# EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

**Mnenje Evropskega nadzornika za varstvo podatkov o predlogu sklepa Sveta o dostopu organov držav članic, odgovornih za notranjo varnost, in Europola do Vizumskega informacijskega sistema (VIS) za iskanje podatkov v namen preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj (COM (2005) 600 konč.)**

(2006/C 97/03)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE —

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

ob upoštevanju Listine o temeljnih pravicah Evropske unije 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 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 ter zlasti člena 41 Uredbe,

ob upoštevanju zaprosila za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki ga je 29. novembra 2005 prejel od Komisije —

SPREJEL NASLEDNJE MNENJE:

## 1. **UVOD**

### 1.1. **Uvodna pripomba**

Komisija je 24. novembra 2005 Evropskemu nadzorniku za varstvo podatkov (EDPS) pismeno poslala predlog sklepa Sveta o dostopu organov držav članic, odgovornih za notranjo varnost, in Europola do Vizumskega informacijskega sistema (VIS) za iskanje podatkov v namen preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj (v nadaljevanju „predlog“). Evropski nadzornik za varstvo podatkov (EDPS) je pismo razumel kot zaprosilo, da institucijam in organom Skupnosti svetuje v skladu s členom 28(2) Uredbe (ES) št. 45/2001. EDPS meni, da je treba pričujoče mnenje omeniti v preambuli Sklepa.

Po mnenju EDPS je pomembno, da o tej občutljivi temi poda mnenje, saj ta predlog izvira neposredno iz vzpostavitve VIS, ki ga bo EDPS nadzoroval in o katerem je 23. marca 2005 [1] podal mnenje. Domneva o dostopu organov pregona je bila v tem mnenju že predvidena (glej spodaj); oblikovanje novih pravic za dostop do VIS ima odločilen vpliv na sistem, in sicer z vidika varstva podatkov. Zato je oblikovanje mnenja o sedanjem predlogu obvezno nadaljevanje prvega mnenja.

### 1.2. **Pomen predloga**

a) *Okvir*

Sedanji predlog je pomemben sam po sebi, pa tudi zato, ker izhaja iz splošne usmeritve, da se organom pregona dovoli dostop do nekaterih velikih informacijskih sistemov in sistemov preverjanja istovetnosti. To je med drugim navedeno v sporočilu Komisije z dne 24. novembra 2005 o izboljšani učinkovitosti, povečani interoperabilnosti in sinergijah med evropskimi zbirkami podatkov na področju pravosodja in notranjih zadev [2], zlasti v točki 4.6 tega sporočila: „*V zvezi s ciljem boja proti terorizmu in kriminalu Svet sedaj ugotavlja, da pomanjkanje dostopa organov za notranjo varnost do podatkov VIS pomeni pomanjkljivost. Enako velja za vse podatke o priseljevanju SIS II in podatke EURODAC*“.

Zato se sedanji predlog lahko obravnava kot predhodnik podobnih pravnih instrumentov, oblikovanih v okviru drugih zbirk podatkov, in je odločilen za opredelitev primerov od samega začetka, v katerih je ta dostop lahko dopusten.

---

[1] 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 (COM(2004) 835 konč.).

[2] COM(2005) 597 konč.

b) *Vpliv novega dostopa do VIS*

EDPS se vsekakor zaveda potrebe, da organi pregona izkoristijo najboljša možna orodja za preverjanje istovetnosti storilcev terorističnih dejanj ali drugih hudih kaznivih dejanj. Prav tako se zaveda, da lahko podatki VIS tem organom v nekaterih okoliščinah predstavljajo pomemben vir informacij.

Vseeno pa je zelo pomembna odobritev dostopa organom pregona do zbirk podatkov prvega stebra, ne glede na to, kako upravičena je z vidika boja proti terorizmu. Upoštevati je treba, da je VIS informacijski sistem, ki je bil oblikovan za uporabo evropske vizumske politike in ne kakor sredstvo kazenskega pregona. Rutinski dostop bi resnično predstavljal resno kršitev načela omejitve namena. Povzročil bi nesorazmerni poseg v zasebnost potnikov, ki so privolili v obdelavo podatkov za pridobitev vizuma in ki pričakujejo, da se bodo njihovi podatki zbirali, posredovali in se bo v te podatke izvajal vpogled le v ta namen.

Ker so informacijski sistemi oblikovani za posebni namen, ki določa varnostne ukrepe, zaščito in pogoje za dostop, bi odobritev sistematičnega dostopa za namen, ki je drugačen od prvotnega, ne le kršila načelo omejitve namena, temveč bi zaradi tega lahko postali omenjeni elementi tudi neprimerni in pomanjkljivi.

Enako bi takšna pomembna sprememba sistema lahko razveljavila rezultate študije o presoji vplivov (ki je obravnavala uporabo sistema le za prvotni namen). Enako velja za mnenja organov za varstvo podatkov. O tem, da novi predlog spreminja osnovo njihove analize skladnosti, je mogoče razpravljati.

c) *Stroga omejitev tega dostopa*

Glede na zgornje pripombe želi EDPS poudariti, da se dostop organom pregona do VIS lahko dovoli le v posebnih okoliščinah, za vsak primer posebej, spremljati pa ga morajo stregi varnostni ukrepi. Povedano drugače, vpogled organov pregona mora biti z ustreznimi tehničnimi in pravnimi sredstvi omejen na posebne primere.

To je EDPS v svojem mnenju o VIS že poudaril: *„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 varnostnih ukrepov pa se sistematični dostop ne sme dovoliti“.*

Osnovne zahteve se na koncu lahko povzamejo na naslednji način:

— Sistematični dostop se ne sme odobriti: Sklep mora zagotoviti, da organi iz tretjega stebra kadar koli in za vsak primer posebej preverijo potrebo do dostopa in njegovo sorazmernost. V povezavi s tem je bistvenega pomena natančno besedilo pravnega instrumenta, da se preprečijo obsežne razlage, ki bi vodile do rutinskega dostopa.

— Kadar je dostop dovoljen, pa je treba ob upoštevanju občutljive narave tega dostopa sprejeti ustrezne varnostne ukrepe in pogoje, vključno z obsežnim sistemom varstva podatkov za nacionalno uporabo podatkov.

### 1.3 **Prvotne pripombe**

EDPS priznava, da je bila v tem predlaganem instrumentu precejšnja pozornost namenjena varstvu podatkov, predvsem na področju omejevanja dostopa do posebnih primerov in le v okviru boja proti hudim kaznivim dejanjem ([1]).

EDPS želi poleg drugih pozitivnih strani omeniti zlasti:

— omejitev na nekatere oblike kaznivih dejanj iz Konvencije o Europolu;

— obveznost držav članic, da pripravijo seznam organov, ki imajo dostop, in te sezname objavijo;

— obstoj osrednje točke dostopa za države članice (in posebej usposobljene enote znotraj Europola), ki bi omogočala boljše presojanje zahtev za dostop in boljši nadzor;

— stroga pravila o nadaljnjem posredovanju podatkov iz člena 8(5) predloga;

— obveznost za države članice in Europol, da vodijo evidenco o osebah, ki so odgovorne za vpogled v podatke.

## 2. **ANALIZA PREDLOGA**

### 2.1. **Uvodna pripomba**

Da bi se dostop organom iz tretjega stebra odobril, mora glavni predlog o VIS prvega stebra zagotoviti premostitveno klavzulo, ki bi predvsem določila možno vsebino pravnega instrumenta tretjega stebra, kakor je ta predlog. Premostitvena klavzula v času, ko je EDPS predložil svoje mnenje o VIS, še ni bila uvedena, zato EDPS o njej ni mogel podati pripomb. Zato so vse naslednje pripombe podane s pridržkom glede na vsebino premostitvene klavzule.

([1]) To je tudi v skladu s sklepi Sveta iz marca in julija 2005, v katerih je zahtevano, da se organom za notranjo varnost odobri dostop do VIS *„ob upoštevanju strogega izpolnjevanja pravil o varstvu osebnih podatkov“.*

### 2.2 **Namen dostopa**

Pomembno je, da se skrbno opredelijo pogoji za dostop do VIS in se tako zagotovi primerna omejitev dostopa. Zaželeno je, da poleg predlaganega sklepa, obrazložitveni memorandum in uvodne izjave (glej predvsem uvodno izjavo 7) jasno navedejo, da je namen omogočiti dostop le za vsak primer posebej.

Na člen 5 predloga je mogoče dati pripombo, da se usmeri razlago tega člena.

Člen 5 omejuje obseg dostopa z osnovnimi pogoji:

b) dostop do vpogleda mora biti nujen v namen preprečevanja, odkrivanja ali preiskovanja terorističnih dejanj ali drugih hudih kaznivih dejanj;

c) dostop do vpogleda mora biti nujen v posebnem primeru (…); in

d) obstajati morajo utemeljeni razlogi, na podlagi dejanskih znamenj, ob upoštevanju katerih bo vpogled v podatke VIS prispeval k preprečevanju, odkrivanju in preiskovanju katerega koli zadevnega kaznivega dejanja.

Ti pogoji se združujejo, pogoj pod (b) pa je bolj opredelitev področja uporabe *ratione materiae*. To tako rekoč pomeni, da mora organ, ki želi dostop, obravnavati hudo kaznivo dejanje iz točke (b) predloga; obstajati mora posebni primer, kakor je navedeno pod (c). Poleg tega mora biti organ sposoben dokazati, da bo v posebnem primeru vpogled v podatke VIS prispeval k preprečevanju, odkrivanju in preiskovanju tega dejanja, kakor je predvideno pod (d).

EDPS tudi ob tej razlagi člena 5 skrbi ohlapno besedilo točke (d): „prispevati k“ ima precej širok pomen. Podatki VIS lahko v veliko primerih „prispevajo k“ preprečevanju ali preiskovanju hudih kaznivih dejanj. Da se upraviči dostop do podatkov VIS v odstopanju od načela omejitve namena, EDPS meni, naj ta vpogled „bistveno prispeva k“ preprečevanju, odkrivanju ali preiskovanju zadevnih hudih kaznivih dejanj ter temu ustrezno predlaga spremembo člena 5.

Člen 10 določa, da morajo zapisi prikazati točen namen dostopa. „Točen namen“ mora vsebovati elemente, zaradi katerih je vpogled v VIS nujen v smislu odstavka (d) člena 5. To bi pripomoglo k zagotavljanju, da se preskus nujnosti uporablja za vsak vpogled v VIS in bi zmanjšalo tveganje za rutinski dostop.

### 2.3. **Ključa za iskanje v zbirki podatkov VIS**

Člen 5(2) in (3) določata dvostopenjski dostop do podatkov VIS; dostop do sklopa podatkov je mogoč le, če je že na podlagi prvega sklopa podatkov poskus iskanja uspel. To je samo po sebi smiselni pristop. Vendar pa se zdi prvi sklop podatkov zelo obširen. Zlasti pa se za prvi sklop podatkov lahko dvomi o pomembnosti podatkov, kakor so navedeni v točkah (e) in (i) člena 5(2):

— Zdi se, da je „namen potovanja“ zelo splošen ključ za omogočanje učinkovitega iskanja v sistemu. Poleg tega zbuja nevarnost za oblikovanje profilov potnikov na podlagi tega elementa.

— Glede „fotografij“ je možnost iskanja v tako obsežni zbirki podatkov na podlagi fotografij omejena; rezultati takšnih iskanj imajo glede na trenutno stanje tehnologije nesprejemljivo stopnjo napačnih zadetkov. Posledice nepravilnega preverjanja istovetnosti so za vpletenega posameznika zelo resne.

EDPS zato zahteva, da se podatki iz točk (e) in (i) drugega odstavka člena 5 obravnavajo kakor dodatne informacije, ki so dostopne, če prvi vpogled pokaže na obstoj podatkov v sistemu, in se prenesejo v člen 5(3).

Lahko pa je možnost iskanja v zbirki podatkov na podlagi fotografij predmet presoje te tehnologije s strani svetovalnega odbora in se bo izvajalo le, ko bo tehnologija dovolj razvita in bo ocenjena kot dovolj zanesljiva.

### 2.4. **Uporaba za države članice, za katere Uredba VIS ne velja**

Dostop do VIS za namen vpogleda imajo lahko organi, odgovorni za notranjo varnost, iz držav članic, ki niso del VIS. Te službe morajo vpogled opraviti preko sodelujoče države članice, ob upoštevanju pogojev iz člena 5(1)(b) do (d) (tj. za vsak primer posebej), in predložiti ustrezno utemeljeno pisno zahtevo.

EDPS želi poudariti, da je treba določiti nekaj pogojev za obdelavo po vpogledu. Za države članice, ki sodelujejo v VIS, se uporablja pravilo, da je treba podatke v skladu z Okvirnim sklepom o varstvu podatkov v tretjem stebru obdelati, ko so ti pridobljeni iz VIS (glej spodaj). Enak pogoj mora veljati za države članice, za katere Uredba VIS ne velja, vendar pa opravljajo vpogled v podatke VIS. Enak zaključek se mora uporabiti glede vodenja evidenc za namen bodočega nadzora. EDPS zato priporoča, da se v tem smislu členu 6 predloga doda odstavek, da se člena 8 in 10 Sklepa uporabljata tudi za države članice, za katere Uredba VIS ne velja.

### 2.5. **Sistem varstva podatkov**

a) *Uporaba Okvirnega sklepa o varstvu podatkov v tretjem stebru*

Ker predstavlja dostop organov, odgovornih za notranjo varnost, izjemo v namenu VIS, mora biti predmet doslednega sistema varstva podatkov, ki zagotavlja visoko raven varstva podatkov, ki so jih nacionalni organi ali Europol pridobili iz VIS in obdelali.

Člen 8 predloga določa, da se Okvirni sklep o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (v nadaljevanju: „Okvirni sklep“) uporablja za obdelavo podatkov v skladu s predlaganim sklepom. Kar zadeva varstvo podatkov je treba sedanji predlog obravnavati kakor *lex specialis*, ki prispeva k *lex generalis* ali pa ga podrobno opredeljuje (tj. Okvirni sklep). Na primer pravila za nadaljnje posredovanje podatkov so v tem predlogu strožja in jih je treba spoštovati. Enako velja za razloge za dostop do podatkov.

b) *Področje uporabe*

EDPS pozdravlja dejstvo, da se sistem varstva podatkov iz Okvirnega sklepa uporablja za vse obdelave osebnih podatkov v skladu s predlaganim sklepom. Pomeni, da je stopnja varstva podatkov enaka, ne glede na to, kateri organ opravlja vpogled v podatke VIS.

Ker člen 2 uporablja funkcionalni kriterij za opredelitev teh organov („tisti organi v državah članicah, ki so odgovorni za preprečevanje, odkrivanje ali preiskovanje terorističnih dejanj ali drugih hudih kaznivih dejanj“), bi ta opredelitev lahko vključevala obveščevalne službe in organe pregona. Zato za obveščevalne službe, ki opravljajo vpogled v VIS, veljajo enake obveznosti z vidika varstva podatkov, kar je očitno pozitivni element.

Ker lahko obstajajo nekateri pomisleki glede razlage o uporabi Okvirnega sklepa za primere, kadar obveščevalne službe dostopajo do podatkov VIS, EDPS predlaga nadomestno besedilo, in sicer:

„Kadar se Okvirni sklep (…) ne uporablja, države članice zagotovijo stopnjo varstva podatkov, ki je najmanj enaka tisti, ki je zagotovljena z Okvirnim sklepom“.

c) *Nadzor*

Kar zadeva besedilo člena 8 je treba pojasniti, da odstavek 1 obravnava obdelavo podatkov znotraj ozemlja držav članic. Odstavka 2 in 3 pojasnjujeta svoji področji uporabe (obdelava podatkov s strani Europola in Komisije), pojasniti pa je treba, da odstavek 1 obravnava drugo domnevo.

Porazdelitev nadzornih pristojnosti na podlagi zadevnih dejavnosti različnih akterjev je smiselni pristop. Vendar pa manjka en element: potreba po usklajenem pristopu pri nadzoru. V mnenju EDPS o VIS je že bilo navedeno: „Kar zadeva nadzor nad VIS, je pomembno tudi poudariti, da bi bilo treba nadzorne dejavnosti nacionalnih nadzornih organov in EDPS uskladiti do določene mere. Dejansko obstaja potreba po usklajenem izvajanju Uredbe ter po približevanju k skupnemu pristopu za reševanje skupnih težav.

Člen 35 [predloga o VIS] mora vsebovati določbo, v skladu s katero EDPS vsaj enkrat letno skliče sestanek z vsemi nacionalnimi nadzornimi organi.“

Enako velja za to posebno uporabo sistema VIS (v tem primeru tudi z vključitvijo skupnega nadzornega organa Europola). Nadzor mora biti v celoti usklajen z nadzorom „VIS prvega stebra“, saj je to enak sistem. Poleg tega so usklajevalni sestanki, ki jih EDPS skliče z vsemi v nadzor vpletenimi stranmi, tudi vzorec, ki je bil izbran v okviru nadzora drugih velikih informacijskih sistemov, kakor je Eurodac.

EDPS se zaveda, da je usklajevanje do neke mere predvideno v predlogu, ki omenja vlogo bodoče Delovne skupine za varstvo posameznikov glede varstva osebnih podatkov, vzpostavljene s členom 31 predlaganega Okvirnega sklepa. Vendar pa je treba ponovno poudariti, da naloge tega svetovalnega organa ne vključujejo samega nadzora.

EDPS predlaga, da se doda določba, ki predpisuje, da imajo usklajevalni sestanki, ki jih EDPS skliče v okviru nadzora „VIS prvega stebra“, prav tako pristojnost nad podatki, obdelanimi v skladu s tem predlogom, in v tem smislu je treba zastopati skupni nadzorni organ Europola.

### 2.6. **Samorevidiranje**

Člen 12 predloga določa sisteme spremljanja za VIS. EDPS meni, da naj to spremljanje ne bi obravnavalo zgolj vidikov rezultata, racionalnosti in kakovosti storitev, ampak tudi izpolnjevanje zakonskih zahtev, zlasti na področju varstva podatkov. Člen 12 je treba ustrezno spremeniti.

Za izvedbo samorevidiranja zakonitosti obdelave je treba Komisiji omogočiti, da uporabi evidenco, ki se hrani v skladu s členom 10 predloga. V skladu s tem mora člen 10 zagotoviti, da se ti zapisi ne shranjujejo le zaradi nadzora nad varstvom podatkov in zagotavljanja varnosti podatkov, ampak tudi zaradi rednega samorevidiranja VIS. Poročila o samorevidiranju bodo prispevala k nalogam EDPS in drugih nadzornikov na področju nadzora, ki bodo lahko bolje izbrali svoja prednostna področja za nadzor.

## 3. **ZAKLJUČEK**

EDPS glede na omenjeno poudarja ključni pomen, da se organom, odgovornim za notranjo varnost, in Europolu dovoli dostop, in sicer za vsak primer posebej in pod strogimi varnostnimi ukrepi. S predlogom je ta cilj dosežen na splošno zadovoljiv način, čeprav so možne nekatere izboljšave, kakor je predlagano v tem predlogu:

— Pogoj za dostop do VIS v skladu s členom 5 mora biti, da bo iskanje podatkov „bistveno“ prispevalo k preprečevanju, odkrivanju ali preiskovanju hudih kaznivih dejanj, zahtevane evidence iz člena 10 pa morajo omogočati vrednotenje tega stanja za vsak posamezni primer.

— Ponovno je treba preučiti ključa za iskanje za dostop do VIS, ki sta omenjena v členu 5(2), in sicer „namen potovanja“ in „fotografije“, ki naj bosta na voljo kakor dodatne informacije v primeru zadetkov.

— Stopnja varstva podatkov, ki velja po vpogledu, mora biti enaka, ne glede na to, kateri organ opravlja vpogled v podatke VIS. Člena 8 in 10 morata prav tako veljati za države članice, za katere Uredba VIS ne velja.

— Zagotoviti je treba usklajen pristop k nadzoru, tudi z vidika dostopa do VIS, kakor je predvideno v tem predlogu.

— Določbe o sistemih spremljanja morajo zagotoviti tudi samorevidiranje skladnosti z zahtevami na področju varstva podatkov.

V Bruslju, 20. januarja 2006

Peter HUSTINX

*Evropski nadzornik za varstvo podatkov*