

Eiropas datu aizsardzības uzraudzītājs

Eiropas Datu aizsardzības uzraudzītāja atzinums par priekšlikumu Padomes Pamatlēmumam par informācijas apmaiņu saskaņā ar pieejamības principu (COM(2005) 490 galīgā redakcija)

(2006/C 116/04)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

ņemot vērā Eiropas Kopienas dibināšanas līgumu un jo īpaši tā 286. pantu;

ņemot vērā Eiropas Savienības Pamattiesību hartu un jo īpaši tās 8. pantu;

ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti;

ņemot vērā 28. panta 2. punktu Eiropas Parlamenta un Padomes Regulā (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās, kā arī par šādu datu brīvu apriti,

IR PIENĒMIS ŠO ATZINUMU.

I PROVIZORISKAS PIEZĪMES

1. Komisija 2005. gada 12. oktobra vēstulē Eiropas Datu aizsardzības uzraudzītājam (EDAU) ir nosūtījusi priekšlikumu Padomes Pamatlēmumam par informācijas apmaiņu saskaņā ar pieejamības principu. EDAU šo vēstuli saprot kā lūgumu sniegt padomu Kopienas iestādēm un struktūrām, kā paredzēts 28. panta 2. punktā Regulā 45/2001/EK. Pēc EDAU domām šis atzinums būtu jāpiemin pamatlēmuma preambulā.

2. Šā atzinuma būtība ir jāskata saistībā ar II nodaļu. Kā norādīts II nodaļā, nebūt nav acīmredzams, ka pašreizējais priekšlikums — vai arī priekšlikumā ierosinātā pieejamības pieeja — beigās būs par pamatu juridiska instrumenta pieņemšanai. Ievērojams skaits dalībvalstu atbalsta citas pieejas.

3. Tomēr ir acīmredzams, ka dalībvalstu darba kārtībā — gan Padomē, gan ārpus tās, kā arī Eiropas Parlamentā, — augsta prioritāte piešķirta jautājumam par tiesībaizsardzības informācijas pieejamību pāri iekšējām robežām — vai plašāk, par šādas informācijas apmaiņu.

4. Tāpat ir arī acīmredzams, ka šis jautājums ir ārkārtīgi būtisks no personas datu aizsardzības viedokļa, kā tas arī norādīts šajā atzinumā. EDAU atgādina, ka pašreizējo priekšlikumu Komisija iesniedza, to cieši saistot ar priekšlikumu Padomes Pamatlēmumam par to personas datu aizsardzību, kurus apstrādā saistībā ar policijas un tiesu sadarbību krimināllietās; par šo priekšlikumu EDAU sniedza atzinumu 2005. gada 19. decembrī.

5. EDAU izmantos šo iespēju, lai šajā atzinumā iekļautu dažas vispārējas un dažas būtiskas piezīmes saistībā ar tiesībaizsardzības informācijas apmaiņu un šā jautājuma reglamentācijas iespējām. Iesniedzot šo atzinumu, EDAU paredz nodrošināt, lai datu aizsardzības perspektīva būtu pienācīgi ņemta vērā turpmākajās pārrunās pa šo tematu.

6. EDAU vēlāk būs pieejams turpmākām konsultācijām pēc attiecīgiem jaunumiem likumdošanas procesā saistībā ar šo un citiem saistītiem priekšlikumiem.

II PRIEKŠLIKUMA KONTEKSTS

7. Pieejamības princips Hāgas programmā ir ieviests kā svarīgs jauns tiesību princips. Tā būtība ir šāda — informācijai, kas nepieciešama cīņā pret noziedzību, būtu jāšķērso ES iekšējās robežas bez jebkādiem šķēršļiem. Pašreizējā priekšlikuma mērķis ir īstenot šo principu ar saistošu juridisku instrumentu.

8. Gan ES sistēmā, gan ārpus tās likumdevēju iemīļots temats ir policijas informācijas apmaiņa starp dažādām valstīm. Nesen EDAU vērsa uzmanību uz šādām ierosmēm.

9. Pirmkārt, 2004. gada 4. jūnijā Zviedrija ierosināja Pamatlēmumu par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu. Attiecībā uz šo priekšlikumu Padome savā 2005. gada 1. decembra sanāksmē panāca vienošanos par vispārēju pieeju.
10. Otrkārt, 2005. gada 27. maijā septiņas dalībvalstis Prīmā (Vācija) parakstīja Konvenciju par pārrobežu sadarbības izvērsšanu, jo īpaši, apkarojot terorismu, pārrobežu noziedzību un nelegālu migrāciju. Tajā, *inter alia*, ieviesti pasākumi, lai uzlabotu informācijas apmaiņu ar DNS un pirkstu nospiedumiem. Konvencijai var pievienoties jebkura Eiropas Savienības dalībvalsts. Līgumslēdzēju pušu mērķis ir iekļaut konvencijas noteikumus Eiropas Savienības tiesiskajā regulējumā.
11. Treškārt, tiesībaizsardzības informācijas pieejamība pāri Eiropas Savienības iekšējām robežām tiks veicināta arī ar citiem juridiskiem instrumentiem, kā piemēram, priekšlikumiem saistībā ar otrās paaudzes Šengenas Informācijas sistēmu (SIS II), priekšlikumu par Vīzu informācijas sistēmas (VIS) pieejamību meklēšanai un priekšlikumu pamatlēmumam par informācijas, kas iegūta no sodāmības reģistra, apmaiņas organizāciju un saturu. Šajā sakarā būtu lietderīgi pieminēt arī Komisijas 2005. gada 25. novembrī publicēto Paziņojumu par Eiropas datubāzu lielāku efektivitāti, pastiprinātu darbaspēju un savstarpēju sinerģiju tieslietu un iekšlietu jomā.
12. Tā kā visas šīs ierosmes jau ir publicētas, pašreizējais priekšlikums pamatlēmumam par pieejamību nebūtu jāizskata atsevišķi, bet gan kopainā ar citām tiesībaizsardzības informācijas apmaiņas iespējām. Tas ir īpaši svarīgi tādēļ, ka pašreizējā tendence Padomē liecina, ka priekšroka tiek dota citām informācijas apmaiņas un pieejamības koncepcijas iespējām, nekā tai vispārējai iespējai, ko Komisija piedāvājusi pašreizējā priekšlikumā. Pašreizējo priekšlikuma tekstu Padome var pat arī nemaz neapspriest.
13. Turklāt šis priekšlikums ir cieši saistīts ar priekšlikumu pamatlēmumam par personas datu aizsardzību. Pašreizējais atzinums jāskata saistībā ar pilnīgāku atzinumu par minēto pamatlēmumu.
14. Savā atzinumā par priekšlikumu pamatlēmumam par personas datu aizsardzību EDAU uzsver, cik svarīga ir piemērota datu aizsardzība kā vēlamās juridiska instrumenta sekas pieejamības jomā. Pēc EDAU domām šādu juridisku instrumentu nedrīkstētu pieņemt bez nepieciešamiem datu aizsardzības pasākumiem.
15. EDAU ir tāds pats viedoklis attiecībā uz citu juridisku instrumentu pieņemšanu, kas atvieglotu tiesībaizsardzības informācijas plūsmu pāri Eiropas Savienības iekšējām robežām. Tādēļ EDAU pauž gandarījumu par to, ka Padome, kā arī Eiropas Parlaments ir piešķirusi prioritāti minētajam priekšlikumam pamatlēmumam par personas datu aizsardzību.

III PIEEJAMĪBAS PRINCIPA BŪTĪBA

16. Pēc būtības pieejamības princips ir vienkāršs. Informācijai, kas pieejama konkrētām iestādēm kādā dalībvalstī, jābūt pieejamai arī līdzvērtīgām iestādēm citās dalībvalstīs. Informācijas apmaiņai dalībvalstu iestāžu starpā jānotiek pēc iespējas ātri un vienkārši un, vēlams, izmantojot tiešu tiesiskās saistes pieeju.

17. Grūtības rada vide, kurā pieejamības princips jāīsteno:

- Neviendabīgas dalībvalstu policijas un tiesu iestāžu organizācijas, ar atšķirīgām pilnvaru nodalīšanas sistēmām.
- Ir iekļauta dažāda veida (jūtīga) informācija (piemēram, DNS vai pirkstu nospiedumi).
- Arī pašās dalībvalstīs ir atšķirīgi veidi, kā kompetentās iestādes piekļūst informācijai.
- Ir grūti nodrošināt, lai informācija, kas radusies citā dalībvalstī, tiktu pareizi saprasta, ņemot vērā valodu, tehnoloģisko sistēmu (savietojamības) un tiesu sistēmu atšķirības.
- Tā ir jāiekļauj pašreizējā plašajā tiesību normu tīklā, kas saistītas ar tiesībaizsardzības informācijas apmaiņu valstu starpā.

18. Neatkarīgi no šīs sarežģītās vides, ir vispārēji skaidrs, ka šis princips darboties pats par sevi nevar. Ir nepieciešami papildu pasākumi, lai nodrošinātu, ka informāciju var efektīvi atrast un tai piekļūt. Jebkurā gadījumā šiem pasākumiem ir jāatvieglo tiesībaizsardzības iestāžu centieni izziņāt, vai tiesībaizsardzības iestādes citās dalībvalstīs glabā noderīgu informāciju un kur šo noderīgo informāciju var atrast. Šādus papildu pasākumus varētu veidot interfeisi, kas sniedz tiešu piekļuvi visiem vai dažiem datiem, ko glabā citas dalībvalstis. Šajā sakarā priekšlikumā pamatlēmumam par pieejamību ierosināti "indeksu dati" — īpaši dati, kuriem var tieši piekļūt pāri robežām.

19. Kopumā pieejamības principam būtu jāatvieglo informācijas plūsma starp dalībvalstīm. Iekšējās robežas tiks likvidētas, un dalībvalstīm tā informācija, kas pieejama viņu policijas iestādēm, būs lielākā mērā jādara pieejama citām iestādēm. Dalībvalstis zaudē spēju kontrolēt informācijas plūsmu, kas ir par pamatu arī tam, ka tās vairs nevar paļauties uz savu valstu tiesību aktiem kā pietiekamu instrumentu, kas piemēroti aizsargā informāciju.
20. Tieši šā iemesla dēļ priekšlikumā īpaša uzmanībā jāpievērš personas datu aizsardzībai. Pirmkārt, informācija, kas parasti ir konfidenciāla un droši aizsargāta, ir jāsniedz citu dalībvalstu iestādēm. Otrkārt, lai sistēma darbotos, ir jānosaka indeksu dati un tie jādara pieejami iestādēm citās dalībvalstīs. Tādējādi šā principa īstenošana radīs vairāk datu, nekā tie ir pašreiz pieejami.

IV GALVENIE ELEMENTI

Pieejamības principa darbības joma

21. Pirmkārt, ir ārkārtīgi būtiski noteikt, kādiem informācijas veidiem pieejamības principu piemēros. Šā principa piemērošanas joma ir vispārīgi noteikta priekšlikuma 2. pantā saistībā ar 1. panta 1. punktu un 3. panta a) punktu. Principu piemēro informācijai, kas:
- eksistē;
 - ir minēta II pielikumā, kurā uzskaitīti seši informācijas veidi;
 - ir pieejama kompetentām iestādēm.
- Tie ir trīs galvenie principa darbības jomas elementi, kas minēti Komisijas priekšlikumā. Darbības joma ir sīkāk aplūkota 2. pantā. 2. panta 1. punktā pieejamības principa piemērošana ierobežota tikai līdz posmam, kas ir pirms kriminālvajāšanas uzsākšanas, savukārt 2. panta 2., 3. un 4. punktā paredzēti konkrētāki ierobežojumi.
22. Lai labāk saprastu priekšlikuma ietekmi, ir nepieciešama dziļāka trīs minēto būtiskāko elementu analīze. Pirmie divi elementi paši par sevi ir acīmredzami skaidri. "Informācijas, kas eksistē" definīcija ir izskatīta plašāk 2. panta 2. punktā, minot, ka pamatlēmums neuzliek nekādu pienākumu vākt un glabāt informāciju ar vienīgo mērķi darīt to pieejamu, savukārt II pielikuma sarakstu nevar interpretēt dažādi. Tieši trešais būtiskais elements — gan viens pats, gan kopā ar pirmajiem diviem — ir jāpaskaidro tuvāk.
23. Priekšlikumā nav noteikts, vai "pieejama informācija" ir tikai tā informācija, ko kompetentās iestādes jau ir pārbaudījušas, vai tā ir informācija, ko šīs iestādes iespējami var iegūt. Tomēr pēc EDAU domām varētu saprast, ka priekšlikumā domāti abi informācijas veidi.
24. Patiešām — kaut arī 2. panta 2. punktā, šķiet, minēta šaurāka darbības joma, nosakot, ka pamatlēmums "neuzliek nekādu pienākumu vākt un glabāt informāciju [...] ar vienīgo mērķi darīt to pieejamu", 3. panta a) punkts pieļauj plašāku interpretāciju, minot, ka "informācija" ir "informācija, kas eksistē un kas minēta II pielikumā".
25. II pielikumā minētas vismaz divas datu kategorijas, ko bieži vien kontrolē citas iestādes, nevis policija. Pirmā kategorija ir transportlīdzekļu reģistrācijas informācija. Daudzās dalībvalstīs tiesībsargāšanas iestādes datubāzes ar šādu informāciju nekontrolē, kaut arī šīs iestādes tām regulāri piekļūst. Vai šāda veida informācija būtu iekļaujama "pieejamās informācijas" darbības jomā, ko atbilstīgi 1. pantam nodrošina līdzvērtīgām kompetentām iestādēm citās dalībvalstīs? Otrā datu kategorija, kas norādīta II pielikumā un kas jāpiemin, ir telefona numuri un citi komunikāciju dati: vai šādus datus var uzskatīt par "pieejamiem" pat, ja tos nekontrolē kompetentas iestādes, bet gan privāti uzņēmumi?
26. Turklāt citos priekšlikuma noteikumos un jo īpaši 3. panta d) punktā un 4. panta 1. punkta c) apakšpunktā atbalstīts uzskats, ka "izraudzītās iestādes" un pat "izraudzītās puses" var kontrolēt informāciju, kas ir "pieejama" "kompetentajām iestādēm". Tāpat no priekšlikuma teksta izriet, ka "dalībvalsts kompetentā iestāde" ir iestāde, uz kuru attiecas ES Līguma 29. panta pirmais ievilkums, savukārt jebkura valsts iestāde var būt "izraudzītā iestāde".
27. Pēc EDAU domām pieejamības principa piemērošana informācijai, ko kontrolē izraudzītās iestādes un izraudzītās puses, ir saistīta ar šādiem jautājumiem:
- Vai 30. panta 1. punkta b) apakšpunktā ir nodrošināta pietiekama tiesiskā bāze, ņemot vērā, ka izraudzītām iestādēm un izraudzītām pusēm jābūt tām, kas dara informāciju pieejamu, turklāt no datubāzēm, kas neietilpst trešā pīlāra sistēmā?
 - Vai tiks piemērots pamatlēmums par personas datu aizsardzību, kā tas paredzēts, piemēram, priekšlikuma 8. pantā?
 - Ja nē, vai apstrāde ir saskaņā ar Direktīvas 95/46/EK uzliktajām saistībām?

28. Tāda plaša principa kā "pieejamības principa" īstenošanai ir nepieciešams skaidri un precīzi definēt tos datus, kas tiks uzskatīti par pieejamiem. Tādēļ EDAU ierosina:

— Precizēt darbības jomu.

— Kā pirmo iespēju — ierobežot pieejamības principa darbības jomu tikai ar informāciju, ko kontrolē kompetentas iestādes.

— Kā otru iespēju — ja darbības joma būs plašāka — nodrošināt pietiekamu personas datu aizsardzību. Jāņem vērā 27. punktā minētie jautājumi.

Citi jautājumi saistībā ar darbības jomu.

29. Saskaņā ar priekšlikuma 2. panta 1. punktu pamatlēmumu piemēro informācijas apstrādei, pirms uzsāk kriminālvajāšanu. Tā darbības joma ir ierobežotāka nekā priekšlikumā pamatlēmumam par personas datu aizsardzību, ko pilnībā piemēro tiesu sadarbībai krimināllietās.

30. Tomēr pēc EDAU domām šis ierobežojums pats par sevi neierobežo priekšlikuma darbības jomu tikai līdz policijas sadarbībai. Tajā varētu iekļaut arī tiesu sadarbību krimināllietās, tā kā vairākās dalībvalstīs tiesu iestādes ir tiesīgas veikt arī krimināllietu izmeklēšanu pirms tiek uzsākta kriminālvajāšana. Tomēr fakts, ka priekšlikums ir balstīts tikai uz LES 30. panta 1. punkta b) apakšpunktu, norāda, ka tas attiecas tikai uz policijas sadarbību. Šajā sakarā būtu nepieciešams precizējums.

31. Pašreizējais priekšlikums attiecas uz informācijas piegādi Eiropolam, savukārt priekšlikumā pamatlēmumam par personas datu aizsardzību nav iekļauti noteikumi par Eiropola veiktu personas datu apstrādi. EDAU aicina ierobežot informācijas apmaiņu ar Eiropolu tikai paša Eiropola vajadzībām, kā minēts Eiropola Konvencijas 2. pantā un tai pievienotajā pielikumā. Turklāt būtu jāņem vērā sīki izstrādātie noteikumi attiecībā uz datu apmaiņu ar Eiropolu, kas jau ir ietverti vairākos Padomes tiesību aktos.

Jaunu datubāzu ar personas datiem nebūs

32. Priekšlikuma pamatā ir nodoms neveidot jaunas personu datu datubāzes. Šajā sakarā 2. panta 2. punktā ir skaidri

noteikts: tas neuzliek nekādu pienākumu vākt un glabāt informāciju ar vienīgo mērķi darīt to pieejamu. No datu aizsardzības viedokļa šis ir svarīgs un pozitīvs priekšlikuma elements. EDAU atgādina savu atzinumu par priekšlikumu direktīvai par datu saglabāšanu, kuri apstrādāti saistībā ar publisko elektronisko sakaru pakalpojumu sniegšanu⁽¹⁾, kurā viņš uzsvēra, ka juridiskas saistības, kas veicina lielu datubāzu veidošanos, rada īpašu risku datu subjektiem, *inter alia*, saistībā ar nelikumīgas izmantošanas risku.

33. Tomēr,

— Ir svarīgi nodrošināt, lai priekšlikums neveicinātu datubāzu beznosacījumu savienojumu un tādējādi datubāzu tīklu, ko būtu grūti uzraudzīt.

— Iepriekš minētajam priekšlikuma pamata nodomam ir viens izņēmums: tā 10. pants, kurā paredzēts, ka indeksu dati ir pieejami tiešsaistē. Indeksu datus var būt iekļauti personas dati, vai jebkurā gadījumā tie var atklāt, ka tādi pastāv.

Tieša un netieša piekļuve informācijai

34. Priekšlikumā paredzēta tieša un netieša piekļuve informācijai. Priekšlikuma 9. pantā paredzēta tieša tiešsaistes piekļuve informācijai datubāzēs, kurām attiecīgajām valsts iestādēm ir tieša tiešsaistes piekļuve. 10. pantā paredzēta netieša piekļuve. Indeksu dati attiecībā uz informāciju, kam nevar piekļūt tiešsaistē, ir pieejami tiešsaistē citu dalībvalstu kompetentajām iestādēm un Eiropolam. Ja šī iestāde, iepazīstoties ar indeksu datu saturu, iegūst vajadzīgo rezultātu, tā var izdot informācijas pieprasījumu un nosūtīt to izraudzītajai iestādei, lai saņemtu informāciju, kas identificēta ar indeksu datiem.

35. Tiešā piekļuve nerada jaunas datubāzes, taču tai ir nepieciešama līdzvērtīgu kompetento sistēmu datubāzu savietojamība dalībvalstīs. Vēl jo vairāk — būs vajadzīgs jauns pašreizējo datubāzu lietošanas veids, nodrošinot piekļuves iespējas visām kompetentajām iestādēm dalībvalstīs, kas līdz šim bija atvērtas tikai valsts kompetentajām iestādēm. Tiešā piekļuve automātiski nozīmēs, ka lielāks personu skaits varēs piekļūt datubāzei, un tādējādi tas būs saistīts ar lielāku nepareizas izmantošanas risku.

⁽¹⁾ 2005. gada 26. septembra atzinums par priekšlikumu Eiropas Parlamenta un Padomes Direktīvai par datu saglabāšanu, kuri apstrādāti saistībā ar publisko elektronisko sakaru pakalpojumu sniegšanu, un ar ko groza Direktīvu 2002/58/EK (COM (2005) 438 galīgā redakcijā).

36. Ja citas dalībvalsts kompetentai iestādei ir tieša piekļuve, izcelsmes dalībvalsts izraudzītajām iestādēm nav nekādas kontroles pār piekļuvi datiem un to turpmāku izmantošanu. Šis priekšlikumā paredzētās tiesās piekļuves sekas ir pienācīgi jārisina, jo:

— Šķiet, ka tās atņem izraudzītajām iestādēm spēju atteikt sniegt informāciju (saskaņā ar 14. pantu).

— Tās izvirza jautājumu par atbildību par datu precizitāti un atjaunošanu pēc to iegūšanas. Kā izcelsmes dalībvalsts izraudzītā iestāde var nodrošināt datu atjaunošanu?

— Ne tikai izraudzītās iestādes vairs nespēs pildīt savas saistības atbilstīgi datu aizsardzības likumam, bet arī valsts datu aizsardzības iestādes izcelsmes dalībvalstī vairs nevarēs uzraudzīt saistību izpildi, jo tām nav nekādu pilnvaru attiecībā uz citu dalībvalstu tiesībaizsardzības iestādēm.

— Šīs problēmas kļūst vēl ievērojamākas, kad ir runa par piekļuvi tādu izraudzīto iestāžu un izraudzīto pušu datubāzēm, kas nav tiesībaizsardzības iestādes (skat. 25. — 28. punktu šajā atzinumā).

Šīs tiesās piekļuves sekas ir nopietns iemesls, kāpēc pašreizējā priekšlikuma pieņemšanai būtu jābūt atkarīgai no pamatlēmuma par personas datu aizsardzību pieņemšanas. Taču viena problēma paliek: ir grūti saprast, kā izraudzītās iestādes varētu atteikt sniegt informāciju saskaņā ar 14. pantu.

37. Netiešā pieeja ar indeksu datu palīdzību, kas balstās uz principu "ir informācija/ nav informācijas", nav jauns izdomājums. Tas ir pamatā lielajām Eiropas informācijas sistēmām, kā piemēram, Šengenas informācijas sistēmai. Indeksu datu sistēmas izveides priekšrocība ir tāda, ka tā ļauj izcelsmes dalībvalstīm kontrolēt informācijas apmaiņu no savām policijas datnēm. Ja iestāde, kas meklē informāciju, iepazīstoties ar indeksu datu saturu, iegūst rezultātu, tā var izdot informācijas pieprasījumu attiecībā uz iesaistīto datu subjektu. Iestāde, kurai pieprasījums ir iesniegts, tad var to attiecīgi izvērtēt.

38. Un tomēr ir nepieciešams pamatīgs pētījums, jo indeksu datu sistēmas izveide — jomās, kurās šādu sistēmu vēl nav bijis, izņemot lielās Eiropas informācijas sistēmas, — datu subjektam var radīt jaunus riskus. EDAU uzsver, ka, lai arī

indeksu datos nav pieejama plaša informācija par datu subjektu, meklēšana indeksu datos var sniegt visai jūtīgu rezultātu. Tajā var atklāties, ka persona ir iekļauta policijas lietu materiālos saistībā ar noziedzīgiem nodarījumiem.

39. Tādēļ ir ārkārtīgi svarīgi, lai Eiropas likumdevēji nodrošinātu attiecīgus noteikumus, vismaz saistībā ar indeksu datu izveidi, ar indeksu datu sistematizācijas vadību un ar pienācīgu indeksu datu piekļuves organizāciju. Pēc EDAU domām priekšlikums nav apmierinošs attiecībā uz šiem punktiem. Šajā posmā EDAU novērojis trīs pazīmes:

— Indeksu datu definīcija nav skaidra. Nav saprotams, vai indeksu dati ir domāti kā meta-dati, primārās atslēgas vai pat abi divi? Indeksu datu jēdziens ir jāprecizē, jo tam ir tieša ietekme uz datu aizsardzības līmeni un nepieciešamajiem drošības pasākumiem.

— Priekšlikumā būtu jāprecizē valsts kontaktpunktu nozīme attiecībā uz indeksu datiem. Varētu būt nepieciešams iesaistīt valsts kontaktpunktus, konkrēti gadījumos, kad indeksu datu interpretēšanai nepieciešamas speciālas zināšanas, piemēram, iespējamās pirkstu nospiedumu sakritības gadījumā.

— Priekšlikumā ir paredzēts, ka noteikumus, kas vajadzīgi indeksu datu izveidei, pieņem īstenošanas tiesību aktos saskaņā ar komitoloģijas procedūru, kura paredzēta 19. pantā. Kaut arī īstenošanas noteikumi varētu būt nepieciešami, pamatnoteikumi par indeksu datu izveidi būtu jāiekļauj pašā pamatlēmumā.

Tiesu iestāžu iepriekšēja atļauja

40. Informācijas apmaiņa nekavē dalībvalstis, kuras pieprasa tiesu iestāžu iepriekšēju atļauju, pārsūtīt informāciju pieprasītājiestādei, ja šo informāciju kontrolē tiesu iestāde valstī, kurai pieprasījums iesniegts. Tas ir būtiski, jo saskaņā ar pētījumu par policijas pilnvarām veikt personas datu apmaiņu ⁽¹⁾ ne visās dalībvalstīs policija var autonomi piekļūt datiem. Pēc EDAU domām pieejamības principam nebūtu jāvājina valsts tiesībās paredzētās saistības iegūt iepriekšēju atļauju informācijai, vai vismaz noteikt īpašus noteikumus par tām datu kategorijām, attiecībā uz kurām jāiegūst iepriekšēja atļauja, ko varētu piemērot visās dalībvalstīs.

⁽¹⁾ Atbildes uz aptaujas anketu par Projektu pamatlēmumam par ES dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu, jo īpaši attiecībā uz smagiem noziegumiem, tostarp terora aktiem (Padomes dokuments Nr. 5815/1/05).

41. Šī saistība būtu jāsaprot saistībā ar 11. panta 2. punktu pamatlēmuma priekšlikumā par personas datu aizsardzību, kurā arī paredzēts, ka tā dalībvalsts, kas datus nosūta, nosaka datu tālāku izmantošanu tajā dalībvalstī, uz kuru dati nosūtīti. EDAU atzīmē šā principa nozīmi, kas nepieciešams, lai nodrošinātu, ka ar pieejamību netiek apieti ierobežojoši valsts tiesību akti par tālāku personas datu izmantošanu.

dzības draudus, *inter alia* sakarā ar to, ka ir skarta dalībvalstu kompetence pilnībā kontrolēt datu apmaiņas veicēju. Tas nebūtu jāpieņem neatkarīgi no pamatlēmuma par personas datu aizsardzību.

Nobeiguma piezīme

42. Šiem elementiem nepieciešami augsti datu aizsardzības standarti. Īpaša uzmanība būtu jāvelta tam, lai nodrošinātu mērķu ierobežojuma principu un turpmākas apstrādes principu, kā arī iegūtās informācijas precizitāti un uzticamību (skat. EDAU atzinumu par Pamatlēmumu par personas datu aizsardzību, IV 2 un IV 6 nodaļu).

43. Pirmes Konvencijā piedāvāta cita pieeja pieejamības principa īstenošanai. Ja pašreizējā priekšlikumā pamatlēmumam minēta vispārēja pieeja — neminot īpašus noteikumus specifisku informācijas veidu apmaiņai un to piemērojot visiem informācijas veidiem, ciktāl tie minēti II pielikumā (skat. šā atzinuma 21. — 28. punktu) — tad Pirmes Konvencijas pieeja ir pakāpeniska.

V CITAS PIEEJAS

Zviedrijas priekšlikums

43. Zviedrijas priekšlikums neaprobežojas tikai ar īpašiem informācijas veidiem, bet tajā aptverta visa veida informācija un izlūkdati, pat tāda informācija un izlūkdati, ko glabā iestādes, kas nav tiesībaizsardzības iestādes. Priekšlikumā veicināta sadarbība, nosakot laika ierobežojumus atbilžu sniegšanai uz informācijas pieprasījumiem un novēršot diskrimināciju starp informācijas apmaiņu vienā dalībvalstī un pārrobežu informācijas apmaiņu. Tajā nav paredzēti papildu pasākumi, kas nodrošinātu, ka informācijai var efektīvi piekļūt. Šā iemesla dēļ ir saprotams, kādēļ Komisija ar Zviedrijas priekšlikumu kā ar piemērotu pieejamības instrumentu nebija apmierināta pēc būtības ⁽¹⁾.

44. Šo pieeju dažreiz sauc arī par pieeju “datu lauks pēc datu lauka”. To piemēro specifiskiem informācijas veidiem (DNS, pirkstu nospiedumiem un transportlīdzekļu reģistrācijas datiem) un tajā paredzēta saistība ņemt vērā šo datu specifisko būtību. Konvencijā paredzēts pienākums atvērt un saglabāt DNS analīzes datnes noziedzīgu nodarījumu izmeklēšanai. Līdzīgs pienākums attiecas arī uz datiem par pirkstu nospiedumiem. Attiecībā uz transportlīdzekļu reģistrācijas datiem ir jāatļauj tieša piekļuve citu dalībvalstu valsts kontaktpunktiem.

44. No datu aizsardzības viedokļa Zviedrijas priekšlikuma pieeja ir saistīta ar šādām vispārējām sekām:

— Ir apsveicami, ka priekšlikums ir stingri ierobežots līdz esošo datu apstrādei un neizraisa nekādu jaunu, pat ne “indeksu datu” datubāzu izveidi.

— Tomēr tas, ka “indeksu datu” nav vispār, pēc definīcijas nav pozitīvs elements. Indeksu dati, ja vien tie ir piemēroti droši — var atvieglot precīzāku un tādējādi ar mazāku iejaukšanos saistītu datu meklēšanu, kas var būt jutīgi. Tie paver arī iespēju pieprasījumus labāk filtrēt un labāk pārraudzīt.

— Jebkurā gadījumā priekšlikums veicina lielāku pārrobežu personas datu apmaiņu un personas datu aizsar-

47. Pirmes Konvencijas pieejā var novērot trīs dažādas lietas.

48. Pirmkārt, ir pats par sevi saprotams, ka EDAU neatbalsta šīs konvencijas rašanās procesu, kas ir ārpus Eiropas Savienības iestāžu sistēmas un tādējādi bez ievērojama Komisijas atbalsta. Turklāt tas nozīmē, ka Eiropas Parlaments nevar veikt demokrātisku kontroli, bet Eiropas Kopienu Tiesa — tiesisku kontroli, un rezultātā ir lielāks risks, ka visas (valsts) intereses netiktu vienlīdzīgi ievērotas. Tas attiecas arī uz datu aizsardzības perspektīvu. Citiem vārdiem sakot, Eiropas Savienības iestādēm nav iespējas pirms sistēmas izveides novērtēt, kādas būs izvēlētas politikas sekas uz personas datu aizsardzību.

49. Otrkārt, ir acīmredzams, ka daži Pirmes Konvencijas elementi daudz dziļāk skar datu subjektā nekā priekšlikums pamatlēmumam par pieejamību. Konvencija neizbēgami noved pie jaunu datubāzu izveides, kas pats par sevi jau rada draudus personas datu aizsardzībai. Būtu jāpierāda šo jauno datubāzu nepieciešamība un proporcionalitāte. Būtu jānodrošina piemēroti personas datu aizsardzības pasākumi.

⁽¹⁾ Skatīt Komisijas personāla darba dokumenta pielikumu priekšlikumam Padomes pamatlēmumam par informācijas apmaiņu saskaņā ar informācijas pieejamības principu, SEC 2005 (1270), 12.10.2005.

Pieeja “datu lauks pēc datu lauka”

50. Treškārt, kā jau minēts iepriekš, Konvencijā piedāvāta pieeja “datu lauks pēc datu lauka”. Iepriekš EDAU jau minēja grūtības un neskaidrības, kas saistītas ar vidi, kurā pieejamības princips jāīsteno. Šādos apstākļos pēc EDAU uzskatiem nav ieteicams veidot sistēmu vairākiem datu veidiem, bet gan sākt ar piesardzīgāku pieeju, kas attiektos tikai uz vienu datu veidu, un uzraudzīt, cik lielā mērā pieejamības princips var efektīvi atbalstīt tiesībaizsardzību, kā arī specifiskos draudus personas datu aizsardzībai. Balstoties uz šo pieredzi, sistēmā varētu iekļaut arī citus datu veidus un/ vai to varētu mainīt efektivitātes uzlabošanas nolūkā.

51. Šī pieeja “datu lauks pēc datu lauka” labāk pildītu arī proporcionalitātes principa prasības. Pēc EDAU domām nepieciešamība pēc labākas pārrobežu datu apmaiņas tiesībaizsardzības nolūkos varētu atļaut ES mēroga juridiska instrumenta pieņemšanu, taču proporcionalitātes nolūkā šim instrumentam būtu jābūt piemērotam, lai tas varētu sasniegt savu mērķi un ko pareizāk varētu izveidot pēc praktiskas pieredzes perioda. Turklāt instruments nedrīkstētu nodarīt neproporcionālu kaitējumu datu subjektam. Apmaiņai vajadzētu attiekties tikai uz tiem datu veidiem, kas ir noteikti nepieciešami, ar iespēju veikt anonīmu datu apmaiņu, un tai vajadzētu notikt, ievērojot stingrus datu aizsardzības nosacījumus.

52. Turklāt, pieeja, kas būtu piesardzīgāka par EDAU ieteikto, — iespējami apvienota ar pieeju “datu lauks pēc datu lauka” — varētu ietvert pieejamības principa īstenošanas uzsākšanu tikai ar netiešo piekļuvi, ar indeksu datu starpniecību. EDAU šo min kā jautājumu, kas būtu jāizskata turpmākajā likumdošanas procesā.

VI KĀDI DATI?

53. Il pielikumā ir uzskatīti informācijas veidi, kurus var iegūt saskaņā ar ierosināto pamatlēmumu. Visi seši tur uzskatītie informācijas veidi vairumā gadījumu ir personas dati, jo ir saistīti ar identificētu vai identificējamu personu.

54. Saskaņā ar priekšlikuma 3. panta g) apakšpunktu “indeksu dati” ir “dati, kuru uzdevums ir skaidri identificēt informāciju

un ko var iegūt ar parasto meklēšanas funkciju, lai konstatētu, vai ir pieejama informācija.” Dokumentā “Pieeja pieejamības principa īstenošanai”⁽¹⁾ šādi dati ir kvalificēti kā indeksu dati:

- attiecīgo personu identifikācijas dati;
- attiecīgo priekšmetu (transportlīdzekļu/dokumentu) identifikācijas numurs;
- pirkstu nospiedumi/digitālie fotoattēli.

Vēl viens datu veids, ko varētu kvalificēt kā indeksu datus, ir DNS profili. Indeksu datu saraksts rāda, ka indeksu dati var ietvert personas datus, un tādēļ ir vajadzīga pienācīga aizsardzība.

55. EDAU jo īpaši pievēršas DNS profilu jautājumam. DNS analīze ir izrādījusies ļoti vērtīga noziegumu izmeklēšanā, un efektīva DNS datu apmaiņa var būt būtiska cīņā pret noziedzību. Tomēr ir svarīgi, lai DNS datu jēdziens būtu skaidri definēts un lai šo datu īpašās iezīmes būtu pienācīgi ņemtas vērā. No datu aizsardzības viedokļa atšķirība starp DNS paraugiem un DNS profiliem tiešām ir liela.

56. DNS paraugi (ko bieži savāc un uzglabā tiesībaizsardzības iestādes) būtu jāuzskata par īpaši jutīgiem, jo tie biežāk ietver pilnu DNS “ainu”. Tie var sniegt informāciju par personas ģenētiskajām iezīmēm un veselības stāvokli, kas var būt vajadzīgs gluži citiem mērķiem, piemēram, sniedzot medicīniskus padomus personām un jauniem pāriem.

57. Turpretī DNS profili var ietvert tikai daļēju DNS informāciju, kas iegūta no DNS parauga: tos var izmantot, lai pārbaudītu personas identitāti, bet principā tie neatklāj personas ģenētiskas iezīmes. Neskatoties uz to, zinātnes progress var palielināt informāciju, ko var atklāt DNS profili: kas kādā konkrētā brīdī ir uzskatīts par “nevainīgu” DNS profilu, vēlāk var atklāt daudz vairāk informācijas nekā gaidīts vai vajadzīgs, un jo īpaši informāciju par personas ģenētiskajām iezīmēm. Tātad DNS profilu atklāto informāciju būtu jāuzskata par dinamisku.

58. Šajā sakarā EDAU atzīmē, ka gan Prīmes (Prīm) konvencija, gan Komisijas priekšlikums veicina DNS datu apmaiņu starp tiesībaizsardzības iestādēm, bet pastāv būtiskas atšķirības veidā, kādā tie to dara.

⁽¹⁾ Dokuments, ko prezidentvalsts nosūtīja Padomei 2005. gada 5. aprīlī (Dok. Nr.: 7641/05).

59. EDAU atzinīgi novērtē to, ka Komisijas priekšlikumā nav noteikts nekāds pienākums apkopot DNS datus un ka tas skaidri ierobežo DNS datu apmaiņu uz DNS profiliem. II pielikumā DNS profili definēti sākotnēji vienotā sarakstā, kurā uzskatīti DNS marķieri, ko dalībvalstīs izmanto DNS analīzēm kriminālistikā. Šajā sarakstā, kas balstīts uz Eiropas standarta komplekta septiņiem DNS marķieriem, kā definēts I pielikumā Padomes 2001. gada 25. jūnija Rezolūcijā par apmaiņšanos ar DNS analīzes rezultātiem⁽¹⁾, ir garantēts, ka DNS profili iegūšanas brīdī neietvers nekādu specifisku ģenētisko informāciju.
60. EDAU uzsver, ka šajā Padomes Rezolūcijā noteiktas dažas ļoti būtiskas garantijas, kas īpaši saistītas ar DNS profilu dinamisko būtību. Rezolūcijas III iedaļā noteikts DNS analīzes rezultātu apmaiņas ierobežojums, attiecinot tikai uz "hromosomu zonām [...], par kurām nav zināms, vai tās sniedz informāciju par specifisku ģenētisko informāciju", un turpmāk tekstā dalībvalstīm ieteikts vairs neizmantot tos DNS marķierus, kuri, pateicoties zinātniskajiem sasniegumiem, var sniegt specifisku ģenētisko informāciju.
61. Prīmes (*Prīm*) konvencija piedāvā savādāku pieeju, uzliekot par pienākumu Līgumslēdzējām pusēm atvērt un saglabāt DNS analīzes datnes kriminālnoziedzumu izmeklēšanai. Tādēļ tajā paredzēta jaunu DNS datubāzu radīšana un pastiprināta DNS datu apkopošana. Turklāt nav skaidrs, kādi datu veidi ir iekļauti "DNS analīzes datnēs", un konvencijā nav ņemta vērā DNS profilu dinamiskā attīstība.
62. EDAU norāda, ka jebkuram tiesiskam instrumentam, ar ko nosaka DNS datu apmaiņu, būtu:
- skaidri jāierobežo un jānosaka DNS informācijas veidi, ar kuriem var apmainīties (arī attiecībā uz būtisko atšķirību starp DNS paraugiem un DNS profiliem).
 - jāizveido kopēji tehniski standarti, lai izvairītos no tā, ka atšķirības darbā ar kriminālistikas DNS datubāzēm dalībvalstīs varētu izraisīt grūtības un neprecīzus rezultātus, apmainoties datiem.
 - jāsniedz pienācīgas juridiski saistošas garantijas, lai novērstu to, ka, pateicoties zinātnes sasniegumiem, no DNS profiliem varētu iegūt personas datus, kas ir ne tikai jūtīgi, bet arī nevajadzīgi mērķim, kādam apkopot.
63. Šajā sakarā EDAU ar šo apstiprina un iekļauj piezīmes, kas jau izdarītas tā atzinumā par Pamatlēmumu par personas datu aizsardzību (80. punkts). Šajā atzinumā EDAU attiecībā uz DNS datiem norādīja, ka būtu jānodrošina īpašas garantijas, lai nodrošinātu, ka: pieejamo informāciju var izmantot tikai, lai kriminālnoziedzumu novēršanas, atklāšanas un izmeklēšanas nolūkos identificētu personas; DNS profilu precizitātes pakāpe ir rūpīgi ņemta vērā, un datu subjekts to var apstrīdēt ar viegli pieejamiem līdzekļiem; ir nodrošināta personu cieņas ievērošana⁽²⁾.
64. Šie apsvērumi liek secināt, ka tiesību akti par DNS datņu izveidi un šo datņu datu apmaiņu būtu jāpieņem tikai pēc ietekmes novērtējuma, kurā būtu pienācīgi izvērtēti ieguvumi un riski. EDAU iesaka šajā tiesību aktā iekļaut pienākumu pēc tā stāšanās spēkā to regulāri izvērtēt.
65. Visbeidzot II pielikumā ietverti citi informācijas veidi, ar kuriem var apmainīties. Tajā ietverta informācija no privātā sektora dalībniekiem, jo telefonu numuru un citu saziņas datu, kā arī datu plūsmas datu izcelsme parasti ir telefonu operatori. Paskaidrojuma rakstā apstiprināts, ka dalībvalstīm ir pienākums nodrošināt to, ka no tiesībaizsardzības viedokļa saistošā informācijā, ko kontrolē iestādes vai šim nolūkam izraudzīti privātā sektora dalībnieki, dalās ar līdzvērtīgām iestādēm citās dalībvalstīs un ar Eiropolu. Tā kā priekšlikums attiecas uz personas datiem, kuru izcelsme ir privātā sektora dalībnieki, EDAU uzskata, ka piemērojamajā tiesiskajā pamatā būtu jābūt ietvertām papildu garantijām datu subjektu aizsardzībai, lai nodrošinātu datu precizitāti.

VII DATU AIZSARDZĪBAS PRINCIPI

66. Personas datu aizsardzības noteikumi nav īpaši noteikti ierosinātajā Padomes pamatlēmumā, savukārt citos instrumentos, piemēram, Prīmes (*Prīm*) konvencijā vai Zviedrijas priekšlikumā ir daži specifiski noteikumi par personas datu aizsardzību. Īpašu personas datu aizsardzības noteikumu trūkums pieejamības priekšlikumā ir pieņemams tikai tiktāl, ciktāl pilnībā ir piemērojami vispārēji noteikumi, kas iekļauti priekšlikumā pamatlēmumam par datu aizsardzību trešajā pīlārā, un ciktāl tie sniedz pietiekamu aizsardzību. Turklāt konkrētos instrumentos — piemēram, Zviedrijas priekšlikumā un Prīmes (*Prīm*) konvencijā — paredzētie noteikumi par personas datu aizsardzību nedrīkstētu vājināt vispārējās sistēmas nodrošināto aizsardzību. EDAU iesaka iekļaut īpašu klauzulu par iespējamiem konfliktiem starp dažādiem datu aizsardzības noteikumiem.

⁽²⁾ Šajā pašā sakarā skatīt arī Eiropas Padomes "Progresā ziņojumu par 108. Konvencijas principu piemērošanu biometrijas datu vākšanai un apstrādei", 2005. gada februāris.

⁽¹⁾ OV C 187, 1. lpp.

67. Šobrīd EDAU, atgādinot savu atzinumu attiecībā uz Pamatlēmumu par personas datu aizsardzību, atkal vēlētos uzsvērt to, cik svarīgi ir tādi darbojošies konsekvienti un visaptveroši datu aizsardzības noteikumi attiecībā uz tiesībaizsardzības iestāžu sadarbību, kas attiecas uz visa veida apstrādi. Tādējādi EDAU atkārtoti apstiprina citus šā atzinuma punktus. Šajā punktā ir uzsvērti šādi datu aizsardzības jautājumi:

— Personas datu likumīga apstrāde. EDAU atbalsta pieeju, ka informācija var būt pieejama tikai tad, ja tā apkopota likumīgi (kā minēts 2.2. punktā attiecībā uz informāciju, kas iegūta piespiedu pasākumu ceļā). Likumīga personas datu apstrāde arī nodrošinātu to, ka informācija, kas darīta pieejama un ar ko apmainās, var pienācīgi tikt izmantota arī tiesvedībā. Proti, lai arī apstrādātā informācija pēc kriminālvajāšanas sākuma neietilpst ierosinātā instrumenta darbības jomā, aizvien pastāv iespēja, ka informācija, ar ko tiesībaizsardzības iestādes apmainās, nonāks tiesvedībā.

— Īpaši svarīga ir personas datu kvalitāte, jo saskaņā ar pieejamības principu ir labāk, ja informāciju izmantos tiesībaizsardzības iestādes, kas nepiedalījās datu apkopšanā. Šīm iestādēm pat ir tieša piekļuve citu dalībvalstu datubāzēm. Personas datu kvalitāti var nodrošināt tikai tādā gadījumā, ja to precizitāti regulāri un pienācīgi pārbauda, ja informāciju nodala atbilstīgi dažādām iesaistīto personu kategorijām (cietušajiem, aizdomās turamajiem, lieciniekiem u.c.) un ja vajadzības gadījumā ir norādīta precizitātes pakāpe (skatīt EDAU atzinumu par personas datu aizsardzību, IV 6).

Šajos punktos vēlreiz izskaidrots, kāpēc personas datu aizsardzības noteikumi un jo īpaši noteikumi par precizitāti būtu jāpiemēro visiem apstrādes veidiem, arī vietējai apstrādei. Citādi personas dati, kuriem piekļūst nepastarpināti, varētu būt nepareizi, neaizsargāti un tādējādi aizskartu datu subjekta tiesības un iespaidotu izmeklēšanas efektīvāti.

— Mērķu ierobežojums. Atbilstīgi pieejamības principam personas datiem var piekļūt līdzvērtīgas citu dalībvalstu kompetentās iestādes. Tomēr tiesībaizsardzības iestāžu kompetences dažādās valstīs var būtiski atšķirties. Tādēļ ir svarīgi nodrošināt, ka mērķu ierobežojuma pamatprincips ir ievērots, neskatoties uz dažādo kompetento iestāžu, kuras apmainās ar datiem, dažādajām kompetencēm. Informāciju, ko konkrēta iestāde apkopojusi un apstrādājusi konkrētam mērķim, nevar izmantot citam mērķim, tikai pamatojoties uz saņēmēja iestādes atšķirīgām, varbūt plašākām kompetencēm.

Tādēļ EDAU pauž gandarījumu par 7. pantu ierosinātajā pamatlēmumā, ko būtu jāuzskata kā vispārējo noteikumu, kuri paredzēti ierosinātajā pamatlēmumā par personas datu aizsardzību, precizējums. Turklāt EDAU atzīmē, ka novērtējums par līdzvērtību starp dažādām iestādēm (kas šajā priekšlikumā ir atstāts komitoloģijas procedūras ziņā) būtu jāveic rūpīgi un pienācīgi ņemot vērā mērķa ierobežojuma principu.

— Laika ierobežojumi apmainītās informācijas uzglabāšanai arī būtu jāvērtē, ņemot vērā principu par mērķa ierobežojumu: informācija, kurai piekļūst vai ar ko apmainās vienam mērķim, būtu jāizdzēš, līdzko tā vairs nav vajadzīga šim mērķim. Tā varētu izvairīties no nevajadzīgas datubāzu dublēšanās, reizē tomēr atļaujot kompetentām iestādēm atkal piekļūt (atjauninātai) pieejamai informācijai, ja tas ir vajadzīgs citam likumīgam mērķim.

— Pārsūtītās informācijas reģistrēšana atbilstīgi pieejamības principam. Reģistrēšana būtu jāveic abām pusēm: kā lūguma saņēmējai dalībvalstij, tā lūguma iesniedzējai dalībvalstij. Būtu jāsauglabā arī piekļuves reģistri, ne tikai apmaiņas reģistri (skatīt EDAU atzinumu par personas datu aizsardzību, 133. punkts), lai nodrošinātu arī to, ka valstu kompetentās iestādes uzticas cita citai un pilnībā nezaudē kontroli pār pieejamo informāciju. Vajadzība pēc informācijas izsekojamības ietver arī iespēju atjaunināt un/vai labot informāciju.

— Datu subjektu tiesības. Sistēmas informācijas apmaiņai starp ES tiesībaizsardzības iestādēm palielina to situāciju skaitu, kurās personas datus (pagaidu kārtā) vienlaikus apstrādā kompetentas iestādes dažādās dalībvalstīs. Tas no vienas puses nozīmē, ka būtu jāizveido kopēji ES standarti par datu subjektu tiesībām, un no otras puses, ka datu subjektiem būtu jāspēj īstenot savas tiesības, ciktāl to pieļauj noteikumi par datu aizsardzību trešajā pilārā, gan attiecībā uz iestādēm, kas sniedz piekļuvi datiem, gan attiecībā uz iestādēm, kas piekļūst šiem datiem un apstrādā tos.

— Pārraudzība. EDAU norāda, ka, atkarībā no gadījuma, vairāk nekā viena valsts pārraudzības iestāde var būt kompetenta uzraudzīt personas datu apstrādi, ko veic, pamatojoties uz šiem priekšlikumiem. Šajā sakarā tiesībsaistes piekļuve tiesībaizsardzības informācijai prasa pastiprinātu pārraudzību un koordināciju no valstu attiecīgo datu aizsardzības iestāžu puses.

VIII SECINĀJUMI

Vispārēji secinājumi par pieejamības principu

68. EDAU izmanto šo iespēju, lai atzinumā iekļautu dažas vispārējas un dažas būtiskas piezīmes saistībā ar tiesībsardzības informācijas apmaiņu un šā jautājuma reglamentācijas iespējām. EDAU vēlāk būs pieejams turpmākām konsultācijām pēc attiecīgiem jaunumiem likumdošanas procesā saistībā ar šo un citiem saistītiem priekšlikumiem.
69. Pēc EDAU domām piesardzības princips būtu jāietver saistošā juridiskā instrumentā ar piesardzīgākas, pakāpeniskākas pieejas palīdzību, kas attiektos tikai uz vienu datu veidu, un būtu jāuzrauga, cik lielā mērā pieejamības princips var efektīvi atbalstīt tiesībsardzību, kā arī specifiskos draudus personas datu aizsardzībai. Šī piesardzīgākā pieeja varētu iekļaut pieejamības principa īstenošanas uzsākšanu tikai ar netiešo piekļuvi, ar indeksu datu starpniecību. Balstoties uz šo pieredzi, sistēmā varētu iekļaut arī citus datu veidus un/ vai to varētu mainīt efektivitātes uzlabošanas nolūkā.
70. Nebūtu jāpieņem nekādi juridiski instrumenti pieejamības principa īstenošanai, pirms nav pieņemti pietiekami datu aizsardzības pasākumi, kā minēts priekšlikumā pamatlēmumam par personas datu aizsardzību.

Ieteikumi par pašreizējā priekšlikuma grozījumiem

71. EDAU iesaka šādi precizēt pieejamības principa darbības jomu:
- Iekļaut precīzu un skaidru to datu definīciju, ko uzskatīs par pieejamiem.
 - Kā pirmo iespēju — ierobežot pieejamības principa darbības jomu tikai ar informāciju, ko kontrolē kompetentas iestādes.
 - Kā otru iespēju — ja darbības joma būs plašāka — nodrošināt pietiekamu personas datu aizsardzību. Jāņem vērā šā atzinuma 27. punktā minētie jautājumi.
72. EDAU ir veicis šādus novērojumus par tiešo piekļuvi datubāzēm, ko veic citas dalībvalsts kompetenta iestāde:
- Jautājums ir attiecīgi jārisina, jo tiešās piekļuves gadījumā izraudzītajām iestādēm izcelsmes dalībvalstī nav nekādas kontroles pār piekļuvi datiem un to tālāku izmantošanu.

- Priekšlikums nedrīkst veicināt datubāzu beznosacījumu savienojumu un tādējādi datubāzu tīklu, ko būtu grūti pārraudzīt.
73. Pamatlēmumā būtu precīzāk jānosaka indeksu datu sistēmas izveide. Konkrēti:
- Priekšlikumā būtu jānodrošina attiecīgi noteikumi, vismaz saistībā ar indeksu datu izveidi, ar indeksu datu sistematizācijas vadību un ar pienācīgu indeksu datu piekļuves organizāciju.
 - Jāprecizē indeksu datu definīcija.
 - Priekšlikumā būtu jāprecizē valsts kontaktpunktu nozīme attiecībā uz indeksu datiem.
 - Pamatnoteikumi par indeksu datu izveidi būtu jāiekļauj pašā pamatlēmumā, nevis jāatstāj īstenošanas tiesību aktu ziņā saskaņā ar komitoloģijas procedūru.
74. EDAU atzīmē, ka priekšlikumā attiecībā uz DNS datu apmaiņu būtu:
- skaidri jānorobežo un jānosaka DNS informācijas veids, ar ko var apmainīties (arī ņemot vērā fundamentālās atšķirības starp DNS paraugiem un DNS profiliem);
 - jāizstrādā kopīgi tehniskie standarti, kuru mērķis būtu novērst atšķirības tiesu medicīnas DNS datubāzu darbībās dalībvalstīs, kas varētu radīt grūtības un neprecīzus rezultātus, veicot datu apmaiņu;
 - jānodrošina pienācīgi juridiski saistoši drošības pasākumi, kuru mērķis būtu novērst to, ka zinātnes sasniegumu nolūkā varētu iegūt DNS profilus ar personas datiem, kas ir ne tikai jūtīgi, bet arī nevajadzīgi to iegūšanas mērķim;
 - būtu jāparedz tā pieņemšana tikai pēc ietekmes novērtējuma.
75. EDAU aicina ierobežot informācijas apmaiņu ar Eiropu tikai pašā Eiropas vajadzībām, kā minēts Eiropas Konvencijas 2. pantā un tai pievienotajā pielikumā.

Briselē, 2006. gada 28. februārī

Peter HUSTINX

Eiropas Datu aizsardzības uzraudzītājs