

# EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

## Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl pasiūlymo dėl Tarybos pamatinio sprendimo dėl keitimosi informacija pagal prieinamumo principą (KOM (2005) 490 galutinis)

(2006/C 116/04)

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS,

atsižvelgdamas į Europos bendrijos steigimo sutartį, ypač į jos 286 straipsnį,

atsižvelgdamas į Europos Sąjungos pagrindinių teisių chartiją, ypač į jos 8 straipsnį,

atsižvelgdamas į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo,

atsižvelgdamas į prašymą dėl nuomonės pateikimo pagal 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo 28 straipsnio 2 dalį,

PRIĖMĖ ŠIĄ NUOMONĖ:

### I. PRELIMINARIOS PASTABOS

1. 2005 m. spalio 12 d. laišku Komisija atsiuntė Europos duomenų apsaugos priežiūros pareigūnui (EDAPP) pasiūlymą dėl Tarybos pamatinio sprendimo dėl keitimosi informacija pagal prieinamumo principą. EDAPP mano, kad šis laiškas yra prašymas patarti Bendrijos institucijoms ir organams, kaip numatyta Reglamento 45/2001/EB 28 straipsnio 2 dalyje. EDAPP mano, kad ši nuomonė turėtų būti paminėta pamatinio sprendimo preambulėje.
2. Ši nuomonė turi būti suprantama atsižvelgiant į II dalyje nurodytas aplinkybes. Kaip nurodyta II dalyje, nėra akivaizdu, kad šis pasiūlymas (arba pasiūlyme išdėstytas požiūris į prieinamumo principą) taps priimtu teisės aktu. Daug valstybių narių turi kitokių požiūrius.
3. Tačiau yra akivaizdu, kad teisėsaugos informacijos prieinamumas tarpvalstybiniu lygiu (ar net keitimasis tokia infor-

macija) yra aktualus darbotvarkių klausimas valstybėse narėse, tiek Taryboje, tiek už jos ribų bei Europos Parlamente.

4. Taip pat akivaizdu, kad šis dalykas yra labai aktualus atsižvelgiant į asmens duomenų apsaugos perspektyvą, kaip bus paaiškinta šioje nuomonėje. EDAPP primena, kad šį pasiūlymą Komisija pateikė jį artimai siedama su pasiūlymu dėl Tarybos pamatinio sprendimo dėl asmens duomenų, tvarkomų vykdančios policijos ir teismų bendradarbiavimą baudžiamosiose bylose, apsaugos, dėl kurio EDAPP pateikė nuomonę 2005 m. gruodžio 19 d.
5. EDAPP pasinaudos proga šioje nuomonėje pateikti kai kuriuos bendro pobūdžio ir svarbesnius požiūrio aspektus apie keitimąsi teisėsaugos informacija ir apie galimus šio klausimo reglamentavimo būdus. Pateikdamas šią nuomonę, EDAPP siekia užtikrinti, kad tolesnėse diskusijose dėl šio klausimo bus tinkamai atsižvelgta į duomenų apsaugos aspektus.
6. Su EDAPP bus galima konsultuotis ir vėliau, po to, kai įvyks atitinkami teisėkūros procedūros pokyčiai dėl šio pasiūlymo, taip pat bus galima konsultuotis ir dėl kitų susijusių pasiūlymų.

### II. PASIŪLYMO KONTEKSTAS

7. Į Hagos programą buvo įdiegtas prieinamumo principas, kuris yra naujas ir svarbus teisės principas. Jo esmė yra tai, kad kovai su nusikalstamumu reikalinga informacija turi būti be kliūčių keičiamasi per ES vidaus sienas. Šio pasiūlymo tikslas yra įgyvendinti šį principą privalomu teisės aktu.
8. Keitimasis policijos informacija tarp įvairių šalių yra populiarus tarp įstatymų leidėjų ES ir už jos ribų. EDAPP dėmesį patraukė šios naujos iniciatyvos.

9. Pirmiausia, 2004 m. birželio 4 d. Švedija pateikė pasiūlymą dėl Pamatinio sprendimo dėl keitimosi informacija ir žvalgybos informacija tarp Europos Sąjungos valstybių narių teisėsaugos institucijų supaprastinimo. 2005 m. gruodžio 1 d. posėdyje Taryba susitarė dėl bendrojo požiūrio dėl šio pasiūlymo.
10. Antra, 2005 m. gegužės 27 d. septynios valstybės narės Priume (Vokietija) pasirašė konvenciją dėl tarpvalstybinio bendradarbiavimo gerinimo, pirmiausia kovos su terorizmu, tarpvalstybiniu nusikalstamumu ir neteisėta migracija srityje. Joje *inter alia* įdiegiamos priemonės, kuriomis siekiama pagerinti keitimąsi informacija apie DNR ir pirštų atspaudus. Prie šios konvencijos gali prisijungti visos Europos Sąjungos valstybės narės. Susitariančiosios šalys siekia šios konvencijos nuostatas inkorporuoti į Europos Sąjungos teisinę sistemą.
11. Trečia, teisėsaugos informacijos prieinamumas Europos Sąjungos valstybėse bus padidintas kitais teisės aktais, pavyzdžiui, pasiūlymais dėl antros kartos Šengeno informacinės sistemos (SIS II), pasiūlymu dėl teisės naudotis Vizų informacine sistema (VIS) ir pasiūlymu dėl pamatinio sprendimo dėl valstybių narių keitimosi informacija apie teistumą organizavimo ir turinio. Šiuo atžvilgiu taip pat verta paminėti 2005 m. lapkričio 25 d. Komisijos komunikatą dėl Europos duomenų bazių teisingumo ir vidaus reikalų srityje geresnio veiksmingumo, didesnio sąveikumo ir optimalios sąveikos.
12. Kadangi buvo paskelbtos minėtos iniciatyvos, šis pasiūlymas dėl pamatinio sprendimo dėl prieinamumo neturėtų būti nagrinėjamas atskirai, o taip pat turi būti atsižvelgta ir į kitus požiūrius dėl keitimosi teisėsaugos informacija. Tai yra dar svarbiau, nes Taryboje yra tendencija teikti pirmenybę kitokiems požiūriams dėl keitimosi informacija ir prieinamumo nei šiame pasiūlyme Komisijos pasiūlytas požiūris. Esamo pasiūlymo teksto Taryba gali net ir nesvarstyti.
13. Be to, šis pasiūlymas yra artimai susijęs su pasiūlymu dėl pamatinio sprendimo dėl asmens duomenų apsaugos. Ši nuomonė turi būti nagrinėjama kartu su išsamesne nuomone dėl minėto pamatinio sprendimo.
14. EDAPP savo nuomonėje dėl pasiūlymo dėl pamatinio sprendimo dėl asmens duomenų apsaugos pabrėžė pakankamos duomenų apsaugos svarbą, kuri būtų būtina teisės akto dėl prieinamumo pasekmė. EDAPP manymu, toks teisės aktas neturėtų būti priimtas nesant esminių garantijų dėl duomenų apsaugos.
15. EDAPP laikosi tokios pačios nuomonės dėl kitų teisinių dokumentų, kurie palengvina teisėsaugos informacijos srautą per ES vidaus sienas, priėmimo. Todėl EDAPP palankiai vertina tai, kad Taryba ir Europos Parlamentas suteikė pirmenybę pirmiau minėtam pasiūlymui dėl pamatinio sprendimo dėl asmens duomenų apsaugos.

### III. PRIEINAMUMO PRINCIPŲ ESMĖ

16. Prieinamumo principas pats savaime yra paprastas. Informacija, kuri prieinama tam tikroms valstybės narės institucijoms, taip pat turi būti teikiama atitinkamoms kitų valstybių narių institucijoms. Valstybių narių institucijos informacija turi keistis kuo greičiau ir paprasčiau, pageidautina sudarydamos tiesioginės internetinės prieigos galimybę.

17. Sunkumai atsiranda dėl aplinkos, kurioje turi būti taikomas prieinamumo principas:

- Nevienalytė valstybių narių policijos ir teismų sandara, ir skirtingas atsakomybė ir pareigų paskirstymas;
- Naudojama įvairių rūšių (slapta) informacija (pavyzdžiui, DNR arba pirštų atspaudai);
- Skirtingi būdai kompetentingoms institucijoms pasinaudoti atitinkama informacija, net ir valstybių narių viduje;
- Sudėtinga užtikrinti, kad kitoje valstybėje narėje kilusi informacija bus tinkamai interpretuojama dėl kalbų, technologinių sistemų (sąveikos) ir teisinių sistemų skirtingumų.
- Jis turi būti įtrauktas į esamą ir sudėtingą teisės nuostatų sistemą, kuri skirta valstybių narių keitimuisi teisėsaugos informacija.

18. Nors aplinka sudėtinga, bendrai suvokiama, kad šis principas savaime negali funkcionuoti. Reikia papildomų priemonių siekiant užtikrinti, kad informacija būtų veiksmingai randama ir naudojama. Bet kuriuo atveju, šios priemonės turi padėti teisėsaugos institucijoms išsiaiškinti, ar kitų valstybių narių teisėsaugos institucijos turi reikiamą informaciją ir kur tokią informaciją galima rasti. Tokios papildomos priemonės gali būti sietuvai, kuriais naudojantis galima tiesiogiai pasinaudoti visais ar konkrečiais valstybių narių saugomais duomenimis. Todėl pasiūlyme dėl pamatinio sprendimo dėl prieinamumo nustatomi „rodyklės duomenys“ — konkretūs duomenys, kuriais galima tiesiogiai naudotis tarpvalstybiniu mastu.

19. Iš esmės, prieinamumo principas turėtų palengvinti valstybių narių keitimąsi informacija. Vidaus sienos bus panaikintos ir valstybės narės turi leisti, kad jų policijos institucijoms prieinama informacija vis labiau taptų prieinama kitoms institucijoms. Valstybės narės praranda kompetenciją kontroliuoti informacijos srautą, todėl vien nacionalinės teisės aktai jau nėra pakankama priemonė užtikrinti tinkamą informacijos apsaugą.
20. Todėl pasiūlymui reikia skirti ypatingą dėmesį, atsižvelgiant į asmens duomenų apsaugą. Pirmą, informacija kuri paprastai yra konfidenciali ir gerai saugoma, turi būti teikiama kitų valstybių narių institucijoms. Antra, kad sistema veiktų, reikia sukurti rodyklės duomenis ir leisti jais naudotis kitų valstybių institucijoms. Tuomet, įgyvendinus šį principą, bus galima naudotis daugiau duomenų nei šiuo metu.

#### IV. PAGRINDINIAI ELEMENTAI

##### Prieinamumo principo taikymo sritis

21. Pirmiausia yra svarbu apibrėžti kokių rūšių informacijai bus taikomas prieinamumo principas. Šio principo taikymo sritis bendrais bruožais yra apibrėžta pasiūlymo 2 straipsnyje kartu su 1 straipsnio 1 dalimi ir 3 straipsnio a punktu. Šis principas taikomas informacijai, kuri:
- egzistuoja;
  - išvardyta II priede, kuriame apibrėžiamos šešios informacijos rūšys;
  - prieinama kompetentingoms institucijoms.
- Komisijos pasiūlyme yra trys esminiai principo taikymo srities elementai. Išsamiau taikymo sritis yra apibrėžiama 2 straipsnyje. 2 straipsnio 1 dalyje prieinamumo principo taikymas ribojamas stadija iki baudžiamojo proceso pradžios, o 2 straipsnio 2, 3 ir 4 dalyse nurodoma daugiau konkrečių apribojimų.
22. Norint suprasti pasiūlymo pasekmes, reikia išsamiau išnagrinėti pirmiau minėtus tris esminius elementus. Pirmieji du taikymo srities elementai yra pakankamai aiškūs patys savaime. „Egzistuojančios informacijos“ sąvokos apibrėžimas yra 2 straipsnio 2 dalyje, kurioje nurodyta, kad pamatiniame sprendime nėra pareigos rinkti ir saugoti informaciją tik tam, kad ji būtų prieinama, o II priede esantis sąrašas negali būti aiškinamas kitokiu būdu. Išsamiau aptarti reikia trečiąjį esminį elementą, atskirai ir kartu su pirmaisiais dviem elementais.
23. Pasiūlyme nenurodoma, ar „prieinama informacija“ yra tik kompetentingų institucijų kontroliuojama informacija, ar taip pat apima ir informaciją, kurią šios institucijos gali gauti. Tačiau EDAPP mano, kad pasiūlymas gali būti aiškinamas, kad apimamos abi informacijos rūšys.
24. Iš tiesų, nors atrodo, kad 2 straipsnio 2 dalyje įtvirtinama siauresnė taikymo sritis, nurodant, kad pamatiniame sprendime „neįpareigojama rinkti ir saugoti informaciją [...] tik tam, kad ji būtų prieinama“, pagal 3 straipsnio a punktą galima platesnė interpretacija, nes jame nurodyta, kad „informacija“ — „egzistuojanti informacija, nurodyta II priede“.
25. II priede nurodytos bent dvi duomenų kategorijos, kurias paprastai kontroliuoja ne policijos institucijos. Pirmą kategorija yra transporto priemonių registravimo informacija. Daugelyje valstybių narių duomenų bazių, kuriose yra ši informacija, teisėsaugos institucijos nekontroliuoja, nors ir reguliariai jomis naudojasi. Ar šios rūšies informaciją turėtų apimti sąvoka „prieinama informacija“, kurią pagal 1 straipsnį galima teikti atitinkamoms kitų valstybių narių kompetentingoms institucijoms? Antroji paminėtina II priede nurodyta duomenų kategorija yra telefonų numeriai ir kiti ryšių duomenys: ar šie duomenys turėtų būti laikomi „prieinamais“, net jeigu šiuos duomenis kontroliuoja ne kompetentingos institucijos, o privačios įmonės?
26. Be to, kitos pasiūlymo nuostatos, o būtent 3 straipsnio d punktą ir 4 straipsnio 1 dalies c punktą leidžia manyti, kad „paskirtosios institucijos“ ar net „paskirtosios šalys“ gali kontroliuoti informaciją, kuri yra „prieinama“ „kompetentingoms institucijoms“. Pasiūlymo tekste taip pat matyti, kad „valstybės narės kompetentinga institucija“ yra ES sutarties 29 straipsnio pirmoje įtraukoje nurodyta institucija, o nacionalinė institucija gali būti laikoma „paskirtąja institucija“.
27. EDAPP mano, kad svarstant prieinamumo principo taikymą informacijai, kurią kontroliuoja paskirtosios institucijos ir paskirtosios šalys, kyla tokie klausimai:
- Ar 30 straipsnio 1 dalies b punktą yra pakankamas teisinis pagrindas, nes į trečiojo ramsčio sistemą nepatenka paskirtosios institucijos ir paskirtosios šalys, kurios turi pateikti informaciją, o taip pat duomenų bazės, iš kurių tokia informacija teikiama?
  - Ar pamatinis sprendimas dėl asmens duomenų apsaugos bus taikomas, kaip numatoma, pavyzdžiui, pasiūlymo 8 straipsnyje?
  - Jeigu ne, ar informacijos tvarkymas neprieštarauja pareigoms pagal direktyvą 95/46/EB?

28. Kadangi „prieinamumo principas“ yra labai plataus pobūdžio principas, reikia aiškiai ir tiksliai apibūdinti, kokie duomenys turi būti laikomi prieinamais. Todėl EDAPP rekomenduoja:

- Aiškiau apibūdinti taikymo sritį;
- Pirma galimybė — apriboti prieinamumo principo taikymo sritį iki informacijos, kurią kontroliuoja kompetentingos institucijos;
- Antra galimybė (jei taikymo sritis būtų platesnė) — užtikrinti pakankamas asmens duomenų apsaugos garantijas. Reikia atsižvelgti į šios nuomonės 27 punkte išdėstytus klausimus.

### Kiti su taikymo sritimi susiję klausimai

29. Pagal pasiūlymo 2 straipsnio 1 dalį, pamatinis sprendimas taikomas informacijos tvarkymui iki baudžiamojo persekiojimo pradžios. Jo taikymo sritis yra siauresnė nei pasiūlymo dėl pamatinio sprendimo dėl asmens duomenų apsaugos, kuris visas taikomas teisminiam bendradarbiavimui baudžiamosiose bylose.

30. Tačiau EDAPP mano, kad šis apribojimas pats savaime neapriboja pasiūlymo taikymo srities iki policijos bendradarbiavimo. Taikymo sritis taip pat galėtų apimti bendradarbiavimą baudžiamosiose bylose, nes keliose valstybėse narėse teisminės institucijos taip pat turi kompetenciją kriminalinių tyrimų srityje, iki baudžiamojo persekiojimo pradžios. Tačiau tai, kad pasiūlymas grindžiamas tik ES sutarties 30 straipsnio 1 dalies b punktu, leidžia daryti išvadą, kad jis taikomas tik policijos bendradarbiavimui. Būtų naudinga gauti šio klausimo paaiškinimą.

31. Esamas pasiūlymas taikomas informacijos teikimui Europolui, o pasiūlymas dėl pamatinio sprendimo dėl asmens duomenų apsaugos neapima Europolo vykdomo asmens duomenų tvarkymo. EDAPP pataria apriboti keitimąsi informacija su Europolu tik Europolo tikslais, kaip nurodyta Europolo konvencijos 2 straipsnyje ir jos priede. Be to, reikia atsižvelgti į išsamias keitimosi duomenimis su Europolu taisykles, kurios jau išdėstytos keliuose Tarybos teisės aktuose.

### Naujų duomenų bazių su asmens duomenimis nebus

32. Esminis pasiūlymo aspektas yra tai, kad priėmus pasiūlymą nebus sukurta naujų duomenų bazių, kuriose būtų asmens

duomenų. Šiuo klausimu 2 straipsnio 2 dalis yra aiški: joje nėra jokių pareigų rinkti ir saugoti informaciją tik tam, kad ji būtų prieinama. Duomenų apsaugos atžvilgiu tai yra svarbus ir teigiamas pasiūlymo elementas. EDAPP primena savo nuomonę dėl pasiūlymo dėl direktyvos dėl duomenų, tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas, saugojimo<sup>(1)</sup>, kurioje EDAPP pabrėžė, kad teisinės pareigos pagal kurias sukuriama materialios duomenų bazės, kelia ypatingą pavojų duomenų subjektui *inter alia* todėl, kad yra neteisėto naudojimo rizika.

33. Tačiau:

— Svarbu užtikrinti, kad pasiūlymu nebus remiamas besąlyginis duomenų bazių sąveikumas, kuriam esant atsirastų sunkiai prižiūrimas duomenų bazių tinklas.

— Yra pirmiau išdėstyto aspekto išimtis: pasiūlymo 10 straipsnis, kuriame nurodoma, kad rodyklės duomenys yra prieinami internetu. Rodyklės duomenys gali apimti asmens duomenis ar bet kuriuo atveju gali būti nustatyta, kad tokių duomenų yra.

### Tiesioginė ir netiesioginė prieiga prie informacijos

34. Pasiūlyme numatyta tiesioginė ir netiesioginė prieiga prie informacijos. Pasiūlymo 9 straipsnyje numatyta tiesioginė internetinė prieiga prie duomenų bazėse esančios informacijos, prie kurių tiesioginę internetinę prieigą turi atitinkamos nacionalinės institucijos. 10 straipsnyje numatyta netiesioginė prieiga. Informacijos, kuri neprieinama internetu, rodyklės duomenys turi būti prieinami internetu lygiavertėms kitų valstybių narių kompetentingoms institucijoms ir Europolui. Jei institucija atlikusi paiešką rodyklės duomenyse randa atitikmenį, ji gali parengti informacijos prašymą ir išsiųsti jį paskirtajai institucijai, kad gautų informaciją, rastą pasitelkus rodyklės duomenis.

35. Jei yra tiesioginė prieiga, naujos duomenų bazės nesukuriamos, tačiau reikia, kad valstybių narių lygiavertėms kompetentingų sistemų duomenų bazės sąveikautų. Be to, bus būtina įdiegti naują jau esančių duomenų bazių naudojimo būdą suteikiant visoms valstybių narių kompetentingoms institucijoms galimybes, kurias iki dabar turėjo tik nacionalinės kompetentingos institucijos. Tiesioginė prieiga reiškia, kad daugiau asmenų turės prieigą prie duomenų bazės, todėl bus didesnė piktnaudžiavimo rizika.

<sup>(1)</sup> 2005 m. rugsėjo 26 d. nuomonė dėl Europos Parlamento ir Tarybos direktyvos dėl duomenų, tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas, saugojimo ir iš dalies keičiančios Direktyvą 2002/58/EB (KOM (2005) 438 galutinis).



36. Jei kitos valstybės narės kompetentinga institucija tiesiogiai pasinaudoja duomenų baze, kilmės valstybės narės paskirtosios institucijos nekontroliuoja tokios prieigos ir tolesnio duomenų naudojimo. Pasiūlyme numatytos tiesioginės prieigos pasekmės turi būti tinkamai išnagrinėtos, nes:

- Atrodo, kad tiesioginė prieiga panaikina paskirtųjų institucijų įgaliojimus atsisakyti teikti informaciją (pagal 14 straipsnį);
- Esant tiesioginei prieigai, kyla klausimas dėl duomenų tikslumo ir atnaujinimo po to, kai jais buvo pasinaudota. Kaip kilmės valstybės narės paskirtoji institucija gali užtikrinti, kad duomenys būtų atnaujinami?
- Ne tik paskirtoji institucija daugiau negalės vykdyti visų pareigų pagal duomenų apsaugos įstatymus, bet ir kilmės valstybės narės nacionalinė duomenų apsaugos institucija negalės prižiūrėti, kaip vykdomos pareigos, nes jai truks kompetencijos kitų valstybių narių teisėsaugos institucijų atžvilgiu.
- Šios problemos vyrauja dar labiau, jei duomenų bazėmis pasinaudoja paskirtosios institucijos ir paskirtosios šalys, kurios nėra teisėsaugos institucijos (žr. šios nuomonės 25-28 punktus).

Ši tiesioginės prieigos pasekmė yra svarbi priežastis, dėl kurios esamo pasiūlymo priėmimas turėtų priklausyti nuo to, ar bus priimtas pamatinis sprendimas dėl asmens duomenų apsaugos. Lieka viena problema: neaišku, koku būdu paskirtosios institucijos galėtų atsisakyti teikti informaciją pagal 14 straipsnį.

37. Netiesioginė prieiga, kai naudojantis rodyklės duomenimis gaunama informacija pagal „rasta-nerasta“ sistemą, nėra naujiena. Tai yra funkcionuojančių Europos plataus masto informacinių sistemų, pavyzdžiui, Šengeno informacinės sistemos, pagrindas. Rodyklės duomenų sistemos nustatymo privalumas yra tai, kad kilmės valstybės narės galės kontroliuoti keitimąsi policijos registruose esančia informacija. Jei prašančioji institucija atlikusi paiešką rodyklės duomenyse randą atitikmenį, ji gali parengti informacijos prašymą dėl atitinkamo duomenų subjekto. Šį prašymą gali tinkamai įvertinti institucija, į kurią kreipiamasi.

38. Tačiau reikia atlikti išsamią analizę, nes tose srityse, kuriose tokios sistemos iki šiol nėra (išskyrus Europos plataus masto informacines sistemas), įdiegus rodyklės duomenų sistemą atsirastų naujų pavojų duomenų subjektui. EDAPP pabrėžia, kad, nors rodyklės duomenyse nėra daug infor-

macijos apie duomenų subjektą, atlikus paiešką rodyklės duomenyse gali būti gauti labai slapti rezultatai. Pavyzdžiui, gali paaiškėti, kad asmuo yra įtrauktas į su nusikaltimais susijusį policijos registrą.

39. Todėl yra ypač svarbu, kad Europos įstatymų leidėjas numatytų pakankamas taisykles, susijusias bent su rodyklės duomenų sukūrimu, reglamentuojančias rodyklės duomenų registravimo sistemų valdymą ir tinkamą prieigos prie rodyklės duomenų organizavimą. EDAPP mano, kad pasiūlymas nėra tinkamas dėl šių aspektų. Šiuo metu EDAPP pateikia tris pastabas:

- Rodyklės duomenų sąvokos apibrėžimas yra neaiškus. Neaišku, ar rodyklės duomenys bus meta-duomenys, reikšminiai žodžiai ar ir viena, ir kita? Rodyklės duomenų sąvoka turi būti paaiškinta, nes tai turi tiesioginę įtaką duomenų apsaugos lygiui ir reikiamoms apsaugos priemonėms.
- Pasiūlyme turėtų būti paaiškintas nacionalinių ryšių palaikymo centrų vaidmuo rodyklės duomenų atžvilgiu. Gali būti būtina, kad dalyvautų nacionaliniai ryšių palaikymo centrai, ypač tais atvejais, kai interpretuojant rodyklės duomenis reikia specialių žinių, pavyzdžiui, nustatant galimą pirštų atspaudų atitikimą.
- Pasiūlyme numatyta, kad rodyklės duomenų sukūrimo taisyklės turi būti nustatytos įgyvendinimą reglamentuojančiuose teisės aktuose pagal 19 straipsnyje numatytą komitologijos procedūrą. Nors gali būti reikalingos įgyvendinimo taisyklės, pagrindinės rodyklės duomenų sukūrimo taisyklės turi būti įtrauktos į pamatinį sprendimą.

### Išankstinis teisminių institucijų leidimas

40. Keičiantis informacija valstybėms narėms nedraudžiama prašyti išankstinio teisminių institucijų leidimo perduoti informaciją prašančiai institucijai, jei šią informaciją valstybėje, į kurią kreipiamasi, kontroliuoja teisminės institucijos. Tai yra svarbu, nes pagal policijos įgaliojimų keistis asmens duomenimis tyrimą<sup>(1)</sup> ne visose valstybėse narėse policija gali savarankiškai naudotis tokiais duomenimis. EDAPP mano, kad prieinamumo principas neturi riboti pareigos pagal nacionalinę teisę gauti išankstinį leidimą dėl informacijos, ar bent turi būti nustatytos visose valstybėse narėse taikomos konkrečios taisyklės, pagal kurias dėl tam tikrų kategorijų duomenų reikėtų gauti išankstinį leidimą.

<sup>(1)</sup> Atsakymai į klausimą dėl pamatinio sprendimo dėl keitimosi informacija ir žvalgybos informacija, ypač informacija apie sunkius nusikaltimus, įskaitant teroro aktus, tarp Europos Sąjungos valstybių narių teisėsaugos institucijų supaprastinimo (Tarybos dokumentas Nr. 5815/1/05).

41. Ši pareiga turėtų būti aiškinama kartu su pasiūlymo dėl pamatinio sprendimo dėl asmens duomenų apsaugos 11 straipsnio 2 dalimi, kurioje taip pat numatyta, kad perduodančioji valstybė narė gali turėti įtakos tam, kaip duomenys bus toliau naudojami valstybėje narėje, kuriai jie buvo perduoti. EDAPP pabrėžia šio principo svarbą, nes jis reikalingas užtikrinti tai, kad prieinamumas nebūtų naudojamas apeiti tolesnio asmens duomenų naudojimo apribojimus nustatančius nacionalinės teisės aktus.

### Galutinė pastaba

42. Šiems elementams reikalingi aukšti duomenų apsaugos standartai. Ypatingas dėmesys turėtų būti skiriamas tam, kad būtų užtikrintas tikslo ribojimo ir tolesnio naudojimo principų įgyvendinimas bei informacijos, kuria pasinaudota, tikslumas ir patikimumas (žr. EDAPP nuomonės dėl pamatinio sprendimo dėl asmens duomenų apsaugos IV dalies 2 ir 6 punktus).

## V. KITI POŽIŪRIAI

### Švedijos pasiūlymas

43. Švedijos pasiūlymas nėra ribojamas konkrečiomis informacijos rūšimis, o apima visą informaciją ir *žvalgybinę informaciją*, net jei tokių rūšių informaciją saugo ne kompetentingos teisėsaugos institucijos. Pasiūlyme bendradarbiavimas reglamentuojamas išsamiau, nustatant terminus pateikti atsakymus į informacijos prašymus ir panaikinant diskriminacinio pobūdžio skirtumus tarp keitimosi informacija valstybės viduje ir tarpvalstybinio keitimosi informacija. Jame nenumatytos papildomos priemonės, užtikrinančios veiksmingą prieigą prie informacijos. Suprantama, kad dėl šios priežasties Komisijai Švedijos siūlymas netiko kaip pakankamas prieinamumą reglamentuojantis teisės aktas <sup>(1)</sup>.

44. Požiūrio, kurio grindžiamas Švedijos pasiūlymas, bendro pobūdžio pasekmės duomenų apsaugos srityje yra tokios:

— naudinga tai, kad pasiūlymo ribos yra griežtos — tik egzistuojančių duomenų tvarkymas — ir nebūtų kuriamos jokios naujos duomenų bazės, net ir „rodyklės duomenys“;

— tačiau tai, kad nėra „rodyklės duomenų“, savaime nėra teigiamas bruožas. Jei rodyklės duomenų būtų tinkamai apsaugoti, jie padėtų ieškoti slapto pobūdžio duomenų tikslingiau ir todėl mažiau pažeidžiant privatumą. Tokie duomenys taip pat padėtų geriau rūšiuoti prašymus ir geriau prižiūrėti.

— Bet kuriuo atveju, dėl tokio pasiūlymo padidėtų tarpvalstybinis keitimasis asmens duomenimis, keliant pavojų asmens duomenų apsaugai, *inter alia* todėl, kad

būtų neigiamai paveikta valstybių narių kompetencija visiškai kontroliuoti subjektą, kuris keičiasi duomenimis. Toks pasiūlymas neturėtų būti priimtas nepriėmus pamatinio sprendimo dėl asmens duomenų apsaugos.

## Priemo konvencija

45. Priemo konvencijoje yra kitoks požiūris į prieinamumo principo įgyvendinimą. Priemo konvencijoje naudojamas laipsniškas požiūris, o šiame pasiūlyme dėl pamatinio sprendimo požiūris yra bendro pobūdžio — nenumatytos konkrečios taisyklės, kaip keistis tam tikrų rūšių informacija, o numatytos bendros II priede nurodytai visų rūšių informacijai taikomos taisyklės (žr. šios nuomonės 21–28 punktus).

46. Toks požiūris kartais vadinamas „atskiroms duomenų rūšims taikomu požiūriu“. Jis taikomas konkrečioms informacijos rūšims (DNR, duomenims apie pirštų atspaudus ir duomenims apie transporto priemonių registravimą) ir pagal jį numatoma pareiga atsižvelgti į ypatingą duomenų pobūdį. Konvencijoje numatyta pareiga užvesti ir saugoti DNR analizės duomenų bylas nusikaltimų tyrimo tikslais. Toks pats požiūris taikomas duomenims apie pirštų atspaudus. Transporto priemonių registravimo duomenų atveju tiesioginė prieiga turi būti suteikta kitų valstybių narių nacionaliniams ryšių palaikymo centrams.

47. Išnagrinėjus Priemo konvencijoje taikomą požiūrį galima pateikti trijų rūšių pastabas.

48. Pirma, akivaizdu, kad EDAPP nepritaria tvarkai, kurią taikant atsirado ši konvencija, nes nebuvo naudojama Europos Sąjungos institucinė sistema ir todėl rengiant konvenciją Komisija iš esmės nedalyvavo. Be to, tai reiškia, kad nebuvo Europos Parlamento vykdomos demokratinės kontrolės ir nėra Teisingumo Teismo teisminės kontrolės, todėl yra mažiau garantijų, kad visų (viešųjų) interesų pusiavsvyra yra tolygi. Tai apima ir duomenų apsaugos klausimą. Kitaip tariant, Europos Sąjungos institucijos neturi galimybės prieš sukuriant sistemą įvertinti pasirinktos politikos poveikį asmens duomenų apsaugai.

49. Antra, akivaizdu, kad kai kurie Priemo konvencijos elementai yra labiau pažeidžiantys duomenų subjekto privatumą nei pasiūlymas dėl pamatinio sprendimo dėl prieinamumo. Konvencijos pasekmė yra tai, kad bus sukurtos naujos duomenų bazės, o tai savo ruožtu sukelia pavojų asmens duomenų apsaugai. Turi būti įrodyta, kad tokias naujas duomenų sukurti yra būtina ir kad tai yra proporcinga priemonė. Turi būti numatytos pakankamos asmens duomenų apsaugos priemonės.

<sup>(1)</sup> Žr. pasiūlymo dėl Tarybos pamatinio sprendimo dėl keitimosi informacija pagal prieinamumo principą priedą – 2005 m. spalio 12 d. Komisijos tarnybų darbo dokumentą SEC 2005 (1270).

### „Atskiroms duomenų rūšims taikomas požiūris“

50. Trečia, kaip minėta, konvencijoje naudojamas „atskiroms duomenų rūšims taikomas požiūris“. Šioje nuomonėje EDAPP pirmiau paminėjo sunkumus ir neaiškumus, susijusius su aplinka, kurioje turi veikti prieinamumo principas. EDAPP mano, kad tokiomis aplinkybėmis geriau nesukurti sistemos duomenų sričiai, bet pradėti taikyti atsargesnį požiūrį — nagrinėti po vieną duomenų rūšį, ir stebėti, kaip prieinamumo principas gali veiksmingai padėti teisėsaugai, o taip pat — kokie konkretūs pavojai kyla duomenų apsaugos srityje. Naudojantis tokia patirtimi sistemą būtų galima išplėsti ir iki kitų rūšių duomenų ir (arba) ją pakeisti siekiant, kad ji būtų veiksmingesnė.
51. Toks „atskiroms duomenų rūšims taikomas požiūris“ taip pat geriau atitiktų prieinamumo principo reikalavimus. EDAPP mano, kad poreikis tarpvalstybiniu lygiu teisėsaugos tikslais geriau keistis informacija galėtų pagrįsti tai, kad ES lygiu būtų priimtas teisės aktas, tačiau tam, kad šis teisės aktas būtų proporcingas, jis turėtų būti tinkamas tikslui pasiekti, o tai gali būti tiksliau nustatyta tik po tam tikro praktinės patirties laikotarpio. Be to, toks teisės aktas neturėtų daryti neproporcingos žalos duomenų subjektui. Keitimasis informacija neturėtų būti susijęs su daugiau duomenų rūšių nei būtina, turėtų būti numatyta anoniminio keitimosi duomenimis galimybė, ir informacija turėtų būti keičiamasi laikantis griežtų duomenų apsaugos sąlygų.
52. Be to, EDAPP remiamas atsargesnis požiūris galėtų apimti ir tai, kad prieinamumo principas būtų įgyvendinamas numatant tik netiesioginę prieigą naudojant rodyklės duomenis — tai galėtų būti „atskiroms duomenų rūšims taikomo požiūrio“ papildymas. EDAPP nurodo, kad šis klausimas turėtų būti apsvaistytas tolesniame teisėkūros procese.

### VI. KOKIE DUOMENYS?

53. II priede vardijamos informacijos, kurią galima gauti pagal siūlomą pamatinį sprendimą, rūšys. Visos šešios priede nurodytos informacijos rūšys dažniausiai yra asmens duomenys, nes jie turi ryšį su asmeniu, kurio tapatybė nustatyta arba gali būti nustatyta.
54. Pagal pasiūlymo 3 straipsnio g punktą rodyklės duomenys — „tai duomenys, kurių tikslas yra nustatyti informaciją ir kuriuos galima surasti atlikus įprastinę paiešką, kad galima

būtų įsitikinti ar informacija yra prieinama“. „Požiūryje į prieinamumo principo įgyvendinimą“<sup>(1)</sup> rodyklės duomenimis laikomi šie duomenys:

- atitinkamų asmenų tapatybė;
- atitinkamų daiktų (automobilių, dokumentų) identifikacijos numeris;
- pirštų atspaudai ir skaitmeninės nuotraukos.

Kita duomenų rūšis, kuri galėtų būti rodyklės duomenimis, yra DNR charakteristikos. Šis rodyklės duomenų sąrašas rodo, kad rodyklės duomenys gali apimti asmens duomenis ir todėl reikia tinkamos apsaugos.

55. EDAPP atkreipia ypatingą dėmesį į klausimą dėl DNR charakteristikų. DNR analizė, kaip įrodyta, yra vertinga tiriant nusikaltimus, todėl veiksmingas keitimasis DNR duomenimis gali būti esminis kovojant su nusikalstamumu. Tačiau reikia, kad DNR duomenų koncepcija būtų aiškiai apibrėžta ir kad būtų tinkamai atsižvelgta į konkrečias tokių duomenų savybes. Iš tiesų, duomenų apsaugos požiūriu, tarp DNR pavyzdžių ir DNR charakteristikų yra esminis skirtumas.
56. DNR pavyzdžiai (dažnai surinkti ir saugomi teisėsaugos institucijų) turi būti laikomi ypatingai slaptais, nes yra didesnė tikimybė, kad juose bus visas DNR „paveikslas“. Juose gali būti informacijos apie asmens genetines savybes ir sveikatos būklę, kurios gali reikėti visiškai kitiems tikslams, pavyzdžiui, teikti medicinos konsultacijas asmenims ar jaunoms poroms.
57. Tuo tarpu DNR charakteristikose yra tik dalinė DNR informacija, paimta iš DNR pavyzdžio: jos gali būti naudojamos nustatyti asmens tapatybę, tačiau jos iš esmės neatskleidžia genetinių asmens savybių. Nepaisant to, mokslo pažanga gali padidinti informacijos, kurią galima gauti iš DNR charakteristikų, kiekį: tai, kas tam tikru metu laikoma „nekalta“ DNR charakteristika, vėliau gali atskleisti daug daugiau informacijos nei tikėtasi ir reikia, ypač su asmens genetinėmis savybėmis susijusios informacijos. Todėl informacija, kurią galima atskleisti iš DNR charakteristikų, turi būti laikoma dinamiška.
58. Atsižvelgdamas į tai, EDAPP pastebi, kad Priumo konvencijoje ir Komisijos pasiūlyme numatytas teisėsaugos institucijų keitimasis DNR informacija, tačiau yra esminių skirtumų, kaip taip padaryta.

<sup>(1)</sup> 2005 m. balandžio 5 d. pirmininkaujančios valstybės narės dokumentas Tarybai (dok. Nr. 7641/05).

59. EDAPP palankiai vertina tai, kad Komisijos pasiūlyme nenumatyta pareiga rinkti DNR duomenis ir kad keistis galima tik DNR charakteristikomis. II priede DNR charakteristikos apibrėžiamos naudojant pradinį bendrą DNR žymenų sąrašą, valstybėse narėse naudojamą atliekant DNR analizę teismo ekspertizės tikslais. Šis sąrašas, grindžiamas septyniais DNR žymenimis pagal Europos standartinių rinkinių, apibrėžtą 2001 m. liepos 25 d. Tarybos rezoliucijoje dėl keitimosi DNR tyrimų rezultatais <sup>(1)</sup>, užtikrina, kad DNR charakteristikose jas paėmus nebus jokios informacijos apie konkrečias paveldimas savybes.
60. EDAPP pabrėžia, kad šioje Tarybos rezoliucijoje nustatytos kai kurios labai svarbios apsaugos priemonės, kurios yra ypač susijusios su dinamišku DNR charakteristikų pobūdžiu. Iš tiesų, rezoliucijos III skirsnyje nurodžius, kad keitimasis DNR analizės rezultatais ribojamas „chromosomų zonomis [...] apie kurias nežinoma, kad jos gali suteikti informacijos apie konkrečias paveldimas savybes“, toliau rekomenduojama valstybėms narėms nenaudoti tokių DNR žymenų, kurie dėl mokslo pokyčių gali suteikti informacijos apie konkrečias paveldimas savybes.
61. Priemo konvencijoje taikomas kitoks požiūris, nes joje Susitariančios šalys įpareigojamos užvesti ir saugoti DNR analizės duomenų bylas nusikaltimų tyrimo tikslais. Todėl joje numatoma kurti naujas DNR duomenų bazes ir intensyviau rinkti DNR duomenis. Be to, yra neaišku, kokių rūšių duomenys patenka į „DNR analizės duomenų bylas“, o konvencijoje neatsižvelgiama į dinamišką DNR charakteristikų evoliuciją.
62. EDAPP nurodo, kad bet kuriame teisės akte dėl keitimosi DNR duomenimis:
- turėtų būti aiškiai apribota ir apibrėžta informacijos apie DNR, kuria galima keistis, rūšis (taip pat atsižvelgiant į esminį skirtumą tarp DNR pavyzdžių ir DNR charakteristikų);
  - turėtų būti numatyti bendri techniniai standartai, siekiant išvengti, kad dėl skirtingos valstybių narių praktikos teismo ekspertizės DNR duomenų bazių naudojimo srityje kiltų sunkumų ir netikslių rezultatų, kai keičiamasi duomenimis;
  - turėtų būti numatytos tinkamos teisiškai įpareigojančios apsaugos priemonės, skirtos tam, kad būtų išvengta, jog mokslo pokyčiai iš DNR charakteristikų leistų gauti asmens duomenis, kurie yra ne tik slapti, bet ir nebūtini tam tikslui, kuriam jie renkami.
63. Atsižvelgdamas į tai, EDAPP šioje nuomonėje patvirtina ir pakartoja pastabas, pateiktas jo nuomonėje dėl pamatinio sprendimo dėl asmens duomenų apsaugos (80 punktas). Minėtoje nuomonėje EDAPP nurodė, kad DNR duomenų atveju turėtų būti numatytos konkrečios apsaugos priemonės, siekiant užtikrinti, kad: prieinama informacija gali būti naudojama tik nustatyti asmenų tapatybę nusikaltimų prevencijos, nustatymo ir tyrimo tikslais; būtų atidžiai atsižvelgta į DNR charakteristikų tikslumo lygį, o duomenų subjektas jį galėtų užginčyti lengvai prieinamomis priemonėmis; būtų visiškai užtikrinta pagarba asmenų orumui <sup>(2)</sup>.
64. Šie svarstymai leidžia daryti išvadą, kad teisės aktai, kuriuose reglamentuojamos DNR duomenų bylos ir keitimasis duomenimis iš jų, turėtų būti priimami tik atlikus poveikio įvertinimą, kuriame būtų tinkamai įvertinta nauda ir pavojai. EDAPP rekomenduoja, kad tokiuose teisės aktuose būtų numatytos pareigos po jų įsigaliojimo reguliariai atlikti įvertinimą.
65. Galiausiai, II priede nurodytos kitos informacijos, kuria gali būti keičiamasi, rūšys. Priedas apima informaciją, kuri kyla iš privačių šalių, nes telefonų numeriai ir kiti ryšių duomenys, taip pat srauto duomenys, paprastai kyla iš telefono operatorių. Aiškinamajame memorandume patvirtinama, kad valstybės narės turi pareigą užtikrinti, jog institucijų ar tam tikslui paskirtų privačių šalių valdoma teisėsaugai reikalinga informacija būtų dalijamasi su atitinkamomis kitų valstybių narių institucijomis ir Europolu. Kadangi pasiūlymas taikomas iš privačių šalių kilusiems duomenims, EDAPP mano, kad taikomuose teisės aktuose turėtų būti numatytos papildomos apsaugos priemonės, skirtos apsaugoti duomenų subjektą, kad būtų užtikrintas duomenų tikslumas.

## VII. DUOMENŲ APSAUGOS PRINCIPAI

66. Asmens duomenų apsaugos taisyklės siūlomame Tarybos pamatiniame sprendime konkrečiai nenumatytos, o kituose teisės aktuose, pavyzdžiui, Priemo konvencijoje arba Švedijos pasiūlyme, yra kelios konkrečios nuostatos dėl asmens duomenų apsaugos. Tai, kad pasiūlyme dėl prieinamumo nėra specialių asmens duomenų apsaugos taisyklių, gali būti priimtina tik tuo atveju, jeigu pasiūlyme dėl pamatinio sprendimo dėl duomenų apsaugos pagal trečiąją ramstį esančios bendrosios taisyklės bus taikomos visos ir užtikrins pakankamą apsaugą. Be to, specialiuose teisės aktuose, pavyzdžiui, Švedijos pasiūlyme ar Priemo konvencijoje, numatytos asmens duomenų apsaugos taisyklės neturėtų nustatyti žemesnio apsaugos lygio nei tas, kurį nustato bendro pobūdžio sistema. EDAPP rekomenduoja įrašyti specialią nuostatą dėl galimos skirtingų duomenų apsaugos taisyklių kolizijos.

<sup>(2)</sup> Dėl to paties klausimo žr. taip pat Europos Tarybos 2005 m. vasario mėn. „Pažangos ataskaitą dėl 108 konvencijos dėl asmens biometrinių duomenų rinkimo ir apdorojimo principų taikymo“.

<sup>(1)</sup> OL C 187, p. 1.



67. Šioje vietoje EDAPP dar kartą pabrėžia, prisimindamas savo nuomonę dėl pamatinio sprendimo dėl asmens duomenų apsaugos, kad yra svarbu turėti galiojančias nuoseklias ir išsamias duomenų apsaugos taisykles, taikomas bet kokiam duomenų tvarkymui teisėsaugos institucijų bendradarbiavimo srityje. Toliau, EDAPP pakartoja kitus minėtoje nuomonėje išdėstytus aspektus. Šiame punkte pabrėžiami šie klausimai duomenų apsaugos srityje:

— Teisėtas asmens duomenų tvarkymas. EDAPP remia požiūrį, kad informacija gali būti prieinama tik tuo atveju, jeigu ji yra gauta teisėtai (kaip nurodyta 2 straipsnio 2 dalyje dėl prievartos priemonėmis surinktos informacijos). Teisėtas asmens duomenų tvarkymas taip pat užtikrintų, kad teismo procese taip pat tinkamai būtų galima naudoti informaciją, kuri yra prieinama ir kuria pasikeista. Iš tiesų, nors informacijos tvarkymas prasidėjęs baudžiamajam procesui nepatenka į siūlomo teisės akto taikymo sritį, tikėtina, kad informacija, kuria prieš tai pasikeitė teisėsaugos institucijos, bus naudojama teismo procese.

— Asmens duomenų kokybė yra ypač svarbi, nes prieinamumo principas leidžia keistis informacija teisėsaugos institucijoms, kurios veikia kitame kontekste, nei duomenys buvo surinkti. Šios institucijos netgi turi tiesioginės prieigos prie kitų valstybių narių duomenų bazių galimybę. Asmens duomenų kokybė gali būti užtikrinta tik tuo atveju, jeigu jų tikslumas yra reguliariai ir tinkamai tikrinamas, jei informacija skirstoma pagal atitinkamų asmenų kategorijas (nukentėję asmenys, įtariamieji, liudytojai ir t. t.) ir jeigu prareikęs nurodomas tikslumo laipsnis (žr. EDAPP nuomonės dėl asmens duomenų apsaugos IV dalies 6 p.).

Šie aspektai yra dar kartą įrodo, kad duomenų apsaugos taisyklės, ypač su tikslumu susijusios taisyklės, turėtų būti taikomos visoms duomenų tvarkymo rūšims, įskaitant valstybės viduje vykdomą tvarkymą. Priešingu atveju asmens duomenys, kuriais naudojamosi tiesiogiai, galėtų būti neteisingi, pasenę ir tokiu būdu pažeisti duomenų subjekto teises ir neigiamai paveikti tyrimų veiksmingumą.

— Tikslo ribojimas. Pagal prieinamumo principą, prieigą prie asmens duomenų gali turėti atitinkamos kitų valstybių narių institucijos. Tačiau valstybių teisėsaugos institucijų kompetencijos gali būti labai skirtingos. Todėl yra svarbu užtikrinti, kad būtų laikomasi tikslo ribojimo pagrindinio principo, nepaisant skirtingos įvairių teisėsaugos institucijų, kurios keičiasi duomenimis, kompetencijų apimties. Informacija, kurią surenka ir tvarko tam tikra institucija turėdama konkretų tikslą, negali būti naudojama kitam tikslui tik

todėl, kad gaunančiosios institucijos kompetencija yra kitokia ar galbūt platesnė.

Todėl EDAPP palankiai vertima siūlomo pamatinio sprendimo 7 straipsnį, kuris turi būti laikomas specialia norma siūlomame pamatiniame sprendime dėl asmens duomenų apsaugos numatytų bendrųjų taisyklių atžvilgiu. Be to, EDAPP atkreipia dėmesį, kad skirtingų institucijų atitikties įvertinimas (kuris dabartiniame pasiūlyme yra numatytas pagal komitologijos procedūrą) turėtų būti atliekamas atsargiai ir tinkamai laikantis tikslo ribojimo principo.

— Informacijos, kuria pasikeista, saugojimo terminai taip pat turi būti nagrinėjami atsižvelgiant į tikslo ribojimo principą: informacija, kuria pasinaudojama ar pasikeičiama konkrečiam tikslui, turi būti kuo greičiau panaikinta, kai ji tampa tam tikslui nereikalinga. Tokiu būdu galima būtų išvengti nebūtino duomenų bazių dubliavimo, tuo pačiu metu vėl sudarant kompetentingoms institucijoms prieigos prie (atnaujintos) informacijos galimybę, jei to prireiktų kitam teisėtam tikslui.

— Pagal prieinamumo principą perduotos informacijos registravimas. Registruojama turėtų būti abiejose šalyse — valstybėje narėje, į kurią kreipiamasi, ir prašančiojoje valstybėje narėje. Turėtų būti saugomi ne tik keitimosi registrai, bet ir prieigos registrai (žr. EDAPP nuomonės dėl asmens duomenų apsaugos 133 p.), taip pat siekiant užtikrinti ir tai, kad nacionalinės kompetentingos institucijos viena kita pasitikėtų bei visiškai neprarastų prieinamos informacijos kontrolės. Kadangi yra būtina, kad informaciją būtų galima atsekti, turi būti galimybė informaciją atnaujinti ir (arba) pataisyti.

— Duomenų subjekto teisės. Dėl ES teisėsaugos institucijų keitimosi informacija sistemų daugėja situacijų, kai asmens duomenis (laikiniai) tuo pačiu metu tvarko skirtingų valstybių narių kompetentingos institucijos. Viena vertus tai reiškia, kad turėtų būti nustatyti bendri ES standartai dėl duomenų subjekto teisių, o kita vertus, duomenų subjektai turėtų turėti galimybę įgyvendinti savo teises tiek, kiek tai leidžia duomenų apsaugos taisyklės pagal trečiąją ramstį, institucijų, kurios suteikia prieigą prie duomenų, ir institucijų, kurios tuos duomenis tvarko, atžvilgiu.

— Priežiūra. EDAPP atkreipia dėmesį, kad gali būti atvejų, kad daugiau nei viena nacionalinė priežiūros institucija turėtų kompetenciją stebėti asmens duomenų apdorojimą, kuris būtų atliekamas pagal dabartinius pasiūlymus. Todėl, jei būtų numatyta tiesioginė internetinė prieiga prie teisėsaugos informacijos, reikia numatyti sustiprintą atitinkamų nacionalinių duomenų apsaugos institucijų atliekamą priežiūrą ir koordinavimą.

## VIII. IŠVADOS

**Bendro pobūdžio išvados apie prieinamumo principą**

68. EDAPP naudojasi proga šioje nuomonėje pateikti kai kuriuos bendro pobūdžio ir svarbesnius požiūrio aspektus apie keitimąsi teisės saugos informacija ir apie galimus šio klausimo reglamentavimo būdus. Su EDAPP bus galima konsultuotis ir vėliau, po to, kai įvyks atitinkami teisėkūros procedūros pokyčiai dėl šio pasiūlymo, taip pat bus galima konsultuotis ir dėl kitų susijusių pasiūlymų.
69. EDAPP mano, kad prieinamumo principas turėtų būti įdiegtas į privalomą teisės aktą atsargiau ir labiau laipsniškai, po vieną duomenų rūšį, ir kad reikia stebėti, kaip prieinamumo principas gali veiksmingai padėti teisės saugai, o taip pat — kokie konkretūs pavojai kyla duomenų apsaugos srityje. Naudojant atsargesnį požiūrį, prieinamumo principą būtų galima pradėti įgyvendinti tik nustatant netiesioginę prieigą naudojant rodyklės duomenis. Naudojantis tokia patirtimi sistemą būtų galima išplėsti ir iki kitų rūšių duomenų ir (arba) ją pakeisti siekiant, kad ji būtų veiksmingesnė.
70. Bet koks teisės aktas, kuriuo įgyvendinamas prieinamumo principas, neturėtų būti priimamas prieš tai nepriėmus duomenų apsaugos esminių garantijų, kurios numatytos pasiūlyme dėl pamatinio sprendimo dėl asmens duomenų apsaugos.

**Rekomendacijos, skirtos pataisyti esamą pasiūlymą**

71. EDAPP rekomenduoja aiškiau apibūdinti prieinamumo principo taikymo sritį tokiais būdais:
- įrašyti aiškų ir tikslų duomenų, kurie laikomi prieinamais, sąvokos apibrėžimą;
  - pirma galimybė — apriboti prieinamumo principo taikymo sritį iki informacijos, kurią kontroliuoja kompetentingos institucijos;
  - antra galimybė (jei taikymo sritis būtų platesnė) — užtikrinti pakankamas asmens duomenų apsaugos priemones. Reikia atsižvelgti į šios nuomonės 27 punkte išdėstytus klausimus.
72. EDAPP pateikia šias pastabas dėl kitos valstybės narės kompetentingos institucijos tiesioginės prieigos prie duomenų bazių:
- ši problema turi būti tinkamai išspręsta, nes, tiesioginės prieigos atveju, kilmės valstybės narės paskirtosios institucijos nekontroliuoja prieigos prie duomenų ir tolesnio jų naudojimo;
  - pasiūlyme neturėtų būti numatomas besąlyginis duomenų bazių ryšys ir dėl to atsirandantis duomenų bazių tinklas, kurį bus sunku prižiūrėti.

73. Pamatiniame sprendime turėtų būti tikslesnių nuostatų, reglamentuojančių rodyklės duomenų sistemos parengimą. Būtent:

- pasiūlyme turi būti numatytos pakankamos taisyklės, susijusios bent su rodyklės duomenimis, reglamentuojančios rodyklės duomenų registravimo sistemų valdymą ir tinkamą prieigos prie rodyklės duomenų organizavimą;
- rodyklės duomenų sąvokos apibrėžimas turi būti aiškiau apibūdintas;
- pasiūlyme turėtų būti paaiškintas nacionalinių ryšių palaikymo centrų vaidmuo rodyklės duomenų atžvilgiu;
- į pamatinį sprendimą turi būti įtrauktos rodyklės duomenų sukūrimo pagrindinės taisyklės; jos neturėtų būti nustatytos įgyvendinimą reglamentuojančiuose teisės aktuose pagal komitologijos procedūrą.

74. EDAPP nurodo, kad tiek, kiek pasiūlyme numatytas keitimasis DNR duomenimis:

- turėtų būti aiškiai apribota ir apibrėžta informacijos apie DNR, kuria galima keistis, rūšis (taip pat atsižvelgiant į esminį skirtumą tarp DNR pavyzdžių ir DNR charakteristikų);
- turėtų būti numatyti bendri techniniai standartai, siekiant išvengti, kad dėl skirtingos valstybių narių praktikos teismo ekspertizės DNR duomenų bazių naudojimo srityje kiltų sunkumų ir netikslių rezultatų, kai keičiamasi duomenimis;
- turėtų būti numatytos tinkamos teisiškai įpareigojanti apsaugos priemonės, skirtos tam, kad būtų išvengta, jog mokslo pokyčiai iš DNR charakteristikų leistų gauti asmens duomenis, kurie yra ne tik slapti, bet ir nebūtini tam tikslui, kuriam jie renkami;
- pasiūlymas turėtų būti priimtas tik atlikus poveikio įvertinimą.

75. EDAPP pataria apriboti keitimąsi informacija su Europolu tik Europolo tikslais, kaip nurodyta Europolo konvencijos 2 straipsnyje ir jos priede.

Priimta Briuselyje, 2006 m. vasario 28 d.

Peter HUSTINX  
Europos duomenų apsaugos priežiūros  
pareigūnas