EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o predlogu uredbe Evropskega parlamenta in Sveta o Vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov o vizumih za kratkoročno prebivanje med državami članicami (KOM(2004) 835 končno)

(2005/C 181/06)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti in zlasti člena 286 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah in zlasti člena 8 Listine,

ob upoštevanju Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov,

ob upoštevanju Uredbe (ES) št. 45/2001/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov in zlasti člena 41 Uredbe,

ob upoštevanju prošnje za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki jo je 25. januarja 2005 prejel od Komisije –

SPREJEL NASLEDNJE MNENJE:

1. **UVOD**

1.1. **Uvodne opombe**

Vzpostavitev Vizumskega informacijskega sistema (VIS) je pomemben del skupne vizumske politike EU in je bila predmet več med seboj prepletenih instrumentov.

— Aprila 2003 je bila pripravljena študija izvedljivosti ([1]) VIS, ki jo je naročila Komisija.

— Septembra 2003 je Komisija predlagala spremembo ([2]) prejšnje uredbe, ki je določala enotno obliko za vizume. Glavni cilj pri novi obliki za vizume je bila uvedba biometričnih podatkov (podoba obraza in dva prstna odtisa). Ti biometrični podatki bi bili shranjeni na mikročipu.

([1]) Vizumski informacijski sistem, končno poročilo, ki ga je naročila ES ter pripravil Trasys, aprila 2003.
([2]) KOM(2003) 558 končno z 2003/0217 (CNS) in 2003/0218 (CNS)

— Junija 2004 se je s sklepom ([1]) Sveta sprožil postopek gradnje Vizumskega informacijskega sistema, ki je pravna podlaga za njegovo vključitev v proračun EU. Ta sklep je predlagal vzpostavitev centralne podatkovne baze s podatki v zvezi z vlogami za izdajo vizuma ter načrtoval „komitološki“ proces, z namenom upravljanja tehnološkega razvoja VIS.

Decembra 2004 je Komisija sprejela predlog uredbe v zvezi z VIS in izmenjavo podatkov o vizumih za kratkoročno prebivanje ([2]) med državami članicami (v nadaljnjem besedilu: „predlog“), ki je predmet tega mnenja. Predlogu je priložena študija Razširjene ocene vplivov ([3]) (v nadaljevanju: „EIA“).

Kakor je navedeno v obrazložitvenem memorandumu, bodo kljub temu za dopolnitev te uredbe potrebni novi pravni instrumenti, zlasti za:

— spremembo Skupnih konzularnih navodil o vizumih za diplomatske misije in konzularna predstavništva schengenskih držav (v nadaljnjem besedilu „Skupna konzularna navodila“), ki se nanašajo na uvedbo biometričnih podatkov v postopke;

— razvoj novega mehanizma za izmenjavo podatkov z Irsko in Združenim kraljestvom;

— izmenjavo podatkov v zvezi z vizumi za dolgoročno prebivanje.

Kakor je odločil Svet za pravosodje in notranje zadeve dne 5. in 6. junija 2003 in kakor je opisano v členu 1(2) sklepa prej omenjenega Sveta iz junija 2004, bo VIS zasnovan na centralizirani arhitekturi, ki se sestoji iz podatkovne baze, kjer se bodo shranjevali podatki o vlogah za izdajo vizumov: centralni vizumski informacijski sistem (CS-VIS) in nacionalni vmesnik (NI-VIS), ki se nahaja v državah članicah. Države članice imenujejo ([4]) centralni nacionalni organ, ki bo povezan z nacionalnim vmesnikom in preko katerega bodo imeli pooblaščeni organi držav članic dostop do CS-VIS.

1.2. **Glavni elementi predloga z vidika varstva podatkov**

Cilj predloga je izboljšanje upravljanja skupne vizumske politike z vzpostavitvijo centralne podatkovne baze za učinkovitejšo izmenjavo podatkov med državami članicami. Uredba načrtuje vpeljavo biometričnih podatkov (fotografije in prstnih odtisov) v postopek obdelave vloge ter njihovo shranjevanje v centralni podatkovni bazi.

Biometrični podatki se lahko uporabijo tudi v vizumskih nalepkah, kakor je bilo predvideno v predlogu spremenjene uredbe Komisije v zvezi z enotno obliko vizumov ob vpeljavi fotografije in prstnega odtisa, ki sta shranjena na mikročipu (pričakuje se sklep Sveta, ki bo temeljil na analizi, ki je v teku).

Predlog do potankosti opisuje različne postopke obdelave podatkov (vnos, sprememba, izbris in uporaba) ter razne podatke, ki jih je treba dodati v VIS, odvisno od statusa vloge (sprejeta, zavrnjena, itd.).

Predlog določa petletno obdobje hrambe podatkov, ki se navezujejo na posamezno prošnjo.

Predlog vsebuje omejen seznam pristojnih organov – sem ne sodijo organi, pristojni za izdajo vizumov –, ki bodo imeli dostop do VIS, ter določa dostopne pravice, ki jih bodo dobili:

— pristojni organi za izvajanje kontrol vizumov na zunanjih mejah in na ozemlju države članice

— pristojni organi za priseljevanje

([1]) 2004/512/ES, UL L 213, 15.6.2004, str. 5.
([2]) KOM(2004) 835 končno z 2004/0287 (COD)
([3]) Študija Razširjene ocene vplivov Vizumskega informacijskega sistema, končno poročilo EPEC, december 2004
([4]) Člen 24(2) predloga.

— pristojni organi za azil

V opisu delovanja VIS in nanj se nanašajočih odgovornosti se v predlogu poudarja, naj Komisija predela podatke VIS v imenu držav članic. Opisuje potrebo po uporabi evidenc obdelave podatkov, z namenom zagotoviti varnost podatkov, ter navaja posamezne odgovornosti za zagotovitev omenjene stopnje varnosti.

Predlog vsebuje poglavje o varstvu podatkov, pri čemer je podrobno opisana vloga nacionalnih organov, kakor tudi vloga Evropskega nadzornika za varstvo podatkov (v nadaljnjem besedilu: „EDPS“).

Predlog zaupa tehnično izvedbo VIS ter izbor potrebne tehnologije odboru, ki ga določa člen 5(1) Uredbe (ES) št. 2424/2001 o razvoju druge generacije Schengenskega informacijskega sistema (SIS II).

V prilogi predloga se nahaja razširjena ocena vplivov VIS, ki jo je naročila Komisija ter pripravil EPEC. Ocena se zaključi z ugotovitvijo, da je uporaba VIS ob podpori biometričnih podatkov trenutno najboljša rešitev za izboljšanje skupne vizumske politike.

2. **USTREZNI OKVIR**

Predlog bo močno vplival na zasebnost in druge temeljne pravice posameznikov, zato ga je treba preveriti v skladu z načeli varstva podatkov. Glavne referenčne točke za naš pregled so naslednje.

— Spoštovanje zasebnega življenja je v Evropi zagotovljeno že od sprejetja Konvencije o varstvu človekovih pravic in temeljnih svoboščin leta 1950 (v nadaljnjem besedilu: „ECHR“) s strani Sveta Evrope. Člen 8 ECHR določa „pravico do spoštovanja zasebnega in družinskega življenja“.

  V skladu s členom 8(2) je vsako vmešavanje s strani javne oblasti v izvrševanje te pravice dovoljeno le, če je to „določeno z zakonom“ in „nujno v demokratični družbi“ za zaščito pomembnih interesov. V sodni praksi Evropskega sodišča za človekove pravice so zaradi teh pogojev nastale dodatne potrebe na področju kakovosti pravne podlage za vmešavanje, sorazmernosti vsakega ukrepa ter potrebe po ustreznih nadzornih ukrepih za preprečevanje zlorabe.

  V Konvenciji o varstvu podatkov, sprejeti s strani Sveta Evrope leta 1981, so zabeležena temeljna načela za varstvo posameznikov, zlasti kar zadeva obdelavo osebnih podatkov.

— Nedavno bila določena pravica do spoštovanja zasebnega življenja ter varstvo osebnih podatkov v členih 7 in 8 Listine o temeljnih pravicah Evropske Unije, ki je postala sestavni del Dela II nove Ustave EU.

  V skladu s členom 52 Listine se priznava, da so te pravice lahko omejene, pod pogojem, da so izpolnjeni podobni pogoji, kakršni veljajo v skladu s členom 8 ECHR. Te pogoje je treba upoštevati, kadar koli se ocenjuje predlog za morebitno vmešavanje.

Danes so v zakonodaji EU osnovna pravila o varstvu podatkov zapisana v:

— Direktivi 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, str. 31). Ta direktiva bo v nadaljnjem besedilu imenovana „Direktiva 95/46/ES“. Direktiva natančno določa načela, ki bodo merilo za preverjanje predloga v tolikšni meri, v kolikšni zadeva države članice. To je zlasti pomembno, ker se bo predlog uporabljal skupaj z nacionalno zakonodajo, ki bo direktivi zagotovila učinkovitost. Učinkovitost predlaganih določb in nadzornih ukrepov bo torej odvisna od učinkovitosti te kombinacije v vsakem posameznem primeru.

— Uredbi (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, str. 1). Ta uredba bo v nadaljnjem besedilu imenovana „Uredba 45/2001“. Določa podobna načela kakor Direktiva 95/46/ES ter je v zvezi s tem pomembna v tolikšni meri, v kolikšni bo predlog vplival na dejavnosti Komisije, skupaj z določbami Uredbe. Zato je treba tudi tej kombinaciji posvetiti nekaj pozornosti.

Direktiva 95/46/ES in Uredba 45/2001 se morata brati skupaj z drugimi instrumenti. Drugače povedano, direktivo in uredbo si je treba razlagati v luči temeljnih pravic v tolikšni meri, v kolikšni se dotikata osebnih podatkov, zaradi katerih se lahko kratijo temeljne svoboščine, zlasti pravica do zasebnosti. To sledi tudi iz sodne prakse Evropskega sodišča. ([1])

— EDPS bo v svojo analizo vključil tudi Mnenje št. 7/2004 z dne 11. avgusta 2004 v zvezi s členom 29 Delovne skupine za varstvo podatkov ([2])„v zvezi z vključitvijo biometričnih podatkov v dovoljenja za prebivanje in vizume, ob upoštevanju vzpostavitve Evropskega vizumskega informacijskega sistema (VIS).“ V tem mnenju je delovna skupina izrazila skrbi v zvezi z več elementi predloga. EDPS bo preveril, ali so bile pri predlogu te skrbi upoštevane in kako so bile upoštevane.

3. **ANALIZA PREDLOGA**

3.1. **Splošno**

EDPS priznava, da je za nadaljnji razvoj skupne vizumske politike potrebna učinkovita izmenjava ustreznih podatkov. Eden izmed mehanizmov, ki lahko zagotovi nemoten pretok informacij, je VIS. Toda tak nov instrument je treba omejiti na zbiranje in izmenjavo podatkov, kolikor sta takšno zbiranje in izmenjava potrebna za razvoj skupne vizumske politike ter sorazmerna s tem ciljem.

Vzpostavitev VIS lahko ugodno učinkuje na druge zakonite javne interese, kar pa ne spreminja namena VIS. Omejen namen sistema je ključnega pomena pri določanju legitimne vsebine ter uporabe sistema, posledično tudi pri podeljevanju pravice do dostopa do VIS (ali delov njegovih podatkov) organom držav članic za namene zakonitih javnih interesov.

Predlog poleg tega dejansko uvaja uporabo biometričnih podatkov v VIS. EDPS se zaveda prednosti uporabe biometričnih podatkov, vendar izpostavlja močan vpliv uporabe takšnih podatkov ter predlaga vnos strogih nadzornih ukrepov pri uporabi biometričnih podatkov.

To mnenje je treba brati ob upoštevanju teh glavnih pomislekov. Poudarjeno je, da bi bilo treba trenutno mnenje omeniti v preambuli uredbe pred uvodnimi izjavami („ob upoštevanju mnenja …“).

([1]) V tem kontekstu je koristno omeniti sodbo Sodišča v zadevi Österreichischer Rundfunk and Others (združene zadeve C-465/00, C-138/01 in C-139/01, sodba z dne 20. maja 2003, občna seja, (2003) PSES I-4989). Sodišče je obravnavalo avstrijski zakon, ki določa prenos podatkov o plačah uslužbencev javnega sektorja Avstrijskemu računskemu sodišču ter njihovo naknadno objavo. V svoji sodbi je Sodišče zabeležilo številne kriterije iz člena 8 Evropske konvencije o varstvu človekovih pravic, naj bi se uporabljali pri uporabi Direktive 95/46/ES, kolikor ta direktiva dovoljuje določene omejitve pri pravici do zasebnosti.

([2]) To je neodvisna posvetovalna skupina, ki je nastala na podlagi Direktive 95/46/ES ter se sestoji iz predstavnikov organov držav članic za varstvo podatkov, EDPS in Komisije.

3.2. **Namen**

Namen VIS je ključnega pomena tako v luči člena 8 ECHR kot splošnega okvirja varstva podatkov. V skladu s členom 6 Direktive 95/46/ES morajo biti osebni podatki „zbrani za določene, izrecne ter zakonite namene in se ne smejo naprej obdelovati na način, ki je nezdružljiv s temi nameni." Le z jasno opredelitvijo namenov se bosta lahko pravilno ocenila sorazmernost in natančnost obdelave osebnih podatkov, kar je ključnega pomena zaradi oblike podatkov (vključno z biometričnimi podatki) in razsežnosti načrtovanega postopka obdelave.

Namen VIS je izrecno naveden v členu 1(2) predloga:

> „VIS bo z olajšanjem izmenjave podatkov o vlogah za izdajo vizumov in spremljajočih sklepov med državami članicami izboljšal upravljanje skupne vizumske politike, konzularno sodelovanje in posvetovanje med centralnimi konzularnimi oblastmi."

Zato morajo biti vsi elementi VIS potrebni in sorazmerni instrumenti za doseganje tega cilja v interesu skupne vizumske politike.

V členu 1(2) predloga so navedene tudi dodatne prednosti izboljšanja vizumske politike kot npr.:

(a) preprečevanje groženj notranji varnosti,

(b) lajšanje boja proti goljufijam,

(c) lajšanje kontrol na zunanjih mejnih prehodih.

EDPS te elemente obravnava kot primere pozitivnih posledic vzpostavitve VIS in izboljšanja skupne vizumske politike, ne pa kot samostojne namene.

Iz tega lahko na tej stopnji sklepamo na dve glavni posledici:

— EDPS se zaveda, da organi pregona želijo pridobiti pravico do dostopa do VIS; v zvezi s tem so bili dne 7. marca 2005 sprejeti sklepi Sveta. Ker je namen VIS izboljšanje skupne vizumske politike, je treba omeniti, da rutinski dostop organov pregona ne bi bil v skladu s tem namenom. Medtem ko bi bil v skladu s členom 13 Direktive 95/46/ES tak dostop lahko odobren na *ad hoc* osnovi, v posebnih okoliščinah in v odvisnosti od ustreznih nadzornih ukrepov, se sistematični dostop ne sme dovoliti.

  Bolj splošno povedano je ocena sorazmernosti in potrebe ključnega pomena, če se bodo v prihodnje sprejemale odločitve o tem, ali se določenim drugim oblastem dovoli dostop do VIS. Naloge, za katere je odobren dostop, se morajo ujemati z nameni VIS.

— Izrecna omemba „preprečevanja groženj notranji varnosti vsake države članice" v (a) ni posrečena. Glavne prednosti VIS bodo preprečevanje goljufij in trgovanja z vizumi (boj proti goljufijam je tudi glavni razlog za vpeljevanje biometričnih podatkov v sistem) ([1]). Preprečevanje groženj varnosti se mora obravnavati kot „drugotna", čeprav zelo dobrodošla prednost.

  EDPS priporoča izrazitejše razlikovanje med „namenom" in „prednostmi" v besedilu člena I(2) denimo na naslednji način:

  „VIS ima namen z olajšanjem izmenjave podatkov o vlogah za izdajo vizumov in spremljajočih sklepov med državami članicami izboljšati upravljanje skupne vizumske politike, konzularno sodelovanje in posvetovanje med centralnimi konzularnimi oblastmi. Pri tem tudi prispeva …"

([1]) EIA to izrecno navaja (str. 6, §2.7): *neučinkovitost pri boju proti trgovanju z vizumi in goljufijam ter pri izvajanju kontrol povzroča tudi neučinkovitost na področju notranje varnosti držav članic*. To pomeni, da je varnost ogrožena deloma zaradi neučinkovite vizumske politike. Prvi ukrep na tem področju je izboljšanje vizumske politike, predvsem z bojem proti goljufijam in boljšim izvajanjem kontrol. Varnost se bo izboljšala, ko se bo izboljšala vizumska politika.

V zvezi s tem je koristno omeniti tudi, da so „Smernice za vpeljavo skupnega sistema za izmenjavo podatkov o vizumih“, ki ji je sprejel Svet ministrov za pravosodje in notranje zadeve (JHA) dne 13. junija 2002 ([1]), uvrstile preprečitev groženj notranji varnosti na konec seznama. Isto bi lahko storili tudi v tem besedilu, kar bi bilo bistveno bolj v skladu z namenom VIS.

3.3. **Kakovost podatkov**

V skladu s členom 6 Direktive 95/46/ES morajo biti osebni podatki tudi „primerni, ustrezni in ne pretirani glede na namene, za katere se zbirajo in/ali naprej obdelujejo.“ To se nanaša na sorazmernost samega VIS ter na podatke, ki jih je treba zbrati in shraniti v VIS, ter na njihovo nadaljnjo uporabo, kakor tudi na dodatne nadzorne ukrepe, ki sodijo v ta okvir. Ti elementi so ravno tako pomembni za ocenitev predloga v luči člena 8 ECHR.

Vzpostavitev VIS je nedvomno pomemben vmesnik ob izvajanju pravice do zasebnosti, četudi zgolj zaradi svojega obsega in kategorij osebnih podatkov, ki jih obdela. Zato je Delovna skupina iz člena 29 v svojem mnenju št. 7/2004 vprašala, katere študije v obsegu in resnosti teh pojavov, ki bi upravičevale tak pristop, so razkrile nujne razloge za javno varnost ali javni red.

EDPS je skrbno zabeležil dokaze, predstavljene v EIA. Čeprav ti dokazi niso povsem prepričljivi, se zdi, da obstajajo zadostni razlogi za vzpostavitev VIS z namenom izboljšanja skupne vizumske politike.

V tem kontekstu se zdi, da je vzpostavitev VIS kot instrumenta za zboljšanje pogojev za izdajo vizumov s strani držav članic znotraj tolerance zakonodajne oblasti. Takšen sistem bi lahko okrepil in se dobro prilagodil napredni vzpostavitvi območja svobode, varnosti in pravice, kakor je predvideno v Pogodbi ES.

Vendar vzpostavitev in uporaba VIS nikoli ne bi imela takšnega učinka, da na tem področju ne bi bilo moč zagotoviti visoke ravni varstva osebnih podatkov. Med posvetovalne naloge EDPS sodi, da preuči, v kolikšni meri bo VIS vplival na obstoječo raven varstva podatkov o posameznikih, na katere se podatki nanašajo.

V tem smislu se bo EDPS v tem mnenju osredotočil na naslednja vprašanja:

— sorazmernost in natančnost podatkov ter njihova uporaba (npr. kategorije podatkov, dostop do podatkov za vsak posamezen organ in obdobje hrambe);

— delovanje sistema (npr. odgovornosti in varnost);

— pravice posameznikov, na katere se podatki nanašajo (npr. podatki, možnost poprave ali izbrisa nepravilnih ali nepomembnih podatkov);

— nadzor in spremljanje sistema.

Z izjemo naslednjih odstavkov predlog ne daje pomembnih pripomb v zvezi s kategorijami podatkov, ki naj bi bile vključene v VIS, in njihovo uporabo. Zadevne določbe so bile skrbno pripravljene in zdi se, da so kot celota natančne in skladne.

([1]) „Okvirni sklep Sveta z dne 13. junija 2002 o boju proti terorizmu (2002/475/JHA)“, (UL). 22.6.2002, št. L 164, str. 3.

3.4. **Biometrični podatki**

3.4.1. *Vpliv uporabe biometričnih podatkov*

Uporaba biometri čnih podatkov v informacijskih sistemih je zmeraj pomembna izbira, zlasti ko sistem zadeva tako ogromno število posameznikov. Biometrični podatki niso zgolj še ena oblika informacijske tehnologije. Biometrični podatki nepreklicno spremenijo odnos med telesom in identiteto s tem, da značilnosti človeškega telesa prilagodijo v „strojno čitljivo obliko“ in za nadaljnjo uporabo. Tudi če človeško oko ne zna prebrati biometričnih značilnosti, jih je z ustreznimi orodji moč prebrati in uporabiti kadar koli in kjer koli se oseba nahaja.

Čeprav so biometrični podatki koristni za določene namene, bo njihova razširjena uporaba imela močan vpliv na družbo in bi morala biti predmet obsežne ter javne razprave. EDPS navaja, da ta razprava ni bila udejanjena pred oblikovanjem predloga. To le poudarja potrebo po strogih nadzornih ukrepih pri uporabi biometričnih podatkov ter skrbnem premisleku in razpravi v zakonodajnem postopku.

3.4.2. *Posebne značilnosti biometričnih podatkov*

Kakor je bilo že izpostavljeno v številnih mnenjih Delovne skupine iz člena 29 ([1]), je treba vpeljevanje in obdelavo biometričnih podatkov za osebne dokumente podpreti z izrazito skladnimi in resnimi nadzornimi ukrepi. Zaradi nekaterih posebnih značilnosti so biometrični podatki izredno občutljivi.

Drži, da je izguba biometričnih podatkov za zadevno osebo skoraj nemogoča, za razliko od gesla ali ključa. Biometrični podatki nudijo *skoraj popolno razločevanje*, kar pomeni, da ima vsak posameznik edinstvene biometrične podatke. Ti se v teku življenja posameznika skoraj nikoli ne spremenijo, kar tem značilnostim zagotavlja *trajnost*. Vsi imamo enake fizične „elemente“, kar biometričnim podatkom daje *univerzalno* razsežnost.

Preklic biometričnih podatkov pa je skoraj nemogoč: prst ali obraz se težko spremenita. Poleg številnih pozitivnih značilnosti imajo tudi veliko pomanjkljivost v primeru *kraje identitete*: shranjevanje prstnih odtisov in fotografije v podatkovni bazi lahko v povezavi z ukradeno osebno izkaznico privede do resnih težav za dejanskega lastnika te identitete. Zaradi svojih značilnosti biometrični podatki *niso tajni* in lahko celo za seboj *pustijo sledove* (prstni odtisi, DNK), ki omogočajo zbiranje teh podatkov, *ne da bi se njihov lastnik tega zavedal*.

Zaradi teh tveganj, do katerih pride zaradi značilnosti biometričnih podatkov, bodo potrebni pomembni nadzorni ukrepi (zlasti v smislu spoštovanja načela omejitve namena, omejitve dostopa in varnostnih ukrepov).

3.4.3. *Tehnična nepopolnost prstnih odtisov*

Glavne prednosti biometričnih podatkov, kakor so opisane zgoraj (splošnost podatkov, razločevanje, trajnost, uporabnost, itn.), niso nikoli stoodstotne. To neposredno vpliva na učinkovitost postopkov vpisa in preverjanja biometričnih podatkov, ki so načrtovani v uredbi.

Ocenjuje se ([2]), da ne bo moč vpisati do 5 % ljudi (ker nimajo čitljivih prstni odtisov ali jih sploh nimajo). V prilogi predloga je EIA v letu 2007 predvidela približno 20 milijonov prosilcev za vizume, kar pomeni, da se do milijon ljudi ne bo moglo udeležiti „običajnega“ vpisnega postopka, kar bo imelo jasne posledice pri vlogah za vizume in pri kontrolah na mejnih prehodih.

([1]) Mnenje 7/2004 v zvezi z vključitvijo biometričnih podatkov v dovoljenja za prebivanje in vizume, ob upoštevanju vzpostavitve Evropskega vizumskega informacijskega sistema (VIS) (Markt/11487/04/EN - WP 96) in delovni dokument o boimetričnih podatkih (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and CrimePrevention: Usability and Trust in Information Systems*, v„Foresight cybertrust and crime prevention project“. 04/1151, 10. junija 2004, str.7, and Technology Assessment, „Using Biometrics for Border Security“, United States General Accounting Office, GAO-03-174, november 2002.

Identifikacija s pomočjo biometričnih podatkov je po definiciji statistični postopek. Stopnja napak od 0,5 do 1 % je običajna ([1]), kar pomeni, da bo imel kontrolni sistem na zunanjih mejah napačno stopnjo zavrnitve (FRR) od 0,5 do 1 %. To stopnjo uravnava prag, ki je zasnovan na pogojih tveganja pristojnih oblasti (ujema se z ravnovesjem med številom oseb, ki so bile neupravičeno zavrnjene, in tistih, ki so bile neupravičeno sprejete). Zato je pretirano trditi, da bodo te tehnologije ponudile „natančno prepoznavanje" posameznikov, na katere se nanašajo podatki, kakor je navedeno v 9. uvodni izjavi predloga uredbe.

V skladu z nedavno perspektivno raziskavo ([2]), ki jo je naročil odbor LIBE Evropskega parlamenta, bi morali *nadomestni postopki* imeti možnost vključitve nujno potrebnih nadzornih ukrepov za vpeljavo biometričnih podatkov, ker do njih nimajo vsi dostopa in ker niso povsem natančni. Takšne postopke bi bilo treba vpeljati ter uporabljati, da bi spoštovali dostojanstvo ljudi, ki so bili pri postopku vpisa neuspešni, in da nanje ne bi prenesli bremena nepopolnosti sistema. ([3])

EDPS zato priporoča, da se razvijejo nadomestni postopki ter se vključijo v predlog. Ti postopki naj ne bi zmanjšali stopnje varnosti vizumske politike ali zaznamovali posameznike z nečitljivimi prstnimi odtisi.

3.5. **Posebne kategorije podatkov**

Nekatere kategorije podatkov (poleg biometričnih podatkov) je treba posebej obravnavati: podatke, ki so osnova za zavrnitev izdaje vizuma (3.5.1.) in podatke, ki se nanašajo na druge člane skupine (3.5.2).

3.5.1. *Razlogi za zavrnitev izdaje vizuma*

Člen 10(2) predloga določa obdelavo podatkov, ki se nanašajo na razloge za zavrnitev izdaje vizuma. Ti razlogi za zavrnitev so povsem standardizirani.

— Prva dva razloga v pododstavkih (a) in (b) sta bolj upravnega značaja: če prosilec ni predložil veljavnega potovalnega dokumenta ali veljavnih dokumentov, ki dokazujejo namen in pogoje nameravanega bivanja.

— Pododstavek (c) navaja „opozorilo, da obstajajo razlogi, da se prosilcu zavrne vstop", kar vključuje posvetovanje s podatkovno bazo SIS.

— Pododstavek (d) navaja kot razlog za zavrnitev vizuma dejstvo, da prosilec predstavlja „grožnjo javni politiki, notranji varnosti, javnemu zdravju ali mednarodnim odnosom katere koli od držav članic".

([1])

Biometrični podatki	Obraz	Prst	Šarenica
FTE % neuspeh vpisa	ni na voljo	4	7
FNMR % stopnje zavrnitve	4	2,5	6
FMR1 % stopnja napak pri ugotavljanju ujemanj	10	< 0,01	< 0,001
FMR2 % stopnja napak pri prepoznavanju za velikost dB > 1 m	40	0,1	ni na voljo
FMR3 % stopnja napak pri iskanju ujemanj za velikosti dB = 500	12	< 1	ni na voljo

A. K. Jain *et al., Biometrics: A grand Challenge,* Proceedings of International Conference on Pattern Recognition, Cambridge, UK, avgust 2004

([2]) *Biometrics at the frontiers: assessing the impact on Society*, februar 2005, Institute for Prospective Technological Studies, GD Skupno raziskovalno središče, ES.

([3]) *Poročilo o napredku v zvezi z uporabo načel Konvencije 108 o zbiranju in obdelavi biometričnih podatkov*, Svet Evrope, 2005, str 11.

Vse razloge za zavrnitev je treba zaradi posledic, ki jih vključujejo za posameznika, uporabljati z veliko previdnostjo. Nekateri izmed njih, navedeni v pododstavkih (c) in (d), celo vodijo do obdelave „občutljivih podatkov“ v smislu člena 8 Direktive 95/46/ES.

EDPS bi rad bolj izpostavil pogoj v zvezi z javnim zdravjem, ki se zdi nejasen in vključuje obdelavo zelo občutljivih podatkov. V skladu s komentarjem členov, ki je v prilogi, temelji grožnja za javno zdravje na „vzpostaviti kodeksa Skupnosti o predpisih, ki urejajo gibanje oseb preko meja“ (KOM (2004)391 končno).

EDPS se zaveda, da se v zakonodaji Skupnosti v zvezi s prostim gibanjem oseb pogosto in zelo strogo uporablja kriterij „javnega zdravja“, kakor je prikazano v Direktivi 2004/38/EC Evropskega parlamenta in Sveta z dne 29. aprila 2004 v zvezi s pravico državljanov Unije in njihovih družinskih članov, da se prosto gibljejo in prebivajo na ozemlju držav članic. Člen 29 te direktive določa pogoje za upoštevanje grožnje javnemu zdravju: „Bolezni, ki upravičujejo ukrepe omejitve svobode gibanja, so bolezni z možnostjo epidemije, ki so opredeljene v ustreznih pravnih dokumentih Svetovne zdravstvene organizacije, in druge infekcijske bolezni ali kužne parazitske bolezni, če so predmet zaščitnih določb, ki se uporabljajo za državljane države članice gostiteljice.“

— Kljub temu je treba izpostaviti, da je zgoraj navedeni predlog zaenkrat le predlog in da je vključevanje pogoja, da ne gre za grožnjo javnemu zdravju v Uredbi VIS, odvisno od sprejetja kodeksa Skupnosti.

— Če pa bo predlog sprejet, si je treba razlog za zavrnitev vnosa razlagati restriktivno. Predlog kodeksa Skupnosti dejansko temelji na ravnokar omenjeni Direktivi 2004/38/EC.

EDPS zato priporoča, da se v besedilo predloga vnese sklic na člen 29 Direktive 2004/38/ES, da bi zagotovili razumevanje „grožnje javnemu zdravju“ v luči te določbe. V vsakem primeru je treba ob upoštevanju občutljivosti podatkov slednje obravnavati le, če je grožnja javnemu zdravju pristna, prisotna in dovolj resna.

3.5.2. *Podatki o drugih članih skupine*

Člen 2(7) določa „člane skupine“ kot „druge prosilce, s katerimi prosilec potuje, vključno z zakoncem in njunimi otroki“. V komentarju členov je navedeno, da se opredelitve v členu 2 predloga nanašajo na Pogodbo ali schengenski pravni red v zvezi z vizumsko politiko, razen nekaterih izrazov, vključno s „člani skupine“, ki so opredeljeni posebej za namene te uredbe. Zato je moč sklepati, da se ta opredelitev ne nanaša na opredelitev „skupinskega vizuma“, kakor je navedena v členu 2.1.4. v skupnih konzularnih navodilih. Komentar členov se nanaša na „prosilce, ki potujejo v skupini z drugimi prosilci, npr. v okviru sporazuma ADS, ali skupaj z družinskimi člani.“

EDPS poudarja, da je v Uredbi treba navesti natančno in razumljivo opredelitev „članov skupine“. V trenutnem predlogu EDPS ugotavlja, da je opredelitev preveč ohlapna zaradi nenatančnega sklicevanja na Pogodbo ali schengenski pravni red. V tem pomenu lahko besedna zveza „člani skupine“ vključuje tudi sodelavce, druge stranke iste potovalne agencije, ki so udeleženci organiziranega izleta, itn. Posledice so zelo pomembne:

v skladu s členom 5 osnutka uredbe se bo vloga vlagatelja povezala s podatki o vlogah drugih članov skupine.

3.6. **Hramba podatkov**

Člen 20 osnutka uredbe določa petletno obdobje hrambe vsake vloge. Gre za politično odločitev zakonodaje Skupnosti, da zagotovi ustrezno časovno omejitev.

Ni dokazov – zlasti ne v luči razlogov, omenjenih v komentarjih členov –, da je izbor politike v tem predlogu nesmiseln ali ima nesprejemljive posledice, pod pogojem, da se uvedejo vsi ustrezni mehanizmi popravkov. To pomeni, da je treba zagotoviti popravek ali izbris podatkov, ko slednji več niso pravilni in predvsem ko je oseba dobila državljanstvo države članice ali dobila status, ki ne zahteva njene vključitve v sistem.

Ko so podatki še v sistemu, ne smejo v nobenem primeru vplivati na novo določitev. Nekateri razlogi za zavrnitev (ukrep zoper prosilca v zvezi z zavrnitvijo vstopa, predvsem grožnja javnemu zdravju) imajo časovno omejeno veljavnost. Če so v preteklosti obstajali utemeljeni razlogi za zavrnitev vstopa, to naj ne bi vplivalo na novo odločitev. Situacijo je treba v celoti vnovič oceniti za vsako prošnjo za izdajo vizuma, kar je treba izrecno poudariti v uredbi, kjer je to potrebno.

3.7. **Uporaba in dostop do podatkov**

3.7.1. *Predhodne pripombe*

V predhodni opombi se EDPS zaveda skrbi, ki je bila očitno posvečena upravnemu sistemu za dostop in uporabo podatkov VIS. Vsak organ ima dostop do različnih podatkov za različne namene. To je ustrezen pristop, ki ga EDPS le podpira. Cilj naslednjih pripomb je uporaba tega pristopa v najširšem možnem smislu.

3.7.2. *Kontrole vizumov na zunanjih mejnih prehodih ter znotraj ozemlja*

Pri kontrolah vizumov na zunanjih mejah člen 16 predlagane uredbe jasno navaja dva natančna namena:

— „preverjanje istovetnosti osebe“, kar glede na dano opredelitev pomeni primerjavo „ena na ena“:

— „preverjanje verodostojnosti vizuma“. Kakor je predlagano v standardih ICAO, bi lahko mikročip v vizumu lahko uporabljal javni/zasebni ključ (PKI), da bi preveril istovetnost podatkov.

Ta namena se lahko v celoti dosežeta z izključnim dostopom do zaščitenega mikročipa s strani pooblaščenega organa za izvajanje kontrol vizumov. Dostop do centralne podatkovne baze VIS bi bil potemtakem v tem posebnem primeru nesorazmeren. Pri slednji možnosti bi bilo z VIS povezanih več organov, s čimer bi se povečalo tveganje zlorab. To je morda tudi dražja rešitev, ker se bo število varnih in nadzorovanih dostopov do VIS in potreba po posebnem urjenju, povezanim s slednjim, prav tako bistveno povečala.

Obstajajo tudi dvomi o natančnosti dostopa do podatkov, kakor je predvideno v drugi točki člena 16. V odstavku (2)(a) je res navedeno, da če se po prvi poizvedbi zdi, da so podatki o prosilcu zapisani v VIS (kar bi naj načeloma veljalo), si lahko pristojni organ ogleda druge podatke, vendar še zmeraj z namenom preverjanja istovetnosti. Ti podatki vsebujejo vse informacije v zvezi z vlogo, fotografije in prstne odtise, kakor tudi vse predhodno izdane, razveljavljene, preklicane ali podaljšane vizume.

Če je preverjanje istovetnosti uspešno, ni jasno, zakaj so preostali podatki še potrebni. Dostop do njih bi moral biti dejansko mogoč le ob omejevalnih ukrepih in če so postopki preverjanja istovetnosti neuspešni. V tem primeru bi podatki, navedeni v členu 16(2), ustrezno prispevali k nadomestnemu postopku, ki bi pomagal pri preverjanju istovetnosti osebe. Dostopa do njih ne bi smel imeti vsak član osebja na mejnih kontrolnih točkah, temveč le uradniki, ki preučujejo težavne primere.

Opredelitev organov, ki imajo dostop, bi morala biti natančnejša. Predvsem ni jasno, kateri so „organi, ki so pristojni za kontrolo znotraj ozemlja države članice“. EDPS predvideva, da gre za organe, pristojne za izvajanje kontrol *vizumov*, člen 16 pa bi bilo treba v tem smislu spremeniti.

3.7.3. *Uporaba podatkov za preverjanje istovetnosti in vračanje ilegalnih priseljencev ter za azilne postopke*

V primerih, opisanih v členih 17, 18 in 19 (vračanje ilegalnih priseljencev in azilni postopek), se VIS uporablja za namen preverjanja istovetnosti. Med podatke, ki jih je moč uporabiti v namene preverjanja istovetnosti, sodijo fotografije. Ob upoštevanju trenutne ravni razvitosti tehnologije na področju samodejnega prepoznavanja obrazov za tako obsežne sisteme IT, fotografij ni moč uporabiti za namene preverjanja istovetnosti (načelo *„one-to-many“*); ne morejo namreč zagotoviti zanesljivega rezultata. Zaradi tega se ne upoštevajo kot podatki, ustrezni za namene preverjanja istovetnosti.

Zato EDPS posledično močno priporoča, da se „fotografije“ črtajo iz prvega dela teh členov ter ohranijo v drugem delu (fotografije se lahko uporabijo kot orodje za preverjanje istovetnosti osebe, vendar ne kot orodje za preverjanje istovetnosti v veliki podatkovni bazi).

Druga možnost je sprememba člena 36 v smislu, da se bodo funkcije za obdelavo fotografij za namene preverjanja istovetnosti uporabile le, ko bo ta tehnologija veljala za zanesljivo (verjetno po posvetovanju s tehničnim odborom).

3.7.4. *Objava organov, ki imajo dostop*

Člen 4 osnutka uredbe določa objavo v Uradnem listu Evropske unije v zvezi s pristojnimi organi, določenimi v vsaki državi članici, ki imajo dostop do VIS. Ti organi bi morali biti objavljeni na redni (letni) osnovi, z namenom obveščanja o spremembah na nacionalni ravni. EDPS poudarja pomembnost te objave, ki je nepogrešljivo orodje za nadzor, tako na evropski kot nacionalni ali lokalni ravni.

3.8. **Odgovornosti**

Spomnimo se, do bo VIS temeljil na centralizirani arhitekturi s centralno podatkovno bazo, kjer bodo shranjeni vsi podatki v zvezi z vizumi in kjer bodo nacionalni vmesniki v državah članicah, s pomočjo katerih bodo pristojni organi imeli dostop do centralnega sistema. V skladu z uvodnima izjavama (14) in (15) osnutka uredbe, bo Direktiva 95/46/ES za obdelavo osebnih podatkov s strani držav članic veljala ob uporabi uredbe, Uredba 45/2001 pa bo veljala za dejavnosti Komisije, ki zadevajo varstvo osebnih podatkov. Kakor navedeno v uvodnih izjavah, je cilj predloga razjasnitev določenih točk, med drugim ob upoštevanju odgovornosti za uporabo podatkov in nadzora nad varstvom podatkov.

Dejansko se zdi, da se te točke nanašajo na podrobnosti ključnega pomena, brez katerih se sistem nadzornih ukrepov iz Direktive 95/46/EC in Uredbe 45/2001 ne bi uporabljal ali se ne bi v celoti ujemal s predlogom. Veljavnost nacionalne zakonodaje v skladu z Direktivo običajno predvideva upravljavca, ki se ustanovi v zadevni državi članici (člen 4), medtem ko je veljavnost Uredbe odvisna od obdelave osebnih podatkov s strani institucije ali telesa Skupnosti pri izvajanju dejavnosti, ki so v celoti ali deloma v okviru prava Skupnosti (člen 3).

V skladu s členom 23(2) osnutka uredbe so „podatki v imenu držav članic obdelani v VIS“. V skladu s členom 23(3) države članice določijo organe, ki veljajo za upravljavce v skladu s členom 2(d) Direktive 95/46/ES. Iz tega je moč sklepati, da bi v skladu s sistemom Direktive Komisija morala biti obdelovalec. To je potrjeno v Obrazložitvi členov ([1]).

Izražanje v takšni obliki ne izraža v zadostni meri zelo pomembne in dejansko ključne vloge Komisije, tako v razvojni fazi sistema kot pri njegovem običajnem delovanju. Vlogo Komisije je težko natančno povezati s konceptom upravljavca ali obdelovalca; bodisi gre za obdelovalca z nenavadnimi pooblastili (med drugim tudi kar zadeva oblikovanje sistema) ali upravljavca z omejitvami (ker podatke vnašajo in uporabljajo države članice). Komisija ima v VIS položaj, ki ga je treba priznati kot *sui generis* ([2]).

To pomembno vlogo je treba priznati s celovitim opisom nalog Komisije in ne z ubeseditvijo, ki ne ustreza dejanskemu stanju, ker je preveč omejevalna, ne spreminja ničesar v delovanju VIS in le povzroča zmedo. To je pomembno tudi za doseganje doslednega in učinkovitega nadzora VIS (glej tudi odstavek 3.11). Zato EDPS priporoča črtanje člena 23(2).

EDPS bi rad poudaril, da je popoln opis nalog Komisije, kar zadeva VIS, toliko pomembnejši, če Komisija načrtuje zaupati upravljanje drugemu organu. V „Fiche Financičre“, ki je v prilogi, je omenjena možnost prenosa nalog na Agencijo za zunanje meje. V tem okviru je izrednega pomena, da Komisija ne pusti nobenih dvomov v zvezi z njenimi pooblastili, na osnovi česar bi njen naslednik poznal meje, znotraj katerih lahko ukrepa.

3.9. **Varnost**

Upravljanje in spoštovanje optimalne stopnje varnosti za VIS vsebuje predpogoj za zagotavljanje potrebne zaščite osebnih podatkov, shranjenih v podatkovni bazi VIS. Da bi zagotovili to zadovoljivo stopnjo zaščite, je treba vpeljati resne nadzorne ukrepe za ravnanje z morebitnimi tveganji, povezanimi z infrastrukturo sistema in vpletenimi osebami. Ta zadeva je predmet razprave v različnih delih predloga in jo je treba izboljšati.

Člena 25 in 26 predloga vsebujeta različne ukrepe za varstvo podatkov in izrecno navajata oblike zlorab, ki jih je treba preprečiti. Te določbe bi lahko na drugi strani koristno dopolnili z ukrepi za sistematičen nadzor in poročanje v zvezi z učinkovitostjo že omenjenih varnostnih ukrepov. EDPS natančneje priporoča, naj se tema členoma dodajo določbe v zvezi s sistematičnim (samo)revidiranjem varnostnih ukrepov.

To je povezano s členom 40 predloga, ki zagotavlja nadzor in ocenjevanje. To naj ne bi zadevalo zgolj vidikov rezultata, racionalnosti in kakovosti storitev, ampak tudi izpolnjevanje zakonskih zahtev, zlasti na področju varovanja podatkov. EDPS zato priporoča, da se okvir člena 40 razširi na nadzor in poročanje v zvezi z zakonitostjo obdelave.

Členu 24(4)(c) ali členu 26(2)(e) v zvezi s pravilno pooblaščenim osebjem, ki ima dostop do podatkov, je treba poleg tega dodati, da naj bi države članice zagotovile razpoložljivost natančnih profilov uporabnikov (ti profili naj bi bili na razpolago za kontrole nacionalnim nadzornim organom). Poleg profilov uporabnikov morajo države članice pripraviti in nenehno posodabljati popoln seznam istovetnosti uporabnikov. Enako velja za Komisijo: člen 25(2)(b) je treba dopolniti na enak način.

([1]) Glejte stran 37 predloga.

([2]) Čeprav opredelitev upravljavca v Direktivi 95/46/ES in Uredbi 45/2001 določa tudi možnost več upravljavcev z različnimi odgovornostmi.

Varnostni ukrepi so dopolnjeni z nadzorom in organizacijskimi nadzornimi ukrepi. Člen 28 predloga opisuje pogoje in namene, za katere je treba hraniti zapise vseh procesov obdelave podatkov. Ti zapisi se ne shranjujejo le zaradi nadzora nad varstvom podatkov in zagotavljanja varstva podatkov, ampak tudi zaradi rednega samorevidiranja VIS. Poročila samorevidiranja bodo prispevala k učinkovitemu izvajanju nalog nadzornih organov, ki bodo prepoznali najšibkejše točke ter se nanje osredotočili pri svojem procesu revidiranja.

3.10. **Pravice posameznika, na katerega se podatki nanašajo**

3.10.1. *Obveščanje posameznika, na katerega se podatki nanašajo*

Posredovanje podatkov posamezniku, na katerega se podatki nanašajo, je za zagotovitev poštene obdelave ključnega pomena. To predstavlja nepogrešljiv nadzorni ukrep za pravice posameznika. Člen 30 predloga v ta namen zdaj dejansko sledi členu 10 Direktive 95/46/ES.

Toda ta določba bi lahko imela korist od nekaterih sprememb, tako da bi se bolje ujemala z okvirjem VIS. Direktiva sicer določa, da se nekateri podatki posredujejo, vendar dovoljuje posredovanje več informacij, če je to potrebno ([1]). Posledično naj bi se člen 30 spremenil, da bi lahko vključili naslednje točke:

— Posameznike, na katere se podatki nanašajo, je treba prav tako obvestiti o obdobju hrambe njihovih podatkov.

— Člen 30(1)(e) zadeva „pravico do dostopa in spreminjanja podatkov." Pravilnejša ubeseditev bi bila „pravico do dostopa in pravico do *zahtevanja* spreminjanja *ali izbrisa* podatkov." V tem pogledu bi bilo treba posameznike, na katere se podatki nanašajo, obvestiti o možnosti, da zaprosijo za nasvet ali pomoč pri pristojnih nadzornih organih.

— Končno člen 30(1)(a) navaja podatke o istovetnosti upravljavca in njegovega predstavnika, če ta obstaja. Ker se upravljavec zmeraj nahaja na ozemlju Evropske unije, ni potrebe po predvidevanju slednje možnosti.

3.10.2. *Pravica do dostopa, popravka in izbrisa*

Zadnji stavek v členu 31(1) navaja, da „tak dostop do podatkov lahko odobri zgolj država članica." Lahko se domneva, da to pomeni, da dostop do (ali posredovanje) podatkov ne more odobriti centralna enota, ampak vsaka država članica. EDPS priporoča, da se izrecno navede, da se za takšno posredovanje lahko zaprosi v vsaki državi članici.

Poleg tega kaže besedilo te določbe na to, da dostopa ni moč zavrniti ter da se ta podeli brez pooblastila odgovorne države članice. To razlaga, zakaj morajo nacionalni organi sodelovati, da bi uveljavljali pravice iz člena 31(2), (3) in (4), vendar ne člena 31(1) ([2]).

3.10.3. *Podpora s strani nadzornih organov*

Člen 33(2) določa obveznost nacionalnih nadzornih organov zadevni osebi s svojo prisotnostjo pomagati in svetovati skozi celotno trajanje postopkov (na sodišču). Pomen tega odstavka ni jasen. Nacionalni nadzorni organi imajo različne odnose do svoje vloge med sodnimi postopki. To zveni, kot da morajo biti v vlogi pravnega zastopnika pritožnika na sodišču, kar v številnih državah ni mogoče.

([1]) Omenja *„vsaj naslednje informacije (…), kolikor so take nadaljnje informacije potrebne, ob upoštevanju posebnih okoliščin, v katerih se podatki zbirajo, za zagotovitev poštene obdelave glede na posameznika, na katerega se osebni podatki nanašajo"*.

([2]) Posledično bi lahko člen 31(3), ki govori o sodelovanju med nacionalnimi organi pri uveljavljanju pravice do popravka ali izbrisa, spremenili v tem smislu, da bi postal jasnejši: „če je bila zahteva, *kot je omenjeno v 31(2)*". Zahteve, ki so omenjene v 31(1) (dostop) ne vključujejo sodelovanja med organi.

3.11. **Nadzor**

Predlog deli nadzorne naloge med nacionalne nadzorne organe in EDPS. To se ujema s pristopom predloga k ustreznemu pravnemu redu in odgovornosti za delovanje in uporabo VIS ter s potrebo po učinkovitem nadzoru. EDPS zato *pozdravlja ta pristop* v členih 34 in 35.

Nacionalni nadzorni organi nadzorujejo zakonitost obdelave osebnih podatkov s strani držav članic, *vključno z njihovim prenosom v in iz VIS*. EDPS nadzoruje dejavnosti Komisije, kamor sodi tudi *(…) da se osebni podatki med nacionalnimi vmesniki in centralnim vizumskim informacijskim sistemom zakonito prenašajo*. Posledično lahko pride do prekrivanja, ker sta tako nacionalni nadzorni organ kot EDPS sočasno odgovorna za nadzor zakonitosti prenosa podatkov med nacionalnimi vmesniki in centralnim vizumskim informacijskim sistemom.

EDPS zato predlaga spremembo člena 34, da bi pojasnili, da nacionalni nadzorni organi nadzorujejo zakonitost obdelave osebnih podatkov s strani držav članic, vključno z njihovim prenosom v in iz nacionalnega vmesnika VIS.

Kar zadeva nadzor nad VIS, je pomembno tudi poudariti, da bi bilo treba nadzorne dejavnosti nacionalnih nadzornih organov in EDPS uskladiti do določene mere, z namenom zagotoviti zadostno stopnjo doslednosti in celotne učinkovitosti. Dejansko obstaja potreba po usklajenem izvajanju Uredbe ter po približevanju k skupnemu pristopu za reševanje skupnih težav. Kar zadeva varnost, se lahko celo doda, da bo raven varnosti VIS končno opredeljena z ravnijo varnosti svojega najšibkejšega člena. V zvezi s tem je treba tudi strukturirati in okrepiti sodelovanje med EDPS in nacionalnimi organi. Člen 35 mora zato vsebovati določbo, v skladu s katero EDPS vsaj enkrat letno skliče sestanek z vsemi nacionalnimi nadzornimi organi.

3.12. **Izvajanje**

Člen 36(2) predloga določa: *„Ukrepi, ki so potrebni za tehnično izvajanje procesov iz odstavka 1, se sprejmejo v skladu s postopkom iz člena 39(2).“* Člen 39 se nanaša na odbor, ki nudi pomoč Komisiji in ki je bil ustanovljen decembra 2001 ([1]) ter bil uporabljen pri številnih instrumentih.

Tehnična izvedba funkcij VIS (medsebojno vplivanje s pristojnimi organi in enotna oblika vizumov) predstavlja številne morebiti vprašljive učinke na varstvo podatkov. Tako bo denimo odločitev, ali naj se mikročip vključi v vizume ali ne, ki bo vplivala na način uporabe centralne podatkovne baze, kakor tudi na standard uporabljenega formata za izmenjavo biometričnih podatkov, usmerjala ali oblikovala zadevno politiko o varstvu podatkov ([2]).

Izbor tehnologij bo odločilno vplival na pravilno izvajanje načel namena in sorazmernosti in bi ga bilo treba nadzorovati. Zato je treba tehnološke odločitve, ki močno vplivajo na varstvo podatkov, po možnosti sprejeti z Uredbo, v skladu s postopkom soodločanja. Le na ta način se lahko zagotovi potreben politični nadzor. V vseh drugih primerih, kjer gre za vpliv na varstvo podatkov, mora EDPS imeti možnost svetovanja pri odločitvah tega odbora.

3.13. **Interoperabilnost**

Interoperabilnost je pomemben in odločilen predpogoj za učinkovitost velikih sistemov IT, kakršen je VIS. Nudi možnost zmanjšanja celotnih stroškov na skladen način, da bi se izognili naravnim presežkom heterogenih elementov. Interoperabilnost lahko tudi prispeva k doseganju cilja skupne vizumske politike z izvajanjem enakega postopkovnega standarda pri vseh sestavnih elementih te politike. Vendar je pomembno razlikovati med dvema ravnema interoperabilnosti:

— Interoperabilnost med državami članicami EU je močno zaželena; vloge za izdajo vizumov, ki jih pošljejo organi države članice, morajo biti interoperabilne z vlogami, ki jih pošljejo organi druge države članice.

([1]) Uredba Sveta št. 2424/2001 z dne 6. decembra 2001 o razvoju druge generacije Schengenskega informacijskega sistema (SIS II).

([2]) Predlog uredbe Sveta za spremembo Uredbe (ES)1683/95 (enotna oblika za VIZUME) iz septembra 2003 je vseboval podoben člen.

— Interoperabilnost med sistemi, zgrajenimi za različne namene, ali s sistemi tretjih držav, je bistveno bolj vprašljiva.

Med nadzornimi ukrepi, ki so na voljo za omejitev namena sistema in preprečitev *„function creep“* (postopna širitev področja uporabe sistema), lahko uporaba različnih tehnoloških standardov prispeva k tej omejitvi. Dejansko je treba vsako interakcijo med dvema različnima sistemoma natančno zabeležiti. Interoperabilnost naj ne bi nikoli pripeljala do položaja, kadar lahko organ, ki ni pooblaščen za dostop ali uporabo določenih podatkov, dobi dostop prek drugega informacijskega sistema.

V zvezi s tem EDPS omenja deklaracijo Sveta z dne 25. marca 2004 o boju proti terorizmu, v kateri se Komisija poziva, naj predstavi predloge za povečanje interoperabilnosti ter sinergij med informacijskimi sistemi (SIS, VIS in Eurodac).

EDPS bi rad tudi omenil potekajočo razpravo o tem, kateremu organu bi v prihodnje zaupali upravljanje različnih velikih sistemov (glej tudi odstavek 3.8 tega mnenja).

EDPS vnovič poudarja, da interoperabilnosti med sistemi ni moč izvesti s kršitvijo načela omejitve namena in da je treba vsak predlog v zvezi s tem posredovati njemu.

4. **SKLEPI**

4.1. **Splošne točke**

1. EDPS priznava, da je za nadaljnji razvoj skupne vizumske politike potrebna učinkovita izmenjava ustreznih podatkov. Eden izmed mehanizmov, ki lahko zagotovi nemoten pretok podatkov, je VIS. EDPS je skrbno zabeležil dokaze, predstavljene v EIA. Čeprav ti dokazi niso povsem prepričljivi, se zdi, da obstajajo zadostni razlogi za vzpostavitev VIS z namenom izboljšanja skupne vizumske politike.

   Toda ta nov instrument je treba omejiti na zbiranje in izmenjavo podatkov, kolikor sta takšno zbiranje ali izmenjava potrebna za razvoj skupne vizumske politike ter sorazmerna s tem ciljem.

2. Vzpostavitev VIS lahko ugodno učinkuje na druge zakonite javne interese, kar pa ne spreminja namena VIS. Zato morajo biti vsi elementi VIS potrebni in sorazmerni instrumenti za doseganje cilja zgoraj omenjene politike. Ob tem:

   — rutinski dostop organov pregona ne bi bil v skladu s tem namenom.

   — EDPS priporoča izrazitejše razlikovanje med „namenom“ in „prednostmi“ v besedilu člena 1(2):

   — interoperabilnosti med sistemi ni moč izvesti s kršitvijo načela omejitve namena.

3. EDPS se zaveda prednosti uporabe biometričnih podatkov, vendar izpostavlja močan vpliv uporabe takšnih podatkov ter predlaga vnos strogih nadzornih ukrepov pri uporabi biometričnih podatkov. Zaradi tehnične nepopolnosti prstnih odtisov je treba razviti celo nadomestne postopke ter jih vključiti v predlog.

4. Trenutno mnenje je treba omeniti v preambuli Uredbe pred uvodnimi izjavami („ob upoštevanju mnenja …“).

4.2. **Ostalo**

5. Kar zadeva razloge za zavrnitev izdaje vizuma: v besedilo predloga naj bi se vnesel sklic na člen 29 Direktive 2004/38/ES, da bi zagotovili razumevanje „grožnje javnemu zdravju“ v luči te določbe.

6. Podatki o članih skupine imajo v predlogu poseben pomen: zato je treba navesti natančno in razumljivo opredelitev „članov skupine“.

7. Ni dokazov, da je izbor politike v tem predlogu v zvezi s podaljšanjem obdobja hrambe podatkov nesmiseln ali da bi imel nesprejemljive posledice, pod pogojem, da se uvedejo vsi ustrezni mehanizmi popravkov.

   V predlogu je treba izrecno navesti, da je treba osebne podatke v celoti vnovič oceniti za vsako prošnjo za izdajo vizuma.

8. Kar zadeva kontrolo vizumov na zunanjih mejah: člen 16 predloga je treba spremeniti, ker bi bil dostop do centralne podatkovne baze VIS v teh primerih nesorazmeren. Zadostuje izključni dostop do zaščitenega mikročipa s strani pooblaščenega organa za izvajanje kontrol vizumov.

   Če je preverjanje istovetnosti uspešno, ni jasno, zakaj so preostali podatki še potrebni.

9. Kar zadeva uporabo podatkov za preverjanje istovetnosti in vračanje ilegalnih priseljencev ter za azilne postopke: „fotografije“ je treba črtati iz prvega dela členov 17, 18 in 19 ter ohraniti v drugem delu.

10. Kar zadeva odgovornosti Komisije in držav članic: člen 23(2) je treba črtati.

11. Predlogu je treba dodati določbe v zvezi s sistematičnim (samo)revidiranjem varnostnih ukrepov. Okvir člena 40 je treba razširiti na nadzor in poročanje v zvezi z zakonitostjo obdelave. Še več:

   — Države članice morajo pripraviti in nenehno posodabljati popoln seznam istovetnosti uporabnikov. Enako velja za Komisijo: člen 25(2) bi bilo treba dopolniti na enak način.

   — Člen 28 predloga opisuje pogoje in namene, za katere je treba hraniti zapise vseh procesov obdelave podatkov. Ti zapisi se ne shranjujejo le zaradi nadzora nad varstvom podatkov in zagotavljanja varnosti podatkov, ampak tudi zaradi rednega samorevidiranja VIS.

12. Kar zadeva pravice osebe, na katero se podatki nanašajo:

   — Člen 30 je treba spremeniti, da bi zagotovili, da se posamezniki, na katere se podatki nanašajo, prav tako obvestijo o obdobju hrambe njihovih podatkov.

   — Člen 30(1)(e) naj omenja „pravico do dostopa in pravico do zahtevanja spreminjanja ali izbrisa podatkov.“

   — Člen 31(1) mora izrecno navesti, da se za nekatera posredovanja lahko zaprosi v vsaki državi članici.

13. Kar zadeva nadzor:

— Člen 34 bi bilo treba spremeniti, da bi pojasnili, da nacionalni nadzorni organi nadzorujejo zakonitost obdelave osebnih podatkov s strani držav članic, vključno z njihovim prenosom v nacionalni vmesnik VIS in iz njega.

— Člen 35 naj bi zato vseboval določbo, v skladu s katero EDPS vsaj enkrat letno skliče sestanek z vsemi nacionalnimi nadzornimi organi.

14. Kar zadeva izvajanje:

— Tehnološke odločitve, ki močno vplivajo na varstvo podatkov, je po možnosti treba sprejeti z Uredbo, v skladu s postopkom soodločanja.

— V drugih primerih naj bi EDPS imel možnost svetovanja pri odločitvah odbora, ki ga predvideva predlog.

V Bruslju, dne 23. marca 2005

Peter HUSTINX

Evropski nadzornik za varstvo podatkov