaja

[28] Komisija parėmė tolesnį UMF rengimą 2012 m. Komunikate dėl Europos keitimosi informacija modelio (EKIM) ir šiuo metu finansuoja trečiąjį UMF bandomąjį projektą, kurio tikslas – sukurti bendrą visoms susijusioms duomenų bazėms taikomą standartą, naudojamą nacionaliniu (valstybių narių) lygmeniu, ES lygmeniu (centrinės sistemos ir agentūros) ir tarptautiniu lygmeniu (Interpolas).

- Komisija ir „eu-LISA“ turi padėti valstybėms narėms įdiegti bendrą paieškos sąsają, skirtą vykdyti paiešką centrinėse sistemose.
- Komisija ir „eu-LISA“ turi kartu su ekspertų grupe ištirti, ar bendros paieškos sąsajos gali būti naudojamos „vieno langelio“ paieškoms tuo pačiu metu visose susijusiose sistemose vykdyti, nekeičiant esamų prieigos teisių.

Informacinių sistemų tarpusavio sujungiamumas
- Komisija ir „eu-LISA“ turi kartu su ekspertų grupe išnagrinėti, ar centrinių informacinių sistemų tarpusavio sujungiamumas galėtų būti plėtojamas toliau, be jau siūlomo atvykimo ir išvykimo sistemos ir Vizų informacinės sistemos tarpusavio sujungiamumo.

Biometrinių duomenų atitikties nustatymo paslauga
- Komisija ir „eu-LISA“ turi kartu su ekspertų grupe išnagrinėti bendros biometrinių duomenų atitikties nustatymo paslaugos visoms susijusioms informacinėms sistemoms sukūrimo būtinybę ir technines galimybes.

Bendra duomenų saugykla (pagrindinis modulis)
- Komisija ir „eu-LISA“ turi kartu su ekspertų grupe ištirti ilgesnio laikotarpio tikslo sukurti bendrą duomenų saugyklą teisinį, techninį, veikimo ir finansinį poveikį.
- Komisija ir „eu-LISA“, turi prisijungti prie darbo, kuriuo siekiama sukurti visuotinį vienodą pranešimų formatą, taikomą visoms susijusioms informacinėms sistemoms.

8. IŠVADA

Šiuo komunikatu pradedamos diskusijos apie tai, kaip informacinės sistemos ES gali labiau sustiprinti sienų valdymą ir vidaus saugumą, remiantis didele Europos saugumo ir migracijos darbotvarkių sąveika. Daug informacinių sistemų jau teikia svarbią informaciją sienos apsaugos ir policijos pareigūnams, tačiau šios sistemos nėra tobulos. ES uždavinys – sukurti patikimesnę ir pažangesnę duomenų valdymo struktūrą, visapusiškai laikantis pagrindinių teisių, ypač teisės į asmens duomenų apsaugą ir jos tikslų apribojimo principo.

Esamos ES duomenų valdymo struktūros spragos turi būti pašalintos. Kartu su šiuo komunikatu Komisija pateikė pasiūlymą dėl atvykimo ir išvykimo sistemos, kuris turėtų būti priimtas kuo skubiau. Keleivio duomenų įrašo direktyva taip pat turi būti priimta artimiausiomis savaitėmis. Pasiūlymas dėl Europos sienų ir pakrančių apsaugos pajėgų turėtų būti priimtas iki vasaros. Kartu Komisija toliau dės pastangas stiprinti ir prireikus atnaujinti esamas sistemas, pavyzdžiui, kuriant automatinės pirštų atspaudų identifikavimo sistemos funkciją Šengeno informacinei sistemai.

Laikydamosi savo teisinių įsipareigojimų, valstybės narės turi visapusiškai naudotis esamomis informacinėmis sistemomis bei sukurti reikalingas technines jungtis su visomis informacinėmis sistemomis ir duomenų bazėmis. Esami trūkumai, pavyzdžiui, Priumo sistemoje, turi būti nedelsiant pašalinti. Šiuo komunikatu pradedamos diskusijos ir sisteminių trūkumų bei spragų šalinimo procesas, tačiau valstybės narės turi skubiai pašalinti likusius trūkumus, susijusius su duomenų teikimu ES duomenų bazėms ir informacijos mainais visoje Sąjungoje.

Siekiant struktūriniu požiūriu pagerinti ES sienų kontrolės ir saugumo srities duomenų valdymo struktūrą, šiuo komunikatu pradedamas procesas siekiant informacinių sistemų sąveikumo. Komisija sudarys informacinių sistemų ir sąveikumo ekspertų grupę, kuri išnagrinės sprendimų, kuriais bus užtikrinamas informacinių sistemų sąveikumas ir

šalinami trūkumai bei spragos, teisinius, techninius ir veikimo aspektus. Gavusi ekspertų grupės išvadas, Europos Komisija pateiks tolesnes konkrečias idėjas Europos Parlamentui ir Tarybai, ir jomis remiantis bus galima bendrai diskutuoti dėl tolesnių veiksmų. Komisija taip pat prašys Europos duomenų apsaugos priežiūros pareigūną ir nacionalines duomenų apsaugos institucijas, kurios kartu dirbs 29 straipsnio darbo grupėje, kad pateiktų pastabų.

Tikslas – sukurti bendrą strategiją, siekiant, kad duomenų valdymas ES taptų veiksmingesnis ir efektyvesnis, visapusiškai laikantis duomenų apsaugos reikalavimų, siekiant geriau apsaugoti ES išorės sienas ir didinti vidaus saugumą visų piliečių labui.

1 PRIEDAS. SANTRUMPOS

API	Išankstinė informacija apie keleivius
AFIS	Automatinė pirštų atspaudų identifikavimo sistema: sistema, galinti užfiksuoti, saugoti, palyginti ir patikrinti pirštų atspaudus.
MIS	Muitinės informacinė sistema
ECRIS	Europos nuosprendžių registrų informacinė sistema
EES	(siūloma) Atvykimo ir išvykimo sistema
EKIM	Europos keitimosi informacija modelis
EIS	Europolo informacinė sistema
EPRIS	Europos policijos registrų informacinė sistema
EURODAC	Europos daktiloskopinės informacijos sistema
Europolas	Europos policijos biuras (Europos Sąjungos teisėsaugos agentūra)
ETIAS	(galima) ES kelionių informacijos ir leidimų sistema
eu-LISA	Europos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra
FIND	Interpolo fiksuotojo ryšio tinklo duomenų bazė
FRONTEX	Europos operatyvaus bendradarbiavimo prie Europos Sąjungos valstybių išorės sienų valdymo agentūra
iARMS	(Interpolo) duomenų apie neteisėtus ginklus ir jų sekimo valdymo sistema
Interpolas	Tarptautinė kriminalinės policijos organizacija
MIND	Interpolo judriojo ryšio tinklo duomenų bazė
PIU	Informacijos apie keleivius skyrius: skyrius, kuris turi būti įsteigtas kiekvienoje valstybėje narėje ir gauti PNR duomenis iš vežėjų.
PNR	Keleivio duomenų įrašas
Priumo sistema	Policijos bendradarbiavimo mechanizmas, skirtas keistis informacija apie DNR, pirštų atspaudus ir transporto priemonių registracijos duomenis
„SafeSeaNet“	Europos valstybių narių jūrų institucijų keitimosi laivybos duomenimis platforma
ŠSK	Šengeno sienų kodeksas
SIENA	Saugaus keitimosi informacija tinklo programa
SIS	Šengeno informacinė sistema (kartais vadinama antrosios kartos – SIS II)
PPKD	(Interpolo) Pavogtų ir pamestų kelionės dokumentų duomenų bazė
sTESTA	saugus Telematikos paslaugų tarp Europos administracijų ryšių tinklas (turi būti modernizuotas į naujos kartos TESTA-NG)
UMF	Vienodas pranešimų formatas: pranešimų formatas, kuriuo sudaromos sąlygos suderinti informacines sistemas
VIS	Vizų informacinė sistema
TPRD	Transporto priemonių registracijos duomenys

2 PRIEDAS. ESAMŲ SIENŲ VALDYMUI IR TEISĖSAUGAI SKIRTŲ INFORMACINIŲ SISTEMŲ APRAŠAS

1. Šengeno informacinė sistema (SIS)

SIS yra didžiausia ir plačiausiai naudojama imigracijos ir teisėsaugos informacijos mainų platforma. Tai centralizuota sistema, kuria naudojasi 25 ES valstybės narės[29] ir keturios asocijuotosios Šengeno šalys[30], kurioje šiuo metu yra 63 mln. perspėjimų. Juos registruoja ir jų paiešką vykdo kompetentingos institucijos, kaip antai policija, sienų kontrolės ir imigracijos institucijos. Šioje sistemoje saugomi įrašai apie trečiųjų šalių piliečius, kuriems draudžiama atvykti arba būti Šengeno erdvėje, taip pat ES ir trečiųjų šalių piliečius, kurie yra ieškomi arba dingę (įskaitant vaikus), ir apie ieškomus daiktus (šaunamuosius ginklus, transporto priemones, tapatybės dokumentus, pramonės įrangą ir kt.). Išskirtinė SIS ypatybė, palyginti su kitomis dalijimosi informacija priemonėmis, yra ta, kad šią informaciją papildo nurodymai, kokių konkrečių veiksmų turi imtis pareigūnai vietoje, pavyzdžiui, sulaikyti arba konfiskuoti.

SIS patikrinimai yra privalomi tvarkant trumpalaikes vizas, vykdant trečiųjų šalių piliečių patikrinimus kertant sieną ir, nesistemiškai[31], vykdant ES piliečių ir kitų asmenų, kurie naudojasi laisvo judėjimo teise, patikrinimus kertant sieną. Be to, policijai atliekant kiekvieną patikrinimą Šengeno teritorijoje, turėtų būti automatiškai patikrinama SIS.

2. Vizų informacinė sistema (VIS)

VIS yra centralizuota sistema, skirta valstybėms narėms keistis duomenimis apie trumpalaikes vizas. Ja tvarkomi duomenys ir sprendimai dėl prašymų išduoti trumpalaikes vizas atvykti į Šengeno zoną arba vykti per ją tranzitu. Prie sistemos prisijungę visi Šengeno valstybių konsulatai (apie 2000) ir visi tų valstybių išorės sienos perėjimo punktai (iš viso apie 1800).

VIS pateikiami duomenys apie vizų prašymus ir sprendimus, taip pat informacija apie tai, ar išduotos vizos atšaukiamos, panaikinamos ar pratęsiamos. Šiuo metu joje pateikiami duomenys apie 20 mln. vizų prašymų ir piko metu joje įvykdoma daugiau kaip 50 000 operacijų per valandą. Kiekvienas vizos prašytojas pateikia išsamią biografinę informaciją, skaitmeninę nuotrauką ir dešimt pirštų atspaudų. Tai patikimas būdas patikrinti vizos prašytojo asmens tapatybę, įvertinti galimus neteisėtos migracijos ir saugumo rizikos atvejus, taip pat užkirsti kelią palankiausių vizų išdavimo sąlygų paieškai.

Sienos perėjimo punktuose arba valstybių narių teritorijoje VIS naudojama patikrinti vizos turėtojų tapatybę palyginant jų pirštų atspaudus su VIS saugomais pirštų atspaudais. Šis procesas užtikrina, kad asmuo, pateikęs prašymą išduoti vizą, yra tas pats asmuo, kuris kerta sieną. Pirštų atspaudų paieška VIS taip pat sudaro galimybę atpažinti asmenį, pateikusį prašymą išduoti vizą per pastaruosius penkerius metus, kuris gali su savimi neturėti tapatybės dokumentų.

3. EURODAC

EURODAC (Europos daktiloskopinės informacijos sistema) saugomi prieglobsčio prašytojų ir trečiųjų šalių piliečių, neteisėtai kertančių Šengeno išorės sienas, pirštų

[29] Visos, išskyrus Airiją, Kiprą ir Kroatiją.
[30] Šveicarija, Lichtenšteinas, Norvegija ir Islandija.
[31] Ši taisyklė bus keičiama, kaip numatyta Komisijos pasiūlyme COM/2015/0670 dėl Šengeno sienų kodekso dalinio pakeitimo.

atspaudai. Pagrindinis jos tikslas šiuo metu yra nustatyti, kuri ES šalis yra atsakinga už prieglobsčio prašymo nagrinėjimą pagal Dublino reglamentą. Ji naudojama sienos perėjimo punktuose, tačiau, kitaip nei SIS ir VIS, nėra sienų valdymo sistema.

Neteisėtų migrantų, kurie į ES atvyksta neteisėtai, pirštų atspaudai paimami sienos perėjimo punktuose. Šie atspaudai saugomi EURODAC sistemoje, siekiant patikrinti asmens tapatybę, jei ateityje bus pateiktas prieglobsčio prašymas. Imigracijos ir policijos institucijos taip pat gali palyginti ES valstybėse narėse esančių neteisėtų migrantų pirštų atspaudų duomenis, kad patikrintų, ar jie yra pateikę prieglobsčio prašymą kitoje valstybėje narėje. Teisėsaugos institucijos ir Europolas taip pat turi teisę atlikti paiešką EURODAC sistemoje, kad užkirstų kelią sunkiam nusikaltimui ar teroristiniam nusikaltimui, jį nustatytų arba tirtų.

Prieglobsčio prašytojų arba neteisėtų migrantų pirštų atspaudus užregistravus centrinėje sistemoje galima nustatyti ir stebėti jų antrinį judėjimą[32] ES, kol bus pateiktas tarptautinės apsaugos prašymas arba priimtas sprendimas grąžinti (ateityje, su atitinkamu perspėjimu SIS). Apskritai, nustatyti neteisėtų migrantų tapatybę ir juos stebėti yra būtina, siekiant užtikrinti, kad institucijos jų šalyse galėtų parengti naujus jų dokumentus, ir tokiu būdu būtų palengvinamas jų grįžimas.

4. Pavogtų ir pamestų kelionės dokumentų (PPKD) duomenų bazė

Interpolo pavogtų ir pamestų kelionės dokumentų (PPKD) duomenų bazė yra centrinė duomenų bazė, skirta pasams ir kitiems kelionės dokumentams, kurie, kaip išduodančios institucijos pranešė Interpolui, buvo pavogti arba pamesti. Joje taip pat saugoma informacija apie pavogtus tuščius pasų blankus. Informacija apie kelionės dokumentus, apie kuriuos SIS dalyvaujančių šalių institucijoms buvo pranešta, kad jie pamesti arba pavogti, įtraukiama tiek į PPKD, tiek į SIS. PPKD taip pat saugomi duomenys apie kelionės dokumentus, kuriuos užregistravo SIS nedalyvaujančios šalys (Airija, Kroatija, Kipras ir trečiosios šalys).

Kaip nurodyta 2015 m. lapkričio 20 d. Tarybos išvadose ir 2015 m. gruodžio 15 d. Komisijos pasiūlyme dėl Reglamento dėl Šengeno sienų kodekso tikslinio pakeitimo[33], visų trečiųjų šalių piliečių ir asmenų, kurie naudojasi laisvo judėjimo teise, kelionės dokumentai turėtų būti patikrinti PPKD. Visi pasienio kontrolės postai turi būti prisijungę prie PPKD. Be to, teisėsaugos institucijų nacionaliniu lygmeniu vykdoma paieška PPKD suteiktų papildomos saugumo naudos.

5. Išankstinė informacija apie keleivius (API)

API tikslas – surinkti informaciją apie asmens tapatybę prieš įlaipinimą skrydžiams į ES ir nustatyti neteisėtai atvykstančius migrantus. API duomenis sudaro kelionės dokumente pateikiama informacija, susijusi su keliautojo vardu ir pavarde, gimimo data, pilietybe, kelionės dokumento numeriu ir rūšimi, taip pat informacija apie išvykimo ir atvykimo sienos perėjimo punktą, ir informacija apie transportą. Su keleiviu susiję API duomenys paprastai renkami keleivių registravimo metu.

Iki atvykimo teikiama informacija, susijusi su jūrų transportu, pagal Konvenciją dėl tarptautinės jūrų laivybos sąlygų lengvinimo turi būti perduodama likus 24 valandoms iki

[32] Pavyzdžiui, į Graikiją atvykstantys pabėgėliai, neketinantys pateikti prieglobsčio prašymo Graikijoje, bet sausuma keliaujantys toliau į kitas valstybes nares.

[33] COM(2015) 670 final. Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo dėl atitinkamų duomenų bazių tikrinimo prie išorės sienų sugriežtinimo iš dalies keičiamas Reglamentas (EB) Nr. 562/2006.

numatyto laivo atvykimo. Direktyvoje 2010/65/ES[34] numatytas elektroninis duomenų perdavimas naudojantis vieno langelio sistema, su kuria susiejamos „SafeSeaNet“, elektroninės muitinės ir kitos elektroninės sistemos.

Centrinės ES lygmens API duomenų registravimo sistemos nėra.

6. Europolo informacinės sistemos

Europolo informacinė sistema (EIS) yra centralizuota kriminalinės informacijos duomenų bazė, skirta naudoti tyrimo tikslais. Ja gali naudotis valstybės narės ir Europolas, duomenims apie sunkius nusikaltimus ir terorizmą saugoti ir vykdyti jų paiešką. EIS saugoma informacija yra susijusi su duomenimis apie asmenis, tapatybės dokumentus, automobilius, šaunamuosius ginklus, telefono numerius, elektroninio pašto laiškus, pirštų atspaudus, DNR, ir su elektroniniais nusikaltimais susijusią informaciją, kurie gali būti įvairiais būdais susieti tarpusavyje, siekiant sudaryti išsamesnį ir struktūriškenį nusikaltimo vaizdą. EIS remiamas teisėsaugos bendradarbiavimas ir ji nėra prieinama sienų kontrolės institucijoms.

Keitimasis informacija vyksta per platformą SIENA[35], kuri yra saugus elektroninių ryšių tinklas tarp Europolo, ryšių biurų, nacionalinių Europolo padalinių, paskirtų kompetentingų institucijų (pvz., muitinių, turto susigrąžinimo tarnybų ir kt.) ir susijusių trečiųjų šalių.

2017 m. gegužės mėn. bus pradėtas taikyti naujas teisinis Europolo veiklos pagrindas. Šis pagrindas leis sustiprinti Europolo operatyvinius pajėgumus atlikti analizę ir geriau nustatyti turimos informacijos ryšius.

7. Priumo sistema

Priumo sistema yra pagrįsta daugiašaliu valstybių narių susitarimu[36], kuris sudaro sąlygas keistis DNR, pirštų atspaudais ir transporto priemonių registracijos duomenimis (TPRD). Šis principas pagrįstas konkrečios nacionalinės sistemos sujungimu su visų kitų ES valstybių narių nacionalinėmis sistemomis, siekiant suteikti galimybę nuotoliniu būdu vykdyti kryžminę paiešką. Jeigu atlikus paiešką gaunamas teigiamas rezultatas kitų valstybių narių duomenų bazėje, išsamiais teigiamo rezultato duomenimis keičiamasi per dvišalius mainų mechanizmus.

---

[34] 2010 m. spalio 20 d. Europos Parlamento ir Tarybos direktyva 2010/65/ES dėl pranešimo formalumų, taikomų į valstybių narių uostus įplaukiantiems ir (arba) iš jų išplaukiantiems laivams, kuria panaikinama Direktyva 2002/6/EB.

[35] Angl. *Secure Information Exchange Network Application* (Saugaus keitimosi informacija tinklo programa).

[36] 2005 m. Priumo konvencija. 2008 m. Konvencija buvo įtraukta į ES teisės aktus Tarybos sprendimu 2008/615/TVR.

8. Europos nuosprendžių registrų informacinė sistema (ECRIS)

ECRIS yra elektroninė sistema, leidžianti keistis informacija apie ankstesnius ES baudžiamųjų teismų priimtus nuosprendžius dėl konkrečių asmenų, kuri reikalinga prieš atitinkamus asmenis vykdomame baudžiamajame procese, arba, jei tai leidžiama pagal nacionalinę teisę, kitiems tikslams. Nuosprendį priėmusi valstybė narė turi pranešti apie nuosprendį prieš kitos valstybės narės pilietį jo pilietybės valstybei narei. Pilietybės valstybė narė turi kaupti šią informaciją, todėl paprašyta gali pateikti naujausią informaciją apie savo piliečių teistumą baudžiamosiose bylose, nesvarbu, kurioje ES valstybėje narėje priimtas nuosprendis.

ECRIS taip pat sudaro galimybę keistis trečiųjų šalių piliečių ir asmenų be pilietybės teistumą informacija. Kiekvienoje valstybėje narėje paskirtos centrinės institucijos yra ECRIS tinklo kontaktiniai centrai, atliekantys tokias funkcijas kaip pranešimas apie teistumą, informacijos apie teistumą saugojimas, prašymas ir perdavimas.