Mnenje Evropskega ekonomsko-socialnega odbora – Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU (meje in vizumi) ter spremembi Odločbe Sveta 2004/512/ES, Uredbe (ES) št. 767/2008, Sklepa Sveta 2008/633/PNZ, Uredbe (EU) 2016/399 in Uredbe (EU) 2017/2226

(COM(2017) 793 final – 2017/0351 (COD))

Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU (policijsko in pravosodno sodelovanje, azil in migracije)

(COM(2017) 794 final – 2017/0352 (COD))

(2018/C 283/07)

Poročevalka: **Laure BATUT**

Zaprosilo	Evropska komisija, 18. 1. 2018
	Evropski parlament, 28. 2. 2018
Pravna podlaga	člen 304 PDEU
Pristojnost	strokovna skupina za zaposlovanje, socialne zadeve in državljanstvo
Datum sprejetja mnenja strokovne skupine	25. 4. 2018
Datum sprejetja mnenja na plenarnem zasedanju	23. 5. 2018
Plenarno zasedanje št.	535
Rezultat glasovanja	160/3/2
(za/proti/vzdržani)	

1. **Sklepi in priporočila**

1.1 Evropski ekonomsko-socialni odbor (EESO) meni, da je predlog Evropske komisije za izboljšanje interoperabilnosti informacijskih sistemov EU za meje in vizume ter policijsko in pravosodno sodelovanje, azil in migracije koristen in pozitiven;

1.2 EESO meni, da mora biti interoperabilnost strateški cilj EU, da bo ta ostala odprt prostor, v katerem bodo zagotovljene temeljne pravice in mobilnost. Obveznost EU in držav članic je ščititi življenje vseh ljudi in jim zagotavljati varnost; načelo nevračanja bi morale v celoti upoštevati.

1.3 Ukrepi glede interoperabilnosti bodo še toliko bolj razumljivi, ker:

— v okviru migracijske strategije EU vzpostavljajo pogoje za ravnovesje med svobodo in varnostjo, ob spoštovanju delitve pooblastil,

— bodo osebam, na katere se nanašajo, zagotavljali temeljne pravice, zlasti varstvo osebnih podatkov in zasebnosti, pravico dostopa do njihovih podatkov ter popravka in izbrisa teh podatkov v razumnem roku in v okviru razpoložljivih postopkov,

— bo v zvezi z njimi, tudi v vseh izvedbenih besedilih, poudarjena zahteva po upoštevanju načel varstva podatkov že v fazi načrtovanja (vgrajena zasebnost),

— ne bodo ustvarjali novih ovir za nemoten pretok potnikov in blaga;

1.4 EESO v zvezi z uporabo podatkov za kazenski pregon zahteva takšne postopke in jamstva, ki bodo:

— predvideli uporabo evropske zakonodaje, ki zagotavlja najvišjo raven zaščite (splošna uredba o varstvu podatkov),

— omogočali hitrejšo določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito,

— zainteresiranim osebam zagotavljali pravico do dvostopenjskega sodnega postopka,

— mladoletnim osebam, zlasti tistim brez spremstva, tudi če nimajo urejenega statusa, so preganjane ali so storile kazniva dejanja, zagotavljali pravico do pridobitve vizuma, zaščite in vključitve ter do pozabe v krajšem času, kot velja za polnoletne osebe.

1.5 EESO meni, da bi bilo treba sedanjo pravno podlago informacijskih sistemov okrepiti in pri tem upoštevati dejstvo, da se sistemi zbiranja podatkov lahko spreminjajo. Zavzema se za:

— okrepitev varnosti obstoječih podatkovnih zbirk in njihovih komunikacijskih kanalov,

— oceno učinka povečanega predhodnega nadzora na obvladovanje tveganja,

— stalni nadzor in ocenjevanje struktur, ki bi ju izvajali organi za varstvo podatkov (Evropski nadzornik za varstvo podatkov); EESO zahteva, da odgovorni vsako leto poročajo organom odločanja in Komisiji o varnosti sestavnih delov interoperabilnosti, vsaki dve leti pa o učinku ukrepov na temeljne pravice;

1.6 ESO meni, da se mora projekt opreti na usposobljeno osebje, in priporoča:

— poglobljene programe usposabljanja za ustrezne organe in uslužbence agencije eu-LISA,

— temeljito preverjanje usposobljenosti uslužbencev in kandidatov za to agencijo.

1.7 EESO izraža zaskrbljenost glede financiranja novega sistema. Da bi se izognili proračunskim odklonom in projekt do leta 2029 izvedli do konca, bo ključno spremljanje načrtovanja;

1.8 EESO priporoča obveščanje državljanov o napredovanju projekta vse do njegovega izteka; treba jih je nazorno podučiti, kakšne vrste nadzora nad njimi se izvajajo. Meni, da je treba predvideti možnost, da se celoten projekt prekine, če bi zloraba sistema ogrozila svobodo in temeljne pravice.

2. **Uvod**

2.1 Glede na mednarodne razmere v letu 2017, ki velja za nestabilno tako v smislu geopolitike kot v smislu notranje varnosti držav članic, je Svet večkrat pozval Komisijo, naj sprejme ukrepe za sledenje osebam, za katere se ocenjuje, da pomenijo tveganje in so že bile vključene v postopek shranjevanja podatkov v kateri od držav članic. Zbiranje podatkov o tem, kje prestopijo meje in kje se gibajo v Evropi, bi lahko bilo ključno za varnost Unije.

2.2 Evropski parlament je v resoluciji z dne 6. julija 2016 pozval Komisijo, naj zagotovi potrebna jamstva za zaščito podatkov.

2.3 Obravnavani besedili sta skladni s ciljem ohranitve in okrepitve schengenskega območja ([1]). Unija že ima več predpisov in digitalnih informacijskih storitev na področjih, povezanih z mejnim nadzorom oseb in blaga.

2.4 Naj spomnimo:

— **SIS: schengenski informacijski sistem**, eden najstarejših mehanizmov, ki je bil prenovljen in omogoča upravljanje zelo različnih opozoril v zvezi z osebami in blagom,

([1]) COM(2017) 570 final.

— **Eurodac: evropski sistem za primerjavo prstnih odtisov** prosilcev za azil in državljanov tretjih držav brez urejenega statusa na mejah in v državah članicah ter določitev države članice, odgovorne za prošnje (EESO 2016-02981, poročevalec: José Antonio Moreno Díaz ([2])),

— **VIS: vizumski informacijski sistem** (vizumski zakonik) za upravljanje vizumov za kratkoročno bivanje (EESO 2014-02932, poročevalca: Antonello Pezzini in Luis Miguel Pariza Castaños ([3])),

— **SVI: sistem vstopa/izstopa**, ki še čaka na sklep in naj bi se uporabljal za elektronsko upravljanje podatkov iz potnih listin in datumov vstopa/izstopa državljanov tretjih držav ob vstopu na schengensko območje (EESO 2016-03098 SOC/544, poročevalec: Cristian Pîrvulescu ([4])),

— **ETIAS: evropski sistem za potovalne informacije in odobritve**, ki še čaka na sklep in naj bi bil obsežen avtomatiziran sistem hrambe in predhodnega preverjanja podatkov državljanov tretjih držav, ki ne potrebujejo vizuma za gibanje na schengenskem območju (EESO 2016-06889 SOC/556, poročevalec: Jan Simons ([5])),

— **ECRIS-TCN: evropski sistem za izmenjavo informacij o kazenskih evidencah državljanov tretjih držav**, kot ga je predlagala Komisija, tj. digitalni sistem za izmenjavo informacij o sodnih odločbah, ki so jih nacionalna sodišča že izrekla.

2.5 Orodja, ki so trenutno na voljo pooblaščenemu organu, je mogoče primerjati s pametnim telefonom z različnimi aplikacijami, ki delujejo ločeno in vsaka daje svoje podatke.

2.6 Vsi sistemi razen SIS so usmerjeni v **obravnavo državljanov tretjih držav**. Vzpostavljenih je šest decentraliziranih sistemov, ki se med seboj dopolnjujejo. Rezultat iskanih informacij ustreza skupku različnih podatkov, ki jih iz različnih zbirk pridobijo preiskovalne službe, odvisno od pravic dostopa, ki so jim dodeljene.

2.7 Komisija je pripravljena odgovoriti na naslednje vprašanje:

— Katera metoda naj se uporabi, ne da bi bilo treba spreminjati vzpostavljene strukture in da bi se ohranilo njihovo dopolnjevanje, za uskladitev vseh podatkovnih zbirk istočasno, da bi se na točki vstopa na evropsko ozemlje z eno samo poizvedbo v sistemu vse informacije, ki so že zbrane v obstoječih podatkovnih zbirkah, usmerile k nadzornemu organu, ki je pooblaščen za poizvedovanje, ob upoštevanju predpisov o varstvu podatkov in temeljnih pravic?

2.8 Evropska komisija želi v obravnavanih predlogih:

2.8.1 ponuditi dodatne možnosti z dostopom do podatkovnih zbirk Europola in Interpola, ki že sodelujeta z evropskimi nadzornimi organi;

2.8.2 „sinhronizirati“ iskanje informacij, da bi se skrajšal odzivni čas za reševanje zadev migrantov ter po potrebi pospešil odziv varnostnih služb. Zato predlaga, da se vzpostavijo novi organi, ki bi omogočili usklajeno delovanje sedanjih podatkovnih zbirk.

2.9 **Cilji Komisije so odpraviti čim več pomanjkljivosti posameznih sistemov, izboljšati** upravljanje zunanjih meja schengenskega območja, prispevati k notranji varnosti Unije, obravnavati identitetne prevare, razrešiti primere posameznikov z več identitetami, poiskati osumljene ali obsojene osebe in preverjati njihovo identiteto na schengenskem območju.

2.10 Če ponovno uporabimo prispodobo pametnega telefona, pooblaščeni organ ne bo imel na razpolago le veliko aplikacij, temveč bo lahko z eno samo poizvedbo in z uporabo svoje kode za dostop zbiral podatke na vseh svojih nosilcih (namiznem računalniku, prenosnem računalniku, telefonu, tablici itd.).

([2]) UL C 34, 2.2.2017, str. 144.
([3]) UL C 458, 19.2.2014, str. 36.
([4]) UL C 487, 28.12.2016, str. 66.
([5]) UL C 246, 28.7.2017, str. 28.

3. **Delovanje sistema**

3.1 Komisija je izvedla posvetovanja in sestavila strokovno skupino na visoki ravni za informacijske sisteme in interoperabilnost ([6]), katere člane imenujejo države članice, države schengenske skupine in evropske agencije, kot sta eu-LISA ([7]) in FRA ([8]), pod vodstvom GD HOME.

Metoda: medsebojna povezljivost ali interoperabilnost?

3.1.1 **Medsebojna povezljivost** informacijskih sistemov pomeni, da je mogoče sisteme povezati tako, da lahko samodejno dostopajo do podatkov v drugem sistemu.

3.1.2 **Interoperabilnost** ([9]) je zmožnost različnih sistemov, da med seboj komunicirajo, si izmenjavajo podatke in uporabljajo izmenjane informacije glede na pravice za dostop do sistemov.

3.2 *Izbira interoperabilnosti*

3.2.1 Komisija meni, da interoperabilnost ne ovira trenutnega delovanja struktur in ne posega v trenutne pristojnosti ter da se bodo podatki še naprej hranili v varnih podatkovnih zbirkah. Kljub več možnostim prenosa bi to pomenilo prednost glede varnosti sistemov in podatkov, ki seveda ne bodo dostopni prek spleta. Besedili, ki sta predmet tega mnenja, sta si zelo podobni:

— eno, COM(2017) 793, se nanaša na interoperabilnost informacijskih sistemov za meje in vizume,

— drugo, COM(2017) 794, pa na policijsko in pravosodno sodelovanje, azil in migracije.

3.3 *Nova orodja*

3.3.1 Za zagotovitev interoperabilnosti bo morala nova struktura s štirimi novimi orodji dopolniti šest podatkovnih zbirk, da bo mogoče delo pospešiti z eno samo poizvedbo v sistemu ter da bodo zahtevke še vedno vlagale pooblaščene osebe.

3.4 *Evropski iskalni portal*

3.4.1 Pooblaščeni nadzorni organ (končni uporabnik) bi moral imeti enoten dostop do celotnega sistema. Namesto šestih iskanj bi bilo potrebno le eno (policija, carinski organi itd.), tako da bi hkrati pregledovali več zbirk iskanih podatkov, vendar pa teh podatkov ne bi hranili. Če podatki obstajajo, jih bo sistem našel. V primeru suma kaznivega dejanja ali teroristične dejavnosti prvo iskanje v zvezi z osebo, ki se preverja, morda ne bo prineslo nobenega rezultata („ni zadetka“), če pa se podatek ujema s katerim drugim („zadetek“) v podatkovnih zbirkah, kot so SIS, SVI in ETIAS, to lahko vodi v poglobljene raziskave in preiskavo.

3.5 *Skupna storitev za ugotavljanje ujemanja biometričnih podatkov (skupna BMS)*

3.5.1 Ta skupna platforma za ugotavljanje ujemanja bo omogočala sočasno iskanje ter primerjavo numeričnih in biometričnih podatkov, prstnih odtisov in fotografij iz osebnih dokumentov iz različnih podatkovnih zbirk, kot so SIS, Eurodac, VIS, *SVI* ([10]), *ECRIS*, ne pa tudi *ETIAS*; podatki, ki jih vsebujejo, bodo morali biti združljivi.

3.5.2 Numerični podatki se ne bodo hranili v prvotni obliki.

3.6 *Skupno odložišče podatkov o identiteti (CIR)*

3.6.1 V skupnem odložišču podatkov o identiteti bodo zbrani podatki o biografski in biometrični identiteti državljanov tretjih držav, ki se preverjajo bodisi na meji bodisi v državah članicah (na schengenskem območju). Funkcija, ki bo prikazovala ujemanje podatkov v različnih podatkovnih zbirkah, bo pospešila iskanje. Ti podatki se bodo pod nadzorom agencije eu-LISA in z njenimi varnostnimi ukrepi hranili tako, da nihče ne bo imel dostopa do več kot ene alfanumerične vrstice hkrati. Skupno odložišče podatkov o identiteti, ki bo razvito na podlagi sistemov SVI in ETIAS, ne sme povzročiti podvajanja podatkov. Odložišče bi se lahko uporabljalo tudi za civilna iskanja.

([6]) GD HOME, enota B/3, sklep Komisije C/2016/3780 z dne 17. junija 2016, http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=SLhttp://ec.europa.eu/transparency/regexpert/index.cfm?Lang=SL

([7]) Evropska agencija za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice

([8]) FRA: Agencija EU za temeljne pravice.

([9]) Sporočilo Komisije COM(2016) 205 final: Trdnejši in pametnejši informacijski sistemi za meje in varnost.

([10]) Ležeča pisava označuje, da besedila v zvezi s temi organi še niso bila sprejeta.

3.7 *Detektor več identitet (MID)*

3.7.1 Vloga detektorja več identitet bo zagotavljanje pravilne identifikacije dobrovernih oseb ter preprečevanje identitetne prevare z istočasno poizvedbo v vseh zbirkah podatkov. Doslej še nobena uprava ni uporabljala podobnega orodja, s katerim naj bi se izognili kraji identitet.

3.8 *Vloga agencije eu-LISA* ([11])

3.8.1 Naloga agencije, ki je bila ustanovljena leta 2011, je olajšati izvajanje politik EU na področju pravice, varnosti in svobode. Ta agencija s sedežem v Talinu (Estonija) že zagotavlja izmenjavo informacij med različnimi organi kazenskega pregona držav članic ter nemoteno delovanje obsežnih informacijskih sistemov in prosto gibanje oseb v schengenskem prostoru.

3.8.2 Agencija sodeluje pri projektu pametnih mej, v novem ustroju izmenjave podatkov pa je njena vloga hramba podatkov, ki se nanašajo na posameznike, na primer informacij v zvezi z organi, preiskavami in preiskovalci. Preverjala bo dovoljenja prosilcev ter zagotavljala varnost podatkov, tudi v primeru varnostnega incidenta [člen 44 predlogov COM (2017) 793 in 794].

3.8.3 **Uporaba univerzalnega formata sporočil** (UMF), ki ga je treba še ustvariti, naj bi olajšala delo z novimi obveznimi sistemi. To bo vključevalo vzpostavitev vmesnikov v državah članicah, ki jih še nimajo, ter začasen sistem prevajanja iz enega jezika v druge jezike.

3.9 *Varstvo osebnih podatkov (člena 8 in 7 Listine):*

3.9.1 Predlog uredbe priznava možnost incidentov, povezanih z varnostjo. Države članice in njihovi podatkovni sistemi morajo kot prvo upoštevati načela varstva podatkov, določena v besedilih, Pogodbi, Listini o temeljnih pravicah ter splošni uredbi o varstvu podatkov ([12]), ki začne veljati 25. maja 2018.

4. **Razprava**

4.1 *Dodana vrednost interoperabilnosti v demokraciji*

4.1.1 Unija potrebuje predpise in sredstva za preiskave, s katerimi bi se zaščitila pred kriminalom. Interoperabilnost informacijskih sistemov je priložnost za uveljavitev načela pravne države in varstvo človekovih pravic.

4.1.2 *SVI* in *ETIAS*, povezana z BMS in CIR, bosta omogočila nadzor sumljivih oseb pri prehajanju meja ter hranjenje podatkov o teh osebah. Vendar pa možnost, da organi kazenskega pregona prek BMS dostopajo „do informacijskih sistemov na ravni EU, ki niso povezani s kazenskim pregonom“ [člen 17 (CIR), predlogov COM(2017) 794 in 793)], ni združljiva s cilji, na katerih temeljita obravnavana predloga. EESO se pri tem sklicuje na načelo sorazmernosti (člen 300(4) PDEU) in Komisijo poziva, naj prepreči ureditve, ki bi spominjale na koncept „velikega brata“ ([13]), ter ustvarjanje ovir za prosto gibanje Evropejcev (člen 3 PEU).

4.1.3 Predlagani model za zbiranje in uporabo osebnih podatkov, pridobljenih na meji in na ozemlju Unije med nadzorom gibanja in dokumentov, naj bi bil neprepusten in dostopen le pooblaščenim osebam za zagotavljanje varnosti in upravljanja, omogočil pa bo tudi, da bodo postopki hitreje stekli.

4.1.4 EESO dvomi o neprepustnosti sistema: obstoječe pomanjkljivosti ne bodo odpravljene, sistem se bo razvijal devet let na podlagi temeljev, ki še ne obstajajo, kot sta podatkovni zbirki SVI in ETIAS ter nacionalni vmesniki. Tehnologija se nenehno razvija in projekt mora temeljiti na najnovejšem tehnološkem razvoju, nima pa na voljo sredstev za obvladovanje zastarelosti, ki se pojavlja v nekaterih digitalnih sektorjih.

([11]) Uredba (EU) št. 1077/2011 Evropskega parlamenta in Sveta z dne 25. oktobra 2011 o ustanovitvi Evropske agencije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice.

([12]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). Mnenji EESO: UL C 229, 31.7.2012, str. 90, in UL C 345, 13.10.2017, str. 138.

([13]) Iz romana *1984* Georgea Orwella.

4.1.5 Poleg tega bi se lahko v projektu upošteval hiter napredek pri uporabi algoritmov umetne inteligence, bodisi kot orodje za nadzor sistema bodisi kot varnostni ključ za organe odločanja, ki zagotavljajo demokratično uporabo arhitekture.

4.1.6 Predlog uvaja sistem za tiste, ki delujejo v dobri veri in spoštujejo zakone. Dejstvo, da bi sistem nadzorovali ljudje, je pomirjujoče, vendar pa so lahko ljudje tudi šibki člen. EESO predlaga, naj se doda člen, ki bi določal t. i. varovalke v primeru politične krize ali krize upravljanja, saj lahko kakršna koli težava v eni od podatkovnih zbirk pomeni tveganje za celotno strukturo ([14]). Splošna raba UMF bi lahko privedla do mednarodne uporabe, ki bi bila zelo pozitivna, vendar zelo tvegana z vidika varstva podatkov. Pooblaščeni orani bodo imeli veliko odgovornost. V obravnavanih dokumentih ti vidiki niso predvideni.

4.2 *Varstvo temeljnih pravic*

4.2.1 Temeljne pravice so absolutne; omejitve uresničevanja teh pravic so dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ter če se spoštuje njihova bistvena vsebina (člena 8 in 52(1) Listine o temeljnih pravicah). EESO se sprašuje, kako se lahko oceni sorazmernost nadzornih ukrepov v primeru migrantov, ki bežijo pred preganjanjem in iščejo azil na obalah Unije. [COM(2017) 794 final, obrazložitveni memorandum – temeljne pravice]. Iskanje osumljencev z namenom preprečevanja kaznivih dejanj, zlasti teroristov, **ne sme približati naših demokracij pojmu domneve o krivdi**; ohraniti je treba razlikovanje med dejanji, ki kalijo javni red, in mnenji.

4.2.2 Spoštovanje pravic, določenih v Listini, za vse ljudi mora zagotavljati ravnovesje med varnostjo in svobodo, brez katerega ni demokracije. EESO meni, da je to ravnovesje bistveno in da mora biti stalen cilj vseh organov, vključno z nadzornimi, na nacionalni in evropski ravni.

4.2.3 V sistemu bodo shranjeni podatki o organih, povezanih z določenim iskanjem, ter s tem povezani metapodatki. Spoštovati je treba tudi temeljne pravice teh pooblaščenih organov v zvezi z ustvarjenimi podatki, zlasti v zvezi z njihovo varnostjo in zasebnostjo, v primeru zlonamernega vdora v strukturo in zlorabe podatkov v času od njihovega vnosa do izbrisa.

4.3 *Varstvo podatkov*

4.3.1 Predloga priznavata načelo vgrajenega in privzetega varstva osebnih podatkov, čeprav je iz njunih obrazložitvenih memorandumov razvidno, da po mnenju Sodišča EU ta pravica ni absolutna. EESO priznava prednosti preventivnih ukrepov za zagotavljanje varnosti, preprečevanje lažnih identitet in zagotavljanje pravice do azila, vendar poudarja omejitve numeričnih podatkov in anonimizacije podatkov, saj lahko posamezniki, na katere se podatki nanašajo, te podatke kasneje še potrebujejo.

4.3.2 Poudarja tudi, da je vrsta shranjenih biometričnih in bioloških podatkov v posebnem interesu nekaterih podjetij. Kibernetska varnost je pri tem enako pomembna kot fizična varnost, vendar je v predlogih premalo poudarjena. Podatki se bodo hranili le na eni fizični lokaciji, ki bo kljub zaščiti izpostavljena določenim tveganjem.

4.3.3 Kar zadeva varstvo podatkov in pravico do izbrisa (pravico do pozabe), EESO opozarja, da morajo institucije in organi Unije upoštevati Uredbo (ES) št. 45/2001, ki zagotavlja nižjo stopnjo zaščite kot splošna uredba o varstvu podatkov ([15]) iz leta 2016 (ki začne veljati maja 2018), ki jo morajo upoštevati države članice. EESO poudarja zapletenost izvajanja te pravice in izraža zaskrbljenost, da je potniki, migranti in prosilci za azil ne bodo mogli uveljavljati:

1. varstvo osebnih podatkov mora biti zagotovljeno za vse obstoječe nacionalne in evropske podatkovne zbirke, da zaščiti celoten sistem;

2. nujno je, da se državljani strinjajo s tem obsežnim sistemom nadzora nad njimi.

4.3.4 V predlogih ni jasno določeno, kako dolgo pooblaščeni organi hranijo zbrane podatke. Besedili navajata postopek za izvedbo popravka in/ali izbrisa, ki vključuje zaprošeno državo in odgovorno državo, ne določata pa trajanja hrambe podatkov (člen 47 predlogov). EESO priporoča, da se to obdobje določi in da naj bo krajše za mladoletne osebe (člen 24 Listine), razen v primerih terorizma, zato da bi te imele možnosti za vključevanje.

([14]) Evropski nadzornik za varstvo podatkov, Končno poročilo strokovne skupine na visoki ravni (priloga), maj 2017.
([15]) Splošna uredba o varstvu podatkov (Uredba (EU) 2016/679).

4.4 *Upravljanje in obveznost poročanja*

4.4.1 Za mednarodne podatkovne zbirke ne veljajo enaka pravila kot za evropske informacijske sisteme. Uvedba univerzalnega dostopa, ki bi lahko postala mednarodna, bo le tehnični element, ki ne bo poenotil predpisov, čeprav mora Interpol vsekakor upoštevati člen 17 pakta OZN ([16]). Poleg tega bodo za dovoljenja še naprej pristojne države članice. EESO meni, da bi bilo v teh predlogih treba to vprašanje obravnavati.

4.4.2 Sodbo bosta izrekli ena sama poizvedba in povezanost evropskih podatkovnih zbirk. EESO poudarja, da bo birokracija, povezana s tem, več kot sorazmerna glede na pospešitev postopkov. Za upravljanje bo v okviru postopka nadzora skrbela Komisija skupaj z državami članicami. Osrednji element sistema bo agencija eu-LISA, ki bo odgovorna predvsem za izvajanje postopkov zbiranja informacij o delovanju interoperabilnosti. Prejemala bo informacije od držav članic in Europola ter Svetu, Evropskemu parlamentu in Komisiji vsaka štiri leta predložila poročilo o tehničnem vrednotenju, Komisija pa bo nato leto pozneje objavila svoje splošno poročilo (člen 68 predlogov). Po mnenju EESO so ta obdobja veliko predolga. Oceno varnosti sestavnih delov interoperabilnosti [člen 68(5)(d)] bi bilo treba izvesti vsaj enkrat letno, oceno učinka na temeljne pravice pa vsaj enkrat na dve leti [člen 68(5)(b)].

4.4.3 EESO obžaluje, da so za tako temeljna vprašanja, kot so obravnavana v zadevnih predlogih, odgovorne evropske agencije, saj sta zaposlovanje v teh agencijah in njihovo delovanje po mnenju številnih državljanov nepregledna. Meni, da je treba izmenjati dobre prakse in se posvetovati z vsemi neodvisnimi nadzornimi organi (ENVP) ter drugimi agencijami, kot sta FRA in ENISA.

4.4.4 Vse te nove strukture in postopki bodo uvedeni z delegiranimi in izvedbenimi akti Komisije. EESO upa, da bo cilj spoštovanja temeljnih pravic in varstva osebnih podatkov vključen v vse akte tudi v prihodnosti, da se bo izboljšal postopek sprejema oseb na mejah. Priporoča obveščanje evropskih državljanov o vseh fazah projekta vse do njegovega izteka; nazorno jih je treba podučiti, kakšne vrste nadzora nad njimi se izvajajo.

5. **Potrebno usposabljanje za nadzorne organe v vsej Uniji**

5.1 EESO v nasprotju z mnenjem Komisije iz povzetka ocene učinka (C) meni, da bo na začetku potrebnih veliko usposabljanj (po letu 2021). Komisija omenja znesek 76 milijonov EUR letno. Pri prehodih na nove postopke so vedno potrebne nadgradnje. To velja za vse meje Unije in nacionalne sisteme. Nekatere države članice še nimajo združljivih sistemov ter bodo morale vložiti veliko truda in vzpostaviti vmesnike, ki jim bodo omogočili sodelovanje. Da bi interoperabilnost delovala, bi bilo treba odpraviti razlike med državami članicami.

5.2 Usposabljanje o uporabi kakovostnih podatkov in univerzalnega formata sporočil bo bistveno. EESO predlaga, da se skupaj z agencijami CEPOL ([17]), Frontex, Europol itd. vzpostavi skupni center za usposabljanje pooblaščenih organov, vključno z agencijo eu-LISA, pri čemer je treba temeljito preveriti pristojnosti njenih članov.

5.3 Orodje, kot je detektor več identitet, je edinstveno. Če bo uspešno, bo zelo učinkovito. Za novo strukturo bo potrebna največja možna kakovost podatkov. Da pa bo celoten projekt izpolnil pričakovanja, morajo biti vse države članice sposobne sodelovati na enaki ravni, sicer se bodo vrzeli še povečale, kar bi ogrozilo pravico do azila in pravico do dostopa do mednarodne zaščite (člena 18 in 19 Listine).

6. **Financiranje**

6.1 Celoten predlagani sistem temelji na določenih predpostavkah, in sicer da bodo organi odločanja sprejeli sisteme *SVI, ETIAS* in *UMF*, da bo *MID* deloval pravilno in da bo zagotovljena varnost CIR. Ali bosta imela Evropski nadzornik za varstvo podatkov in agencija eu-LISA ter morda tudi agencija ENISA na voljo dovolj zaposlenih ljudi in dovolj finančnih sredstev? Komisija predlaga sofinanciranje EU in držav članic. EESO ugotavlja, da upravljanje semestra še vedno poteka v znamenju varčevanja in da je treba sedanjo uporabo obstoječih zbirk (SIS, VIS, Prüm, SVI) dodatno poenostaviti v skladu z zakonskimi zahtevami (poročilo strokovne skupine).

([16]) Mednarodni pakt o državljanskih in političnih pravicah, OZN,17. člen: „1. Nikomur se ne sme nihče samovoljno ali nezakonito vmešavati v zasebno življenje, v družino, v stanovanje ali dopisovanje ali nezakonito napadati njegovo čast in ugled. 2. Vsakdo ima pravico do zakonskega varstva pred takim vmešavanjem ali pred takimi napadi."

([17]) CEPOL, Agencija Evropske unije za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Budimpešta, Madžarska).

6.2 EESO se sprašuje o proračunskih posledicah izstopa Združenega kraljestva, čeprav Združeno kraljestvo ni v schengenskem sistemu, na splošno pa o prihodnji zapletenosti upravljanja interoperabilnosti v državah, ki niso v SIS, vendar sodelujejo pri drugih podatkovnih zbirkah, npr. pri Eurodacu.

6.3 Predvideni sklad je Sklad za notranjo varnost, ki naj bi predvidoma začel delovati leta 2023. EESO se sprašuje, ali bo pet let dovolj za zmanjšanje razlik v Evropi in vzpostavitev pogojev za uspeh. Predvideni proračun znaša 424,7 milijona EUR za devet let (2019–2027), pri čemer bodo ta sredstva zagotovile EU (Sklad za notranjo varnost) in države članice. Države morajo poskrbeti za pravilno delovanje sedanjih sistemov z novo računalniško strukturo. EESO meni, da bi morala oživitev gospodarstva pomagati pri izvajanju teh naložb.

V Bruslju, 23. maja 2018

Predsednik
Evropskega ekonomsko-socialnega odbora
Luca JAHIER