# EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

## Mnenje Evropskega nadzornika za varstvo podatkov glede Predloga okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (KOM (2005) 475 končno)

(2006/C 47/12)

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 zaprosila za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001/ES 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 —

SPREJEL NASLEDNJE MNENJE:

### I. PREDHODNE OPOMBE

*Posvetovanje z Evropskim nadzornikom za varstvo podatkov*

1. Komisija je Evropskemu nadzorniku za varstvo podatkov 4. oktobra 2005 v pismu poslala Predlog okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah. Evropski nadzornik za varstvo podatkov je pismo razumel kot zaprosilo, da institucijam in organom Skupnosti svetuje v skladu s členom 28(2) Uredbe št. 45/2001/ES. Meni tudi, da je treba zadevno mnenje navesti v preambuli okvirnega sklepa.

*Pomembnost zadevnega predloga*

2. Evropski nadzornik za varstvo podatkov poudarja, da je zadevni predlog z vidika temeljnih pravic in svoboščin fizičnih oseb za varstvo njihovih osebnih podatkov zelo pomemben. Sprejetje tega predloga bi pomenilo velik napredek na področju varstva osebnih podatkov; to je pomembno področje, ki na ravni Evropske unije zahteva usklajen in učinkovit mehanizem za varstvo osebnih podatkov.

3. V tem okviru Evropski nadzornik za varstvo podatkov poudarja, da postaja policijsko in pravosodno sodelovanje med državami članicami – kot element za postopno vzpostavitev območja svobode, varnosti in pravice – vse pomembnejše. Haaški program uvaja načelo dostopnosti, s čimer bi se zboljšala čezmejna izmenjava informacij organov kazenskega pregona. V skladu s tem programom ([1]) naj bi dejstvo, da informacije prehajajo meje, postalo nepomembno. Uvedba načela dostopnosti predstavlja splošnejši trend olajševanja izmenjave informacij organov kazenskega pregona (glej na primer tako imenovano Konvencijo Prüm ([2]), ki jo je podpisalo sedem držav članic, in švedski predlog okvirnega sklepa o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona ([3])). Nedavno odobritev Direktive Evropskega parlamenta in Sveta o hrambi komunikacijskih podatkov ([4]) s strani Evropskega parlamenta bi lahko razumeli na enak način. Takšen razvoj zahteva sprejetje pravnega instrumenta, s čimer bi se zagotovilo učinkovito varstvo osebnih podatkov v vseh državah članicah Evropske unije na podlagi skupnih standardov.

([1]) Str.18 programa.

([2]) Konvencija med Kraljevino Belgijo, Zvezno republiko Nemčijo, Kraljevino Španijo, Francosko republiko, Velikim vojvodstvom Luksemburg, Kraljevino Nizozemsko in Republiko Avstrijo o okrepitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu, čezmejnem kriminalu in nezakonitem preseljevanju. Prüm (Nemčija ), 27. maja 2005.

([3]) Pobuda Kraljevine Švedske za sprejetje Okvirnega sklepa o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona držav članic Evropske unije, zlasti glede hudih kaznivih dejanj, vključno s terorističnimi dejanji (UL, C 281).

([4]) Na podlagi Predloga direktive Evropskega parlamenta in Sveta o hrambi podatkov, obdelanih v povezavi z zagotavljanjem javnih elektronskih komunikacijskih storitev, in spremembi Direktive 2002/58/ES (KOM (2005) 438 končno).

4. Evropski nadzornik za varstvo podatkov opozarja na dejstvo, da obstoječi splošni okvir za varstvo podatkov na tem področju ne zadošča. Kot prvo se Direktiva 95/46/ES ne uporablja za obdelavo osebnih podatkov pri dejavnostih zunaj okvira zakonodaje Skupnosti, kot so dejavnosti iz naslova VI Pogodbe o Evropski uniji (člen 3(2) Direktive). Čeprav je v večini držav članic področje uporabe veljavne zakonodaje širši, kot to zahteva direktiva, in ne izključuje obdelave podatkov za namene kazenskega pregona, se nacionalne zakonodaje med seboj znatno razlikujejo. Drugič: Konvencija št. 108 Sveta Evrope ([1]), ki zavezuje vse države članice, ne zagotavlja potrebne jasnosti na področju varstva, kakor se je priznavala že ob sprejetju Direktive 95/46/ES. Tretjič: noben od teh dveh pravnih instrumentov ne upošteva posebnosti izmenjave podatkov med policijskimi in pravosodnimi organi ([2]).

*Prispevanje k uspehu samega sodelovanja*

5. Učinkovito varstvo osebnih podatkov ni pomembno le za posameznike, na katere se podatki nanašajo, prispeva tudi k uspešnemu policijskemu in pravosodnemu sodelovanju. Oba javna interesa z več vidikov sovpadata.

6. Upoštevati je treba, da so zadevni osebni podatki pogosto zelo občutljive narave ter da so jih policijski in pravosodni organi pridobili s preiskovanjem oseb. Pripravljenost za izmenjavo teh podatkov z organi drugih držav članic se bo povečala, če se organu zagotovi določena raven varstva podatkov v tej drugi državi članici. Evropski nadzornik za varstvo podatkov navaja kot pomembne elemente varstva podatkov zaupnost in varnost podatkov ter omejitev dostopa in omejitev nadaljnje uporabe.

7. Z visoko ravnjo varstva podatkov se lahko zagotovita točnost in zanesljivost osebnih podatkov. Za izmenjavo podatkov med policijskimi in/ali pravosodnimi organi sta točnost in zanesljivost teh podatkov še pomembnejša, zlasti zato, ker se podatki zaradi zaporednih izmenjav in ponovnih pošiljanj med organi kazenskega pregona na koncu obdelujejo daleč stran od vira in izven konteksta, v katerem so bili prvotno zbrani in uporabljeni. Navadno organi, ki prejmejo podatke, ne poznajo dodatnih okoliščin, zato se morejo v celoti zanašati na podatke same.

8. Uskladitev nacionalnih predpisov glede osebnih podatkov na področju policijskega in pravosodnega sodelovanja – vključno z ustreznimi varovali za varstvo teh podatkov – lahko tako spodbudi vzajemno zaupanje in učinkovitost same izmenjave.

*Spoštovanje načel varstva podatkov skupaj z drugim sklopom pravil*

9. Potreba po zadevnem predlogu in njegova pomembnost sta se poudarjala ob več priložnostih. Na spomladanski konferenci, ki je bila aprila 2005 v Krakovu, so evropski organi za varstvo podatkov sprejeli izjavo in pogajalsko izhodišče, v katerih so pozvali k sprejetju novega pravnega okvira za varstvo podatkov, ki bi se uporabljal za tretji steber. Novi okvir naj bi upošteval načela varstva podatkov iz Direktive 95/46/ES – pomembno je, da se v okviru Evropske unije zagotovi skladnost varstva podatkov – in hkrati zagotavljal dodatna pravila, ki bi upoštevala posebno naravo kazenskega pregona ([3]). Evropski nadzornik za varstvo podatkov pozdravlja dejstvo, da zadevni predlog upošteva obe izhodišči: upošteva načela varstva podatkov iz Direktive 95/46/ES in zagotavlja dodatna pravila.

10. To mnenje analizira, do kolikšne mere je rezultat z vidika varstva podatkov sprejemljiv, pri čemer upošteva posebne okoliščine, pogojene z varstvom podatkov na področju kazenskega pregona. Zadevni podatki so pogosto zelo občutljive narave (glej točko 6 tega mnenja), hkrati pa obstaja z vidika učinkovitega izvajanja kazenskega pregona, ki lahko vključuje varovanje življenja in telesno varnost oseb, močan pritisk glede dostopa do teh podatkov. V skladu z mnenjem Evropskega nadzornika za varstvo podatkov naj bi določbe glede varstva podatkov ustrezala utemeljenim potrebam kazenskega pregona, hkrati pa naj bi varovala posameznika, na katerega se podatki nanašajo, pred neutemeljeno obdelavo podatkov in dostopom do njih. Izid upoštevanja evropskega zakonodajalca mora – da je v skladu z načelom sorazmernosti – spoštovati potencialno nasprotujoča si javna interesa. V tem okviru je Evropski nadzornik za varstvo podatkov ponovno omenil, da ta dva interesa pogosto sovpadata.

*Naslov VI Pogodbe o Evropski uniji*

11. Omeniti je treba, da zadevni predlog spada v okvir naslova VI Pogodbe o Evropski uniji, v t. i. tretji steber. Poseganje evropskega zakonodajalca je vezano na jasne omejitve: omejitve zakonodajnih pristojnosti Unije v zadevah iz členov 30 in 31, omejitve zakonodajnega postopka, ki ne vključuje polnega sodelovanja Evropskega parlamenta, ter omejitve sodnega nadzora, saj pristojnost Evropskega sodišča v skladu s členom 35 PEU ni izključna. Te omejitve zahtevajo še natančnejši pregled besedila predloga.

([1]) Konvencija Sveta Evrope o varstvu posameznikov glede avtomatske obdelave osebnih podatkov, 28. januar 1981.

([2]) Svet Evrope je leta 1987 izdal Priporočilo št. R (87) 15 o ureditvi uporabe osebnih podatkov v policijskem sektorju, ki pa je po svoji naravi za države članice nezavezujoče.

([3]) V enakem smislu tudi: „Evropski nadzornik za varstvo podatkov kot svetovalec institucijam Skupnosti glede zakonodajnih predlogov in pripadajočih dokumentov“, z dne 18. marca 2005, objavljeno na www.edps.eu.int.

## II. KONTEKST: IZMENJAVA INFORMACIJ V SKLADU Z NAČELOM DOSTOPNOSTI, HRAMBA PODATKOV IN POSEBNI OKVIR SIS II IN VIS

### II.1 Načelo dostopnosti

12. Predlog je tesno povezan s Predlogom okvirnega sklepa sveta o izmenjavi informacij v skladu z načelom dostopnosti (KOM(2005) 490 končno). Slednji predlog naj bi izvajal načelo dostopnosti in tako zagotavljal, da se informacije, ki so na voljo pristojnim organom države članice za boj proti kriminalu, zagotovijo enakim organom drugih držav članic. To naj bi privedlo do ukinitve notranjih meja pri izmenjavi zadevnih informacij, saj bi za izmenjavo informacij po vsej Uniji veljali enaki pogoji.

13. Tesno povezavo med obema predlogoma razlaga tudi dejstvo, da informacije organov kazenskega pregona v veliki meri vključujejo osebne podatke. Pravni predpisi o izmenjavi informacij organov kazenskega pregona se lahko sprejmejo le, če zagotavljajo ustrezno varstvo osebnih podatkov. Če ima poseganje na ravni Evropske unije za posledico ukinitev notranjih meja za izmenjavo takšnih informacij, se varstvo osebnih podatkov ne more več urejati le z nacionalno zakonodajo. Naloga evropskih institucij tako postane zagotavljanje varstva osebnih podatkov brez notranjih meja na celotnem ozemlju Unije. Ta naloga je izrecno navedena v členu 30(1)(b) PEU in je posledica obveznosti Unije, da spoštuje temeljne pravice (člen 6 PEU). Poleg tega:

— člen 1(2) zadevnega predloga izrecno navaja, da države članice ne smejo več omejevati niti prepovedati čezmejnega pretoka informacij zaradi razlogov, povezanih z varstvom osebnih podatkov;

— Predlog okvirnega sklepa sveta o izmenjavi informacij v skladu z načelom dostopnosti vsebuje nekaj sklicevanj na zadevni predlog.

14. Evropski nadzornik za varstvo podatkov poudarja, naj se okvirni sklep sveta o izmenjavi informacij v skladu z načelom dostopnosti sprejme le, če se sprejme tudi okvirni sklep o varstvu osebnih podatkov. Zadevni predlog okvirnega sklepa Sveta o varstvu podatkov ima določene prednosti in je potreben, četudi obstaja pomanjkanje pravnih instrumentov v zvezi z dostopnostjo. To je poudarjeno v oddelku I tega mnenja.

15. V takem primeru bo Evropski nadzornik za varstvo podatkov analizo obeh predlogov pripravil v dveh ločenih mnenjih. Eden izmed razlogov za to je tudi praktičnost. Težko je zagotoviti, da bosta Svet in Evropski parlament predloga obravnavala hkrati in enako hitro.

### II.2 Hramba podatkov

16. Evropski nadzornik za varstvo podatkov je 26. septembra 2005 predložil mnenje o predlogu direktive o hrambi komunikacijskih podatkov [1]. V mnenju je izpostavil nekatere večje pomanjkljivosti predloga in predlagal, da se direktivi dodajo posebne določbe o dostopu pristojnih organov do podatkov o prometu in lokaciji in določbe o dodatni uporabi podatkov ter da se direktivi dodajo še določbe o drugih dodatnih varovalih za varstvo podatkov. Besedilo direktive, kakor sta ga sprejela Evropski parlament in Svet, vsebuje omejeno – a nikakor ne zadostujočo – določbo o varstvu in varnosti podatkov ter še manj zadostujočo določbo o dostopu, ki nacionalni zakonodaji nalaga, da ob upoštevanju ustreznih določb zakonodaje Evropske unije ali mednarodnega javnega prava, določi ukrepe glede dostopa do hranjenih podatkov.

17. Zaradi odobritve direktive o hrambi komunikacijskih podatkov je postala vzpostavitev pravnega okvira za varstvo podatkov v tretjem stebru še bolj nujna. S sprejetjem direktive zakonodajalec Skupnosti obvezuje ponudnike telekomunikacijskih in internetnih storitev, da hranijo podatke za namene kazenskega pregona brez potrebnih in ustreznih varoval za varstvo posameznikov, na katere se podatki nanašajo. Varstvo podatkov je še vedno pomanjkljivo, saj direktiva ne obravnava (zadostno) dostopa do podatkov niti njihove nadaljnje uporabe potem, ko pristojni organi kazenskega pregona že imajo dostop do podatkov.

18. Zadevni predlog odpravlja velik del teh pomanjkljivosti, saj se nanaša na nadaljnjo uporabo podatkov potem, ko pristojni organi kazenskega pregona že imajo dostop do podatkov. Evropski nadzornik za varstvo podatkov pa vseeno obžaluje, da tudi ta zadevni predlog ne ureja dostopa do teh podatkov. V nasprotju s tem, kar je predvideno za sistema SIS II in VIS (glej točko II.3 tega mnenja), je zadeva prepuščena nacionalnemu zakonodajalcu.

### II.3 Obdelava podatkov v okviru SIS II in VIS

19. Evropska unija trenutno uporablja ali razvija nekaj obsežnih informacijskih sistemov (Eurodac, SIS II, VIS) in stremi k sinergiji med njimi. Prisotna je tudi vse večja tendenca, da se za namene kazenskega pregona zagotovi širok dostop do teh sistemov. Takšen daljnosežen razvoj pa mora v skladu s haaškim programom upoštevati „potrebo po uravnoteženosti med cilji kazenskega pregona in varovanjem temeljnih pravic posameznikov“.

[1] Mnenje Evropskega nadzornika za varstvo podatkov glede Predloga direktive Evropskega parlamenta in Sveta o hrambi podatkov, obdelanih v povezavi z zagotavljanjem javnih elektronskih komunikacijskih storitev, in spremembi Direktive 2002/58/ES (KOM (2005) 438 končno), objavljeno na www.edps.eu.int.

20. Evropski nadzornik za varstvo podatkov je v Mnenju z dne 19. oktobra 2005 o predlogu za drugo generacijo Schengenskega informacijskega sistema (SIS II) ([1]) izpostavil nekatere elemente glede sočasne uporabe splošnih (lex generalis) in posebnih določb (lex specialis) o varstvu podatkov. Zadevni predlog se lahko razume kot lex generalis, ki v okviru tretjega stebra nadomešča Konvencijo 108 ([2]).

21. Evropski nadzornik za varstvo podatkov v zvezi s tem poudarja, da predlog določa tudi splošni okvir za varstvo podatkov za posebne instrumente, kakršna sta na primer tretji steber sistema SIS II in dostop organov kazenskega pregona do vizumskega informacijskega sistema ([3]).

## III. **JEDRO PREDLOGA**

### III.1 **Skupni standardi, ki se uporabljajo za vso obdelavo**

*Izhodišče*

22. Predlog namerava v skladu s svojim členom 1(1) določiti skupne standarde za zagotovitev varstva osebnih podatkov v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah. Člen 1(1) je treba brati v povezavi s členom 3(1), ki navaja, da se predlog uporablja za obdelavo osebnih podatkov (…) s strani pristojnega organa za namen preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj.

23. Iz teh določb sledi, da ima predlog okvirnega sklepa dve glavni značilnosti: določa skupne standarde ter se uporablja za vso obdelavo za namene izvrševanja kazenskega prava, tudi če pristojni organi ali druge države članice zadevnih podatkov niso posredovale ali dale na voljo.

24. Evropski nadzornik za varstvo podatkov poudarja pomembnost teh dveh glavnih značilnosti. Cilj zadevnega predloga mora biti vzpostavitev okvira za varstvo podatkov, ki v celoti dopolnjuje obstoječi pravni okvir v prvem stebru. Le če je ta pogoj izpolnjen, Evropska unija v celoti izpolnjuje svoje obveznosti iz člena 6(2) PEU o spoštovanju temeljnih pravic, kakor je zajamčeno z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin (ECHR).

*Skupni standardi*

25. Kar zadeva prvo značilnost: cilj zadevnega predloga je zagotoviti, da se bodo obstoječa načela varstva podatkov uporabljala v okviru tretjega stebra. Poleg tega zagotavlja skupne standarde, ki natančno opredeljujejo ta načela, z vidika njihove uporabe na tem področju. Evropski nadzornik za varstvo podatkov poudarja pomembnost teh vidikov predloga. Odražajo posebno in občutljivo naravo obdelave osebnih podatkov na tem področju. Evropski nadzornik za varstvo podatkov predvsem ceni uvedbo načela razlikovanja med osebnimi podatki kategorij oseb kot načela varstva podatkov za področje policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, poleg obstoječih načel varstva podatkov (člen 4(4)). Evropski nadzornik za varstvo podatkov meni, da mora biti samo načelo in njegove pravne posledice za posameznika, na katerega se podatki nanašajo, še *natančneje* določene (glej točke 88–92 tega mnenja).

26. Pravila se morajo uporabljati v različnih situacijah, zato ne smejo biti preveč podrobna. Po drugi strani pa morajo državljanu zagotoviti ustrezno pravno varnost, kakor tudi ustrezno zaščito njegovih osebnih podatkov. Evropski nadzornik za varstvo podatkov meni, da predlog na splošno upošteva ravnovesje med tema dvema morebiti nasprotujočima si zakonskima zahtevama. Določbe dopuščajo prožnost, kjer je ta potrebna, vendar so na večini področij zadosti natančne, da zaščitijo državljane.

27. Vendar pa je predlog v nekaterih točkah preveč prožen in ne zagotavlja potrebnih varoval. Na primer v členu 7(1) predlog predvideva splošno izjemo glede varoval, pod edinim pogojem, „kolikor ni drugače določeno z zakonom“. Tako široka diskrecijska pravica za hrambo podatkov dalj časa, kakor je potrebno za predviden namen, ne bi bila skladna s temeljno pravico varstva podatkov, prav tako pa bi škodila osnovni potrebi po uskladitvi varstva osebnih podatkov, obdelanih v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah.

28. Izjeme je treba, kjer je to potrebno, omejiti na nacionalne ali evropske pravne določbe, ki ščitijo določene javne interese. Člen 7(1) mora omeniti te javne interese.

29. To privede do naslednje točke. Kadar koli kakšen drug poseben pravni instrument iz naslova VI Pogodbe EU določa natančnejše pogoje ali omejitve za obdelavo ali dostop do podatkov, je treba to bolj posebno zakonodajo uporabljati kot *lex specialis*. Člen 17 tega predloga določa odstopanja od členov 12, 13, 14 in 15, ko posebna zakonodaja iz naslova VI določa posebne pogoje za prenos podatkov. To je ponazoritev splošne narave predloga (kot je zgoraj razloženo), vendar ne vključuje vseh hipotez.

([1]) Odst. 2.2.4 Mnenja.

([2]) Konvencija Sveta Evrope o varstvu posameznikov glede avtomatske obdelave osebnih podatkov, 28. januar 1981.

([3]) Predlog sklepa Sveta za dostop organov držav članic, ki so zadolženi za notranjo varnost, in Europola do vizumskega informacijskega sistema z namenom vpogleda zaradi preprečevanja, odkrivanja in preiskovanja terorističnih in drugih hudih kaznivih dejanj (KOM (2005) 600 konč.), izdano 24. novembra 2005. Evropski nadzornik za varstvo podatkov namerava podati mnenje o tem predlogu na začetku leta 2006.

Evropski nadzornik za varstvo podatkov meni, da bi člen 17:

— moral biti zasnovan bolj splošno: če obstaja bolj posebna zakonodaja, ki ureja kateri koli vidik obdelave podatkov (ne le prenos podatkov), se uporablja posebna zakonodaja;

— moral vsebovati varovalo, da odstopanja ne morejo zmanjšati stopnje zaščite.

*Veljavno za vso obdelavo*

30. Kar zadeva drugo značilnost: idealno bi bilo, če bi bilo zajeto vse zbiranje in obdelava osebnih podatkov v okviru tretjega stebra.

31. Da bi okvirni sklep dosegel svoj namen, mora zajemati vse policijske in pravosodne podatke, tudi če pristojni organi ali druge države članice zadevnih podatkov niso posredovale ali dale na voljo.

32. To je veliko bolj pomembno, ker bi vsaka omejitev podatkov, ki se prenašajo ali dajo na voljo pristojnim organom v drugih državah članicah, povzročila, da bi področje uporabe okvirnega sklepa postalo še zlasti negotovo in nezanesljivo, kar bi bilo v nasprotju z njegovim prvotnim ciljem ([1]). Ogrožena bi bila pravna varnost posameznikov. V normalnih okoliščinah se v času zbiranja in obdelave osebnih podatkov ne ve, ali bodo ti podatki potrebni za izmenjavo s pristojnimi organi v drugih državah članicah. Evropski nadzornik za varstvo podatkov v okviru tega omenja načelo razpoložljivosti ter odpravo notranjih meja za izmenjavo podatkov na področju kazenskega pregona.

33. Evropski nadzornik za varstvo podatkov končno opozarja, da se predlog ne nanaša na:

— obdelavo v okviru drugega stebra Pogodbe EU (skupna zunanja in varnostna politika);

— obdelavo podatkov s strani obveščevalnih služb ali na njihov dostop do teh podatkov, kadar jih obdelujejo pristojni organi ali druge stranke (to izhaja iz člena 33 PEU).

Na teh področjih mora ustrezno varstvo posameznikov, na katere se nanašajo osebni podatki, zagotoviti nacionalna zakonodaja. Pri oceni predloga je treba upoštevati luknjo v varstvu na ravni EU ([2]): ker ni mogoče zajeti vse obdelave na področju kazenskega pregona, mora zakonodajalec zagotoviti še učinkovitejšo zaščito na področjih, ki jih predlog dejansko zajema.

([1]) Evropski nadzornik za varstvo podatkov se sklicuje na enako obrazložitev Sodišča (med drugim) v sodbi v zadevi Österreichischer Rundfunk and Others, združene zadeve C-465/00, C-138/01 in C-139/01, PSES [2003], str. I-4989.

([2]) V enakem smislu tudi mnenje Evropskega nadzornika za varstvo podatkov z dne 26. septembra 2005 o predlogu direktive Evropskega parlamenta in Sveta o hrambi podatkov, obdelanih v povezavi z zagotavljanjem javnih elektronskih komunikacijskih storitev, in spremembi Direktive 2002/58/ES, točka 33.

III.2 **Pravna podlaga**

34. Uvodne izjave predloga okvirnega sklepa Sveta o izmenjavi informacij v skladu z načelom dostopnosti navajajo točno določeno pravno podlago, in sicer člen 30(1)(b). Nasprotno pa zadevni predlog izrecno ne določa, katere določbe iz člena 30 ali 31 predstavljajo pravno podlago.

35. Čeprav ni naloga Evropskega nadzornika za varstvo podatkov, ki je zakonodajni svetovalec Evropske unije, da izbere pravno podlago predloga, je koristno domnevati, da bi tudi zadevni predlog lahko temeljil na členu 30(1)(b). Poleg tega bi lahko temeljil na členu 31(1) PEU ter bi se moral v celoti uporabljati za domače primere, pod pogojem, da je to potrebno za izboljšanje policijskega in pravosodnega sodelovanja med državami članicami. V tem okviru Evropski nadzornik za varstvo podatkov vnovič poudarja, da so lahko vsi osebni podatki, ki so bili zbrani, hranjeni, obdelani ali analizirani za namene kazenskega pregona, zlasti v okviru načela dostopnosti, predmet izmenjave s pristojnimi organi druge države članice.

36. Evropski nadzornik za varstvo podatkov se strinja, da člena 30(1)(b) in 31(1)(c) PEU zagotavljata pravno podlago za pravila o varstvu podatkov, ki niso omejena na varstvo osebnih podatkov, ki se dejansko izmenjajo med pristojnimi organi držav članic, temveč se uporabljajo tudi za domače primere. Zlasti:

— člen 30(1)(b), ki je lahko pravna podlaga za pravila o zbiranju, hrambi, obdelavi, analizi in izmenjavi ustreznih informacij, ni omejen na informacije, ki so bile dane na voljo ali posredovane drugim državam članicam; edina omejitev, ki jo nalaga člen 30(1)(b), je pomembnost informacij za policijsko sodelovanje;

— kar zadeva pravosodno sodelovanje, je člen 31(1)(c) še bolj izrecen, ker skupno ukrepanje vključuje „zagotavljanje skladnosti predpisov, ki se uporabljajo v državah članicah, kolikor je to potrebno za izboljšanje takšnega sodelovanja“;

— na podlagi primera Pupino ([3]), kjer Sodišče uporablja načela prava Skupnosti glede zadev iz tretjega stebra; Ta sodna praksa odraža razvoj od preprostega sodelovanja med organi držav članic znotraj tretjega stebra do območja svobode, varnosti in pravice, ki ga je mogoče primerjati z notranjim trgom, kakor je bil vzpostavljen v okviru Pogodbe ES;

([3]) Sodba Sodišča z dne 16. junija 2005, Pupino, primer C-105/03.

— sodeč po Evropskem nadzorniku za varstvo podatkov se zaradi načela učinkovitosti Pogodba ne razlaga na način, ki ovira institucije Evropske unije pri učinkovitem izvajanju njihovih nalog; Sem sodi tudi njihova naloga varstva temeljnih pravic;

— kakor je bilo povedano prej, z omejitvijo na mejne primere se ne bi spoštovale posledice načela dostopnosti in ogrozila bi se pravna varnost posameznikov.

37. Evropski nadzornik za varstvo podatkov poleg tega opozarja na *izmenjavo podatkov s tretjimi državami*. Države članice uporabljajo osebne podatke, zbrane in obdelane v tretjih državah, ki so jim bili posredovani, za namene kazenskega pregona, ter pristojnim organom v tretjih državah in mednarodnim organom posredujejo osebne podatke, ki so jih same pridobile in/ali obdelale.

38. Člena 30 in 31 PEU ne zahtevata različne obravnave osebnih podatkov, ki so jih zbrali organi tretjih držav, in tistih podatkov, ki so jih prvotno zbrali pristojni organi v državi članici. Podatki, posredovani iz tretjih držav, morajo ustrezati enakim standardom kakor podatki, pridobljeni v državi članici. Vendar pa kakovosti podatkov ni zmeraj lahko zagotoviti (to je obravnavano v naslednjem poglavju tega mnenja).

39. Prenos osebnih podatkov s strani pristojnih organov držav članic tretjim državam v strogem pomenu besede ne sodi v področje uporabe Naslova IV Pogodbe EU. Če pa bi bilo možno podatke poslati v tretjo državo brez zagotovitve varstva posameznika, na katerega se podatki nanašajo, bi to resno škodovalo varstvu, ki je predvideno v zadevnem predlogu na ozemlju Evropske unije, zaradi razlogov, navedenih v oddelku III.4 tega mnenja. Na kratko:

— pravice posameznika, na katerega se podatki nanašajo, kakor zagotavlja zadevni predlog, so neposredno prizadete, če prenos tretjim državam ni potekal skladno s pravili varstva podatkov;

— prišlo bi do tveganja, da se pristojni organi držav članic izogibajo strogim normam glede varstva podatkov.

40. Če povzamemo, je veljavnost splošnih pravil glede varstva podatkov za osebne podatke, izmenjane med pristojnimi organi držav članic in organi tretjih držav ter mednarodnimi organizacijami, potrebna za učinkovitost skupnih pravil glede varstva osebnih podatkov med pristojnimi organi držav članic in je potemtakem potrebna za izboljšanje sodelovanja med državami članicami. Člena 30 in 31 PEU zagotavljata potrebno pravno podlago.

### III.3 **Posebne pripombe glede področja uporabe predloga**

*Osebni podatki, obdelani s strani pravosodnih organov*

41. Osebne podatke obdelujejo in si izmenjujejo policijski organi in tudi pravosodni organi. Predlog, ki temelji na členih 30 in 31 Pogodbe EU, se uporablja za sodelovanje med policijskimi organi in za sodelovanje med pravosodnimi organi. Na tej točki ima predlog širše področje uporabe kot predlog okvirnega sklepa Sveta o izmenjavi informacij, ki je omejen na policijsko sodelovanje ter se zgolj nanaša na informacije pred začetkom sodnega pregona.

42. Evropski nadzornik za varstvo podatkov pozdravlja dejstvo, da predlog vključuje tudi osebne podatke, ki jih obdelujejo pravosodni organi. Obstaja dober razlog, zakaj se v istem predlogu obravnavajo policijski podatki in podatki pravosodnih organov, obdelani za namene kazenskega pregona. Na prvem mestu se organizacija verige kazenskih preiskav in sodnega pregona v državah članicah razlikuje. Sodelovanje pravosodnih organov nastopi v različnih državah članicah na različnih stopnjah. Na drugem mestu lahko vsi osebni podatki v tej verigi končajo v sodnem spisu. Na prej omenjenih stopnjah ni logično imeti različne veljavne sisteme za varstvo podatkov.

43. Pri nadzoru obdelave podatkov pa je potreben drugačen pristop. Člen 30 predloga našteva naloge nadzornih organov. Člen 30(9) navaja, da pooblastila nadzornega organa ne vplivajo na neodvisnost sodstva. Evropski nadzornik za varstvo podatkov priporoča, da se v predlogu razjasni, da nadzorni organi ne spremljajo obdelave podatkov s strani pravosodnih organov, kolikor ti delujejo v okviru svoje sodne usposobljenosti ([1]).

*Obdelava s strani Europola in Eurojusta (in Carinskega informacijskega sistema)*

44. V skladu s členom 3(2) predloga se okvirni sklep ne uporablja za obdelavo osebnih podatkov v Europolu, Eurojustu in Carinskem informacijskem sistemu ([2]).

([1]) Ta določba bi lahko bila podobna določbi iz člena 46 Uredbe 45/2001/ES.

([2]) Carinski informacijski sistem je majhen, vendar zapleten sistem, ki se sestoji iz nacionalnih in nadnacionalnih elementov, primerljivih s Schengenskim informacijskim sistemom. Ob upoštevanju relativno omejene pomembnosti zadevnega predloga za Carinski informacijski sistem in zapletenosti samega sistema, se v tem mnenju ne bo upošteval. Evropski nadzornik za varstvo podatkov se bo s Carinskim informacijskim sistemom ukvarjal v drugem okviru.

45. V strogem pomenu besede je ta določba nepotrebna v vsakem primeru, kolikor se nanaša na Europol in Eurojust. Okvirni sklep na podlagi člena 34(b) PEU se lahko sprejme le za namen približevanja zakonov in drugih predpisov držav članic in se ne more nasloviti na Europol in Eurojust.

46. Kar zadeva vsebino, vodi besedilo člena 3(2) do naslednjih ugotovitev:

— zadevni predlog določna splošni okvir, ki bi se moral načeloma uporabljati v vseh primerih, ki sodijo v tretji steber. Usklajenost pravnega okvira varstva podatkov je sama po sebi dejavnik, ki poveča učinkovitost varstva podatkov;

— Europol in Eurojust trenutno razpolagata z zelo dobro opredeljenimi sistemi varstva podatkov, vključno z nadzornim sistemom. Zato v tem trenutku ni nujno, da se predpisi, ki se uporabljajo, prilagodijo besedilu tega predloga;

— dolgoročno gledano pa je treba predpise, ki jih Europol in Eurojust uporabljata na področju varstva podatkov, v celoti uskladiti s tem okvirnim sklepom;

— to je zlasti pomembno, ker se sedanji predlog okvirnega sklepa – razen poglavja III – uporablja za zbiranje in obdelavo osebnih podatkov, ki jih države članice posredujejo Europolu in Eurojustu.

### III.4 **Struktura predloga**

47. Evropski nadzornik za varstvo podatkov je preučil predlog ter zaključil, da predlog na splošno predvideva strukturo varstva v ravneh. Skupni standardi, kakor so določeni v poglavju II predloga (in o določenih zadevah v poglavjih IV–VII), vsebujejo dve ravni varstva:

— prenos splošnih načel varstva podatkov iz Direktive 95/46/ES in drugih pravnih instrumentov Evropskih skupnosti ter Konvencije Sveta Evrope 108 v okvir tretjega stebra;

— dodatna pravila glede varstva podatkov, ki se uporabljajo za vso obdelavo osebnih podatkov znotraj okvira tretjega stebra. Primeri teh dodatnih pravil so v členu 4(3) in (4) predloga.

48. Poglavju III je dodana tretja raven varstva za posebne oblike obdelave. Zdi se, da naslova dveh oddelkov poglavja III in ubeseditev številnih določb predloga kažejo na to, da se to poglavje uporablja zgolj za podatke, posredovane ali dane na voljo s strani pristojnih organov v drugih državah članicah. Zaradi tega se nekatere pomembne določbe za varstvo osebnih podatkov ne bi uporabljale za osebne podatke, če si jih ne bi izmenjale države članice. Besedilo je torej dvoumno, ker se zdi, da same določbe presegajo dejavnosti, ki so neposredno povezane z izmenjanimi podatki. V vsakem primeru omejitev področja uporabe ni izrecno razložena niti utemeljena v obrazložitvenem memorandumu, prav tako ni razložena ali utemeljena presoja vpliva.

49. Evropski nadzornik za varstvo podatkov poudarja dodano vrednost takšne strukture v ravneh, ki lahko zagotovi optimalno varstvo posameznika, na katerega se podatki nanašajo, ob upoštevanju posebnih potreb organov kazenskega pregona. Odraža potrebo po ustreznem varstvu podatkov, kakor je bilo izraženo na spomladanski konferenci aprila 2005 v Krakovu, ter načeloma ustreza členu 8 Listine Evropske unije o temeljnih človekovih pravicah in Evropski konvenciji o varstvu človekovih pravic in temeljnih svoboščin (ECHR), zlasti njenemu členu 8.

50. Vendar pa analiza besedila predloga vodi do naslednjih ugotovitev.

51. Na prvem mestu: treba je zagotoviti, da dodatna pravila za varstvo podatkov v poglavju II (druga raven, omenjena v točki 47) ne odstopajo od splošnih načel varstva podatkov. Evropski nadzornik za varstvo podatkov meni, da bi dodatna pravila v poglavju II morala nuditi dodatno varstvo posameznikov, na katere se podatki nanašajo, in se navezovati na specifično področje tretjega stebra (policijske in pravne informacije). Drugače povedano: nova pravila ne smejo privesti do nižje stopnje varstva.

52. Poleg tega ne sme poglavje III o posebnih oblikah obdelave (kamor je vključena tretja raven varstva) odstopati od poglavja II. Evropski nadzornik za varstvo podatkov meni, da bi morale določbe poglavja III nuditi dodatno varstvo posameznikov, na katere se podatki nanašajo, kadar so vpleteni pristojni organi več držav članic, vendar te določbe ne smejo privesti do nižje stopnje varstva.

53. Na drugem mestu: pravil, ki so splošne narave, se ne vključuje v poglavje III. Evropski nadzornik za varstvo podatkov priporoča, da se te določbe prenesejo v poglavje II. V poglavje III se morajo vključiti le določbe, ki se strogo navezujejo na varstvo osebnih podatkov v primeru izmenjave podatkov med državami članicami. To je toliko pomembnejše, ker poglavje III vsebuje pomembne določbe glede visoke stopnje varstva posameznika, na katerega se podatki nanašajo, v okviru kazenskega pregona (glej IV.1 tega mnenja).

## IV. **ANALIZA ELEMENTOV PREDLOGA**

### IV.1 **Izhodišča analize**

54. Evropski nadzornik za varstvo podatkov bo pri analizi različnih vsebinskih elementov predloga upošteval njegovo posebno strukturo in vsebino. Evropski nadzornik za varstvo podatkov ne bo komentiral posameznih členov predloga.

55. Kot prvič odraža večina določb predloga druge pravne instrumente EU o varstvu osebnih podatkov. Te določbe so skladne s pravnim okvirom EU o varstvu podatkov in zadostne, da zagotovijo ustrezna varovala za varstvo podatkov v tretjem stebru.

56. Vendar pa Evropski nadzornik za varstvo podatkov opozarja, da vsebujejo nekatere določbe, ki so trenutno vključene v poglavje III predloga – o določenih točkah obdelave in ki se na splošno (glej točko 48 tega mnenja) uporabljajo le za podatke, izmenjane z drugimi državami članicami –, splošna in ključna načela zakonodaje EU o varstvu podatkov. Zato bi se morale določbe iz poglavja III prestaviti v poglavje II in se uporabljati za vso obdelavo podatkov s strani organov kazenskega pregona. Sem sodijo določbe, ki se nanašajo na preverjanje kakovosti podatkov (člen 9(1) in (6)) in ki urejajo nadaljnjo obdelavo osebnih podatkov (člen 11(1)).

57. V nekaterih drugih členih poglavja III predloga se ne razlikuje med dodatnimi pogoji, ki se nanašajo posebej na izmenjave podatkov z drugimi državami članicami – kamor sodi soglasje pristojnega organa države članice, ki je poslala podatke –, in varovali, ki pa so pomembna in potrebna tudi glede podatkov, obdelanih v državi članici. V teh primerih Evropski nadzornik za varstvo podatkov priporoča, da se na splošno uporabljajo slednja varovala, tudi za tiste osebne podatke, ki niso bili posredovani ali dani na voljo s strani druge države članice. To priporočilo zadeva:

— prenos podatkov zasebnim strankam in organom, ki niso organi kazenskega pregona (člena 13(a)(b) in 14(a)(b)), in

— prenose tretjim državam ali mednarodnim organom (člen 15 razen točke (c)).

58. Ta del mnenja bo pritegnil tudi pozornost zakonodajalca na nekatera dodatna varovala, ki jih zadevni predlog ne določa. Evropski nadzornik za varstvo podatkov meni, da bi morala biti ta dodatna varovala določena glede na samodejne posamezne odločitve, osebne podatke, prejete s strani tretjih držav, glede na dostop do podatkovnih baz zasebnih strank, obdelavo biometričnih podatkov ter profile DNK.

59. Poleg tega bodo z naslednjo analizo zagotovljena priporočila za izboljšanje sedanjega besedila s ciljem zagotovitve učinkovitosti določb, koherentnosti besedila ter skladnosti z obstoječim pravnim okvirom varstva podatkov.

### IV.2 **Omejitev namena in nadaljnja obdelava**

60. V skladu s členom 4(1)(b) 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. Običajno se bodo podatki zbrali glede na določeno kaznivo dejanje (ali v določenih okoliščinah za preiskavo kriminalne združbe ali mreže, itd.). Lahko se uporabijo za prvotni namen ter se nato obdelajo za drug namen, če je ta v skladu s prvotnim namenom (podatki, zbrani o posamezniku, ki je obsojen prometa s prepovedanimi drogami, bi se lahko uporabili na primer v okviru preiskave mreže preprodajalcev drog). Ta pristop dobro odraža načelo omejitve namena, ker se nahaja tudi v členu 8 Listine Evropske unije o temeljnih človekovih pravicah in se tako sklada z obstoječo zakonodajo na področju varstva podatkov.

*Nadaljnja obdelava v namene v okviru področja delovanja okvirnega sklepa*

61. Evropski nadzornik za varstvo podatkov ugotavlja, da predlog ne obravnava v zadostni meri ene situacije, ki lahko nastane pri policijskem delu: potrebo po nadaljnji uporabi podatkov v namen, ki se šteje kot nezdružljiv z namenom, v katerega so se podatki dejansko zbrali. Podatki, ki jih je zbrala policija, so lahko potrebni za rešitev povsem drugega kaznivega dejanja. Za ponazoritev se lahko navede zbiranje podatkov za preiskavo prometnih prekrškov, ki se nato uporabijo za izsledite in preganjanje tatu avtomobila. Drugi namen, pa čeprav je zakonit, ne more šteti za povsem skladnega z namenom zbiranja podatkov. Če organom kazenskega pregona ne bi bila dovoljena uporaba podatkov za ta drugi namen, bi se lahko nagibali k zbiranju podatkov za široke ali slabo opredeljene namene, pri čemer bi načelo omejitve namena pri zbiranju izgubilo svojo korist. Poleg tega bi bila ovirana uporaba drugih načel, kakršna so sorazmernost, natančnost in zanesljivost (glej člen 4(1)(c) in (d)).

62. V skladu z zakonodajo EU o varstvu podatkov se morajo osebni podatki zbirati v posebne in izrecne namene, ne pa nadalje obdelovati na način, ki je nezdružljiv s temi nameni. Vendar pa Evropski nadzornik za varstvo podatkov meni, da je glede nadaljnje uporabe potrebna določena mera prožnosti. Omejitev zbiranja se bo verjetno bolj spoštovala, če organi, odgovorni za notranjo varnost, vedo, da se lahko z ustreznimi varovali zanesejo na odstopanje od omejitve nadaljnje uporabe.

63. Treba je razjasniti, da se potreba po nadaljnji obdelavi priznava v členu 11 predloga, vendar v nezadostni meri. Člen 11 se uporablja zgolj za podatke, prejete ali dane na voljo s strani pristojnega organa druge države članice, ter ne zagotavlja zadostnih varoval.

64. Evropski nadzornik za varstvo podatkov priporoča uporabo člena 11(1) za vse podatke, ne glede na to, ali so bili prejeti od druge države članice ali ne. Poleg tega je treba določbam člena 11(1)(b) dodati strožja varovala: nadaljnja uporaba podatkov za namen, ki se šteje kot nezdružljiv s prvotnim namenom, naj bi se dovolila le, ko je to nujno potrebno, v posebnem primeru za namen preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali za zaščito interesov ali temeljnih pravic posameznika. Evropski nadzornik za varstvo podatkov dejansko predlaga, da se ta določba določi v novem členu 4a (v vsakem primeru v poglavju II predloga).

65. Člen 11(2)(3) se uporablja v nespremenjeni obliki; zagotavlja dodatna varovala za podatke, prejete od drugih držav članic. Evropski nadzornik za varstvo podatkov opozarja, da se bo člen 11(3) uporabljal za izmenjavo podatkov preko sistema SIS II: Evropski nadzornik za varstvo podatkov je že v svojem mnenju o SIS II omenil, da je treba zagotoviti, da se prav podatki iz sistema SIS ne morejo uporabljati v druge namene kot za namene samega sistema.

*Nadaljnja obdelava za namene izven področja policijskega in pravosodnega sodelovanja*

66. V nekaterih primerih je podatke potrebno obdelati zaradi zaščite drugih pomembnih interesov. V teh primerih lahko podatke obdelajo drugi organi, ki na podlagi tega okvirnega sklepa niso za to pristojni. Te pristojnosti držav članic lahko zajemajo obdelavo, ki posega v zasebnost (na primer preverjanje osebe, ki ni osumljena), in morajo zato biti podvržene zelo strogim pogojem, kot je obveznost držav članic, da sprejmejo posebno zakonodajo, če želijo uporabljati to odstopanje. V okviru prvega stebra to vprašanje obravnava člen 13 Direktive 95/46/ES, ki določa, da so omejitve nekaterih določb te direktive v posebnih primerih dovoljene. Države članice, ki te omejitve uporabljajo, jih morajo uporabljati v skladu s členom 8 ECHR.

67. V skladu z navedenim naj bi ta okvirni sklep v poglavju II določal, da je treba državam članicam dovoliti sprejetje zakonodajnih ukrepov, s katerimi se omogoča nadaljnja obdelava, ko je takšen ukrep potreben za:

— preprečevanje nevarnosti za javno varnost, obrambo ali nacionalno varnost;

— zaščito pomembnega gospodarskega ali finančnega interesa države članice ali Evropske unije;

— varstvo posameznika, na katerega se podatki nanašajo.

### IV.3 **Merila za zakonitost obdelave podatkov**

68. Člen 5 predloga določa, da pristojni organi lahko obdelujejo podatke le, ko zakon navaja, da je obdelava nujna za izpolnitev zakonite naloge zadevnega organa in za namen preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj. Evropski nadzornik za varstvo podatkov podpira stroge zahteve iz člena 5.

69. Vendar besedilo člena 5 podcenjuje potrebo po zakonitosti obdelave podatkov zaradi drugih pravnih razlogov v posebnih okoliščinah. To je pomembna določba, ki ne bi smela onemogočati policije pri izpolnjevanju nacionalnih zakonskih obveznosti glede razkritja informacij uradom za priseljevanje ali davčnim organom. Zato Evropski nadzornik za varstvo podatkov predlaga, da se v členu 5 pri obdelavi osebnih podatkov upoštevajo drugi utemeljeni pravni razlogi, kot je potreba po upoštevanju zakonske obveznosti, ki ji je podvržen upravljavec, nedvoumna privolitev posameznika, na katerega se podatki nanašajo, pod pogojem, da je obdelava izvršena v interesu posameznika, na katerega se podatki nanašajo, ter potrebi po zaščiti pomembnih interesov posameznika, na katerega se podatki nanašajo.

70. Evropski nadzornik za varstvo podatkov opozarja, da ima spoštovanje meril za zakonitost obdelave podatkov poseben pomen v zvezi s policijskim in pravosodnim sodelovanjem, če upoštevamo, da lahko nezakonito zbiranje osebnih podatkov s strani policijskih organov onemogoča uporabo osebnih podatkov kot dokaznega materiala v sodnih postopkih.

### IV.4 **Nujnost in sorazmernost**

71. Namen členov 4 in 5 predloga je zagotoviti, – na splošno zadovoljiv način – da so omejitve varstva osebnih podatkov nujne in sorazmerne, kot zahteva zakonodaja Evropske unije in sodna praksa Evropskega sodišča za človekove pravice v členu 8 ECHR:

— člen 4(1)(c) določa splošno pravilo, po katerem morajo biti osebni podatki primerni, ustrezni in ne pretirani glede na namene, za katere se zbirajo in/ali naprej obdelujejo;

— člen 5 določa, da mora biti obdelava *nujna* za izpolnitev zakonite naloge zadevnega organa in za namen preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj;

— člen 4(4) določa, da je obdelava osebnih podatkov nujna le, če so izpolnjeni nekateri posebni pogoji.

72. Evropski nadzornik za varstvo podatkov opozarja, da predlagano besedilo člena 4(4) ne izpolnjuje meril, ki jih določa sodna praksa Evropskega sodišča za človekove pravice glede člena 8 ECHR, ki navaja, da je omejitev zasebnega življenja možna le, ko je v demokratični družbi nujna. V skladu s predlogom se obdelava podatkov šteje za nujno ne le, ko bo organom kazenskega pregona in pravosodnim organom *omogočala* izvajanje njihovih nalog, temveč tudi, ko na podlagi dejstev *obstajajo razlogi za utemeljen sum*, da bi zadevni osebni podatki le *zagotovili* ali *olajšali* preprečevanje, preiskovanje, odkrivanje ali pregon kaznivega dejanja.

73. Ta merila niso v skladu z zahtevami člena 8 ECHR, ker lahko skoraj vsaka obdelava osebnih podatkov pomeni pospeševanje dejavnosti policijskih ali pravosodnih organov, četudi za izvajanje teh dejavnosti zadevni podatki dejansko niso potrebni.

74. Zdajšnje besedilo člena 4(4) bi ustvarilo razmere za nesprejemljivo veliko zbirko osebnih podatkov, ki temelji le na prepričanju, da lahko osebni podatki *olajšajo* preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj. Nasprotno je obdelava osebnih podatkov nujna le, ko lahko pristojni organi jasno dokažejo, da je potrebna in da ukrepi, ki bi manj posegali v zasebnost, niso na voljo.

75. Evropski nadzornik za varstvo podatkov zato priporoča preoblikovanje prve alinee člena 4(4), da se zagotovi spoštovanje sodne prakse glede člena 8 ECHR. Poleg tega Evropski nadzornik za varstvo podatkov iz sistematičnih razlogov predlaga, da se člen 4(4) premakne na konec člena 5.

### IV.5 **Obdelava posebnih kategorij podatkov**

76. Člen 6 določa načelno prepoved obdelave občutljivih podatkov, t.j. osebnih podatkov, ki kažejo na rasni ali etnični izvor, politična mnenja, verska ali filozofska prepričanja, pripadnost sindikatu, oziroma podatkov v zvezi z zdravjem ali spolnim življenjem. Ta prepoved ne bo veljala, ko obdelavo predvideva zakon in je nujno potrebna za izpolnitev zakonite naloge zadevnega organa za namen preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj. Občutljivi podatki se lahko obdelujejo tudi ko posameznik, na katerega se podatki nanašajo, da izrecno soglasje. V obeh primerih se uvedejo ustrezna posebna varovala.

77. Besedilo člena 6 povzroča dve pripombi. V prvi vrsti se člen 6 preveč zanaša na soglasje posameznika, na katerega se podatki nanašajo. Evropski nadzornik za varstvo podatkov poudarja, da je treba obdelavo občutljivih podatkov na podlagi izrecnega soglasja posameznika, na katerega se podatki nanašajo, dovoliti le, če se ta izvaja v njegovem interesu, zavrnitev soglasja pa zanj ne bi imela negativnih posledic. Evropski nadzornik za varstvo podatkov zato priporoča spremembo člena 6, tudi zaradi njegove uskladitve z veljavno zakonodajo EU o varstvu podatkov.

78. V drugi vrsti Evropski nadzornik za varstvo podatkov meni, da se lahko upoštevajo tudi druge pravne podlage za obdelavo, kot so potreba po varstvu življenjskih interesov posameznika, na katerega se podatki nanašajo, ali druge osebe (kadar posameznik, na katerega se podatki nanašajo, fizično ali pravno ni sposoben dati svoje privolitve).

79. Na področju policijskega in pravosodnega sodelovanja ima obdelava drugih kategorij morebiti občutljivih osebnih podatkov, kot so biometrični podatki in profili DNK, vse večji pomen. Člen 6 predloga teh podatkov izrecno ne zajema. Evropski nadzornik za varstvo podatkov poziva zakonodajalca EU, da nameni posebno pozornost vključitvi splošnih načel o varstvu podatkov, ki jih ta predlog določa, v prihodnjo zakonodajo glede obdelave teh posebnih kategorij podatkov. Primer je zdajšnji predlog okvirnega sklepa Sveta o izmenjavi informacij v skladu z načelom dostopnosti (glej točke 12 do 15), ki izrecno dovoljuje obdelavo in izmenjavo biometričnih podatkov in profilov DNK (glej prilogo II predloga), toda z varnostnega stališča občutljivosti in posebnosti teh podatkov ne obravnava.

80. Evropski nadzornik za varstvo podatkov priporoča, da se določijo posebna varovala, predvsem zaradi zagotovitve, da se:

— biometrični podatki in profili DNK uporabljajo le na podlagi dobro vzpostavljenih in interoperabilnih tehničnih standardov;

— skrbno upošteva stopnja točnosti podatkov in da jo lahko posameznik, na katerega se osebni podatki nanašajo, spodbija s pomočjo zlahka dostopnih sredstev; in

— v celoti zagotovi spoštovanje dostojanstva ljudi.

Zakonodajalec naj odloči, ali naj dodatna varovala zagotovi v tem okvirnem sklepu ali v posebnih pravnih instrumentih, ki urejajo zbiranje in izmenjavo teh posebnih kategorij podatkov.

### IV.6 **Točnost in zanesljivost**

81. Člen 4(1)(d) določa splošna pravila v zvezi s kakovostjo podatkov. V skladu s tem členom mora upravljavec zagotoviti, da so podatki točni in po potrebi posodobljeni. Sprejme vse ustrezne ukrepe za zagotovitev, da se netočni ali nepopolni podatki zbrišejo ali popravijo ob upoštevanju namenov, za katere so bili zbrani ali za katere se nadalje obdelujejo. To je v skladu s splošnimi načeli zakonodaje EU o varstvu podatkov.

82. Tretji stavek člena 4(1)(d) določa, da lahko države članice zagotovijo obdelavo podatkov do različnih stopenj točnosti in zanesljivosti. Za Evropskega nadzornika za varstvo podatkov ta določba pomeni odstopanje od splošnega načela točnosti; na začetku člena 4(1)(d) v tretjem stavku priporoča vstavitev „vendar“ ali „ne glede na to“, da se pojasni odstopanje v določbi. V teh primerih, kadar točnosti podatkov ni možno v celoti zagotoviti, bo upravljavec moral podatke razlikovati glede na stopnjo točnosti in zanesljivosti, predvsem upoštevajoč osnovno razliko med podatki, ki temeljijo na dejstvih, in podatki, ki temeljijo na mnenjih ali osebnih presojah. Evropski nadzornik za varstvo podatkov poudarja pomen te obveznosti za posameznike, na katere se podatki nanašajo, in organe kazenskega pregona, predvsem ko so podatki obdelani daleč od vira (glej točko 7 tega mnenja).

*Preverjanje kakovosti podatkov*

83. Člen 4(1)(d) določa splošno načelo, ki je v členu 9 dopolnjeno z natančnejšimi varovali glede preverjanja kakovosti podatkov. Člen 9 predvsem določa:

1. da se kakovost osebnih podatkov preveri najkasneje do takrat, ko se pošljejo ali dajo na voljo. Poleg tega se podatki, ki so na voljo z neposrednim avtomatičnim dostopom, redno preverjajo (člen 9(1) in (2));

2. da je treba pri vsakem pošiljanju podatkov navesti sodne odločitve in sklepe o nepreganjanju ter podatke, ki temeljijo na mnenjih, preverjenih pri viru preden se pošljejo, in njihovo stopnjo točnosti ali zanesljivosti (člen 9(1));

3. da se osebni podatki označijo na zahtevo posameznika, na katerega se podatki nanašajo, če ta zanika njihovo točnost in če se njihove točnosti ali netočnosti ne da preveriti.

84. Člen (4)(1) in člen 9, če se uporabljata skupaj, zato zagotavljata, da se kakovost osebnih podatkov ustrezno preveri s strani posameznika, na katerega se podatki nanašajo, in s strani organov, ki so najbližji viru obdelanih podatkov, saj so zato v najboljšem položaju, da jih preverijo.

85. Evropski nadzornik za varstvo podatkov pozdravlja te določbe, saj, medtem ko se osredotočajo na potrebe organov kazenskega pregona, zagotavljajo, da se vsak podatek upošteva in uporablja v skladu s točnostjo in zanesljivostjo v izogib temu, da je posameznik, na katerega se podatki nanašajo, preveč prizadet zaradi morebitnega pomanjkanja točnosti nekaterih podatkov, ki se nanj ali nanjo nanašajo.

86. Preverjanje kakovosti podatkov je pomemben element varstva posameznika, na katerega se podatki nanašajo, predvsem v zvezi z osebnimi podatki, ki jih obdelujejo policijski in pravosodni organi. Evropski nadzornik za varstvo podatkov zato obžaluje, da je uporaba člena 9 glede preverjanja kakovosti podatkov omejena na podatke, ki so posredovani ali dani na voljo drugim državam članicam. To je neugodno, saj pomeni, da bo kakovost osebnih podatkov, ki je pomembna tudi za namene kazenskega pregona, v celoti zagotovljena le, ko se ti podatki posredujejo ali dajo na voljo drugim državam članicam, vendar ne, ko so obdelani v državi članici ([1]). Namesto tega je pomembno, – tako v interesu posameznikov, na katere se podatki nanašajo, kot tudi pristojnih organov – da se zagotovi primerno preverjanje kakovosti v zvezi z vsemi osebnimi podatki, vključno s tistimi, ki jih ni posredovala ali dala na voljo druga država članica.

87. Evropski nadzornik za varstvo podatkov zato priporoča črtanje omejitev glede področja uporabe člena 9(1) in (6) s prestavitvijo teh določb v poglavje II predloga.

*Razlikovanje med različnimi kategorijami podatkov*

88. Člen 4(2) določa obveznost upravljavca, da jasno razlikuje med osebnimi podatki različnih kategorij oseb (osumljeni, obsojeni, priče, žrtve, informatorji, kontaktne osebe, drugi). Evropski nadzornik za varstvo podatkov ta pristop pozdravlja. Čeprav je res, da bi morda organi kazenskega pregona in pravosodni organi morali obdelati podatke, ki se nanašajo na različne kategorije oseb, je pomembno te podatke razlikovati v skladu z različno stopnjo udeležbe v zločinu. Predvsem naj pogoji za zbiranje podatkov, roki, pogoji za zavrnitev dostopa ali informacij posamezniku, na katerega se podatki nanašajo, in načini dostopa do podatkov s strani pristojnih organov odražajo posebnosti različnih kategorij obdelanih podatkov in različnih namenov, za katere so organi kazenskega pregona in pravosodni organi te podatke zbrali.

89. V tem smislu Evropski nadzornik za varstvo podatkov zahteva posebno pozornost glede podatkov v zvezi z osebami, ki niso osumljene. Posebni pogoji in varovala so potrebni za zagotovitev sorazmernosti in preprečitev predsodkov glede oseb, ki niso aktivno vpletene v zločin. Predlog naj zajema dodatne določbe za to kategorijo oseb, da se omeji namen obdelave, določijo natančni roki in omeji dostop do podatkov. Evropski nadzornik za varstvo podatkov priporoča ustrezno spremembo predloga.

([1]) Poleg tega to ne bi bilo v skladu s Priporočilom Sveta Evrope št. R(87) 15 o ureditvi osebnih podatkov v policijskem sektorju, ki ga je Odbor ministrov posredoval državam članicam. Načelo 7.2 predvsem določa, da se v dogovoru z nadzornim organom ali v skladu z nacionalno zakonodajo uvedejo „redna preverjanja“ kakovosti osebnih podatkov.

90. Zdajšnje besedilo predloga vsebuje eno posebno varovalo, ki se nanaša na osebe, ki niso osumljene, in sicer člen 7(1) predloga. Evropski nadzornik za varstvo podatkov meni, da je to pomembno varovalo, predvsem ker državam članicam onemogoča določitev odstopanj. Člen 7(1) žal določa posebna varovala le v zvezi z roki, njegova uporaba pa je omejena na kategorije oseb, omenjene v zadnji alinei člena 4(3) predloga. Zato ne zagotavlja zadovoljivih jamstev in ne zajema celotne skupine oseb, ki niso osumljene ([1]).

91. Tudi podatki, ki se nanašajo na obsojene osebe, zaslužijo posebno pozornost. Kar zadeva te podatke je dejansko treba upoštevati nedavne in prihodnje pobude glede izmenjave kazenskih evidenc ter zagotoviti skladnost ([2]).

92. Na podlagi navedenih pripomb Evropski nadzornik za varstvo podatkov priporoča vstavitev novega odstavka v člen 4, ki zajema:

— dodatne določbe za omejitev namena obdelave, določitev natančnih rokov in omejitev dostopa do podatkov v zvezi z osebami, ki niso osumljene;

— obveznost držav članic, da določijo pravne posledice razlikovanj med osebnimi podatki različnih kategorij oseb, ki odražajo posebnosti različnih kategorij obdelanih podatkov in različnih namenov, za katere so organi kazenskega pregona in pravosodni organi podatke zbrali;

— pravne posledice bi se morale nanašati na pogoje glede zbiranja osebnih podatkov, roke, nadaljnji prenos in uporabo podatkov ter pogoje glede zavrnitve dostopa ali informacij posamezniku, na katerega se podatki nanašajo.

### IV.7 **Roki za shranjevanje osebnih podatkov**

93. Splošna načela glede rokov za shranjevanje osebnih podatkov so določena v členu 4(1)(e) in členu 7(1) predloga. Splošno načelo je, da se osebni podatki hranijo le toliko časa, kolikor je potrebno za namen, za katerega so bili zbrani. To je v skladu z zakonodajo EU o varstvu podatkov ([3]).

94. Ne glede na to se splošna določba iz člena 7(1) uporablja le, „če nacionalna zakonodaja ne določa drugače“. Evropski nadzornik za varstvo podatkov ugotavlja, da je ta izjema zelo splošna in presega odstopanja, ki jih dopušča člen 4(1)(e). Predlaga, da se splošno odstopanje iz člena 7(1) črta ali da se vsaj izrecno omejijo javni interesi, ki državam članicam opravičujejo uporabo tega odstopanja ([4]).

95. Člen 7(2) navaja, da se skladnost z roki zagotovi z ustreznimi postopkovnimi in tehničnimi ukrepi ter se redno preučuje. Evropski nadzornik za varstvo podatkov to določbo pozdravlja, predlaga pa, naj se izrecno navede, da je treba z ustreznimi postopkovnimi in tehničnimi ukrepi zagotoviti avtomatsko in redno brisanje osebnih podatkov po izteku določenega časovnega obdobja.

### IV.8 **Izmenjave osebnih podatkov s tretjimi državami**

96. Učinkovito policijsko in pravosodno sodelovanje znotraj meja EU je vse bolj odvisno od sodelovanja s tretjimi državami in mednarodnimi organizacijami. Trenutno se tako na nacionalni ravni kot na ravni EU preučujejo ali načrtujejo mnoge dejavnosti, namenjene zboljšanju sodelovanja s tretjimi državami ali mednarodnimi organizacijami na področjih kazenskega pregona in pravosodja ([5]). Razvoj tega mednarodnega sodelovanja bo najverjetneje v veliki meri odvisen od izmenjav osebnih podatkov.

97. Zato je bistvenega pomena, da tudi za zbiranje in izmenjavo osebnih podatkov prek meja Unije veljajo načela poštene in zakonite obdelave – kot tudi načela predpisanega postopka na splošno – in da se osebni podatki posredujejo tretjim državam ali mednarodnim organizacijam samo, če zadevne tretje stranke zagotovijo ustrezno stopnjo varstva ali primerna varovala.

---

([1]) Glej zlasti točko 94 tega mnenja.

([2]) Sklep Sveta 2005/876/PNZ o izmenjavi podatkov, izpisanih iz kazenske evidence, je začel veljati 9. decembra. Sklep dodaja nove in pospešuje obstoječe mehanizme za pošiljanje informacij v zvezi z obsodbami, ki temeljijo na obstoječih konvencijah; takšni instrumenti so Evropska konvencija o pravni pomoči v kazenskih zadevah iz leta 1959 in Konvencija o pravni pomoči v kazenskih zadevah med državami članicami iz leta 2000. To besedilo bo kasneje zamenjal natančnejši okvirni sklep Sveta. Na tem področju Komisija načrtuje predlog novega okvirnega sklepa.

([3]) Predlog poleg splošne določbe glede rokov za shranjevanje osebnih podatkov iz člena 7 določa nadaljnje posebne določbe, ki zadevajo osebne podatke, izmenjane z drugimi državami članicami. Člen 9.7 posebej določa, da se osebni podatki izbrišejo:
1. če ti podatki ne bi smeli biti poslani, dani na voljo ali prejeti;
2. po roku, ki ga je sporočil organ, ki je poslal podatke, razen če so osebni podatki nadalje potrebni za sodne postopke;
3. če ti podatki niso več potrebni za namen, za katerega so bili poslani.

([4]) Lahko bi razmislili o omejitvi na boj proti terorizmu in/ali posebne javne namene, navedene v členu 4(1)(e): za zgodovinsko, statistično ali znanstveno uporabo.

([5]) Kot primer glej nedavno sporočilo Komisije o „strategiji glede zunanje razsežnosti območja svobode, varnosti in pravice“ (COM(2005) 491 konč.).

*Prenosi osebnih podatkov v tretje države*

98. EDPS v zvezi s tem pozdravlja člen 15 predloga, ki predvideva varstvo v primeru prenosa pristojnim organom v tretjih državah ali mednarodnim organom. Ta določba iz poglavja III predloga pa velja samo za podatke, prejete ali dane na voljo pri pristojnem organu druge države članice. Posledica te omejitve je, da je sistem varstva podatkov na ravni Evropske unije še vedno pomanjkljiv, kar zadeva podatke, ki niso prejeti od pristojnih organov iz drugih držav članic. Po mnenju Evropskega nadzornika za varstvo podatkov taka pomanjkljivost zaradi naslednjih razlogov ni dopustna.

99. Prvič, stopnja varstva, ki jo zagotavlja zakonodaja EU, se v primeru prenosa v tretjo državo ne sme določati pri viru podatkov – policiji v državi članici, ki posreduje podatke tretji državi, ali policiji v drugi državi članici.

100. Drugič, treba je opozoriti, da pravila, ki urejajo prenose osebnih podatkov v tretje države, predstavljajo temeljno načelo zakonodaje o varstvu podatkov. To načelo ni zgolj ena izmed temeljnih določb Direktive 95/46/ES, temveč je vsebovano tudi v Dodatnem protokolu h Konvenciji 108 ([1]). Skupnih standardov pri varstvu osebnih podatkov iz člena 1 predloga ne bi bilo mogoče zagotoviti, če skupna pravila za prenose osebnih podatkov v tretje države ne bi zajemala vseh postopkov obdelave. Posledično bi bile pravice posameznikov, na katere se podatki nanašajo, kakor jih zagotavlja zadevni predlog, neposredno ogrožene, če bi se osebni podatki lahko posredovali tretjim državam, ki ne nudijo ustrezne stopnje varstva.

101. Tretjič, če bi se področje uporabe teh pravil omejilo na „izmenjane podatke“, bi to pomenilo, da v zvezi s podatki, ki se obdelujejo samo v eni državi, ne bi bilo varoval: paradoksalno bi se lahko osebni podatki v tretje države – ob zanemarjanju vsakršnega ustreznega varstva osebnih podatkov – posredovali „enostavneje“ kot v druge države članice. S tem bi se dopustila možnost „pranja informacij“. Pristojni organi držav članic bi lahko obšli stroge norme glede varstva podatkov, tako da bi podatke poslali tretjim državam ali mednarodnim organizacijam, kjer bi lahko bili dostopni pristojnemu organu druge države članice oziroma bi se temu organu lahko celo poslali nazaj.

102. Evropski nadzornik za varstvo podatkov zato priporoča spremembo zadevnega predloga, s katero se zagotovi, da se člen 15 uporablja za izmenjavo *vseh* osebnih podatkov s tretjimi državami. To priporočilo ne zadeva člena 15(1)(c), ki lahko po svoji naravi velja zgolj za osebne podatke, izmenjane z drugimi državami članicami.

*Izjemni prenosi v države, kjer ni ustreznega varstva*

103. Člen 15 določa vrsto pogojev za prenose pristojnim organom v tretjih državah ali mednarodnim organizacijam, primerljivih s pogoji iz člena 25 Direktive 95/46/ES. Kljub temu pa člen 15(6) dopušča možnost prenosa podatkov tretjim državam ali mednarodnim organizacijam, pri katerih ni zagotovljena ustrezna stopnja varstva podatkov, če je prenos nujno potreben zaradi zaščite osnovnih interesov države članice ali zaradi preprečevanja neposredne hude nevarnosti, ki grozi javni varnosti ali določeni osebi ali osebam.

104. Treba je pojasniti uporabo izjeme, ki jo določa odstavek 6. Evropski nadzornik za varstvo podatkov zato priporoča:

— naj se jasno navede, da ta izjema določa zgolj odstopanje od pogoja „ustreznega varstva“ in ne posega v druge pogoje iz prvega odstavka člena 15;

— naj se doda, da morajo za prenose podatkov, ki se izvedejo v skladu s to izjemo, veljati ustrezni pogoji (kot je izrecen pogoj, da se podatki obdelujejo le začasno in za posebne namene) in da se sporočijo pristojnemu nadzornemu organu.

*Obdelava osebnih podatkov, prejetih iz tretjih držav*

105. Glede na to, da se s policijskimi in pravosodnimi organi tretjih držav izmenja vedno več osebnih podatkov, je treba posebno pozornost nameniti osebnim podatkom, „uvoženim“ iz tistih tretjih držav, kjer niso zagotovljeni ustrezni standardi spoštovanja človekovih pravic – zlasti kar zadeva varstvo osebnih podatkov.

([1]) Dodatni protokol h Konvenciji o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov v zvezi z nadzornimi organi in čezmejnim prenosom podatkov je bil podpisan 8.11.2001, veljati pa je začel 1.7.2004. Ta zavezujoč mednarodni pravni instrument je do sedaj podpisalo 11 držav (med njimi 9 članic EU). Člen 2.1 Protokola določa splošno načelo, da vsaka pogodbenica zagotovi prenos osebnih podatkov prejemniku, za katerega velja zakonodaja države ali organizacije, ki ni pogodbenica Konvencije, samo če ta država ali organizacija zagotavlja ustrezno stopnjo varstva za nameravan prenos podatkov.

106. Gledano širše, je Evropski nadzornik za varstvo podatkov mnenja, da mora zakonodajalec zagotoviti skladnost osebnih podatkov, prejetih iz tretjih držav, vsaj z mednarodnimi standardi v zvezi s spoštovanjem človekovih pravic. Na primer, podatkov, pri zbiranju katerih je prišlo do mučenja ali kršitve človekovih pravic, „črnih list“, zasnovanih zgolj na političnem prepričanju ali spolni usmerjenosti, organi kazenskega pregona in pravosodni organi ne smejo obdelovati in uporabljati, razen če to storijo v korist posameznika, na katerega se podatki nanašajo. Evropski nadzornik za varstvo podatkov zato priporoča, da se to pojasni vsaj v uvodni izjavi predloga, po možnosti s sklicevanjem na ustrezne mednarodne instrumente ([1]).

107. S posebnim ozirom na varstvo osebnih podatkov Evropski nadzornik za varstvo podatkov opozarja, naj se za osebne podatke, ki jih pošljejo države, kjer ni ustreznih standardov in jamstev za varstvo osebnih podatkov, ustrezno preveri, ali je njihova kakovost morda pomanjkljiva, da bi se organi kazenskega pregona EU tako izognili zmotni uporabi takih informacij in ne bi delovali v škodo posameznikov, na katere se podatki nanašajo.

108. Evropski nadzornik za varstvo podatkov zato priporoča, da se členu 9 predloga doda določba, ki navaja, da je treba kakovost osebnih podatkov, poslanih iz tretjih držav, posebej preveriti takoj ob prejemu ter navesti stopnjo točnosti in zanesljivosti teh podatkov.

### IV.9 **Izmenjave osebnih podatkov z zasebnimi strankami in organi, ki niso organi kazenskega pregona**

109. Člena 13 in 14 predloga določata vrsto zahtev, ki se morajo izpolniti v primerih, kadar se osebni podatki pošljejo naprej zasebnim strankam in organom, ki niso organi kazenskega pregona. Kot že rečeno, ta člena dopolnjujeta bolj splošna pravila iz poglavju II, ki jih je treba vedno upoštevati.

110. Evropski nadzornik za varstvo podatkov je mnenja, da se morajo za prenos podatkov zasebnim strankam in drugim javnim organom uporabljati posebni in strogi pogoji, četudi je ta v posameznih primerih nujen za namen preprečevanja kriminala in boja proti njemu. To je v skladu s stališčem, ki so ga evropski komisarji za varstvo podatkov izrazili v pogajalskem izhodišču iz Krakova ([2]).

111. V zvezi s tem EDPS meni, da bi dodatni pogoji iz členov 13 in 14 lahko zadostovali, če bi se ti uporabljali skupaj s splošnimi pravili iz poglavja II, vključno s popolno uporabo pravil o nadaljnji obdelavi (glej IV. 2 zgoraj). Kljub temu pa trenutni predlog omejuje uporabo členov 13 in 14 na osebne podatke, prejete ali dane na voljo pri pristojnih organih druge države članice.

112. Splošna uporaba omenjenih pogojev se zdi še pomembnejša, če upoštevamo, da se med organi kazenskega pregona in drugimi organi ali zasebnimi strankami tudi znotraj držav članic izmenjuje vedno več podatkov. Kot primer lahko navedemo sodelovanje med zasebnim in javnim sektorjem pri dejavnostih na področju kazenskega pregona ([3]).

113. Evropski nadzornik za varstvo podatkov zato priporoča, da se zadevni predlog spremeni tako, da bo zagotovljena uporaba členov 13 in 14 pri izmenjavi *vseh* osebnih podatkov, tudi tistih, ki jih ne pošlje ali da na voljo druga država članica. To priporočilo ne velja za člena 13(c) in 14(c).

*Dostop do osebnih podatkov, s katerimi upravljajo zasebne stranke, in njihova nadaljnja uporaba*

114. Izmenjava osebnih podatkov z zasebnimi strankami poteka v dveh smereh: pomeni tudi to, da zasebne stranke osebne podatke pošiljajo ali dajejo na voljo organom kazenskega pregona in pravosodnim organom.

115. V tem primeru so osebni podatki, zbrani za komercialne namene (trgovinsko poslovanje, trženje, opravljanje storitev itd.) in s katerimi upravljajo zasebni upravljavci, pozneje dostopni javnim organom, ki jih uporabljajo za povsem drugačen namen preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj. Poleg tega naj se skrbno presodi točnost in zanesljivost podatkov, obdelanih za komercialne namene, kadar se ti podatki uporabljajo za namene kazenskega pregona ([4]).

([1]) Konvencija ZN proti mučenju in drugim krutim, nečloveškim ali poniževalnim kaznim ali ravnanju, ki so jo podpisale vse države članice EU in je začela veljati 26. junija 1987. Zlasti člen 15, ki se glasi: „Vsaka država članica mora zagotoviti, da nobena izjava, za katero se ugotovi, da je bila dobljena z mučenjem, ne bo uporabljena kot dokaz v nobenem postopku, razen v postopku proti osebi, ki je obtožena mučenja in to le kot dokaz, da je bila izjava pridobljena z mučenjem.“

([2]) *Pogajalsko izhodišče za kazenski pregon in izmenjavo informacij v EU*, sprejeto na spomladanski konferenci evropskih organov za varstvo podatkov v Krakovu, 25. in 26. aprila 2005.

([3]) Glej Zakonodajni in delovni program Komisije za leto 2006, COM(2005) 531 konč.

([4]) Na primer, telefonski račun bo za komercialne namene uporaben, če le pravilno navaja opravljene telefonske klice; isti telefonski račun pa za organe kazenskega pregona ne more biti popolnoma zanesljiv kot trden dokaz glede tega, kdo je opravil določen telefonski klic.

116. V zvezi z dostopom do zasebnih podatkovnih baz za namene kazenskega pregona ima velik pomen nedavno odobreno besedilo Direktive o hrambi komunikacijskih podatkov (glej točke 16–18 zgoraj), v skladu s katerim bodo morali ponudniki javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij za obdobje do dveh let hraniti določene podatke o komunikacijah ter tako zagotoviti, da bodo ti podatki na voljo za namen preiskovanja, odkrivanja in pregona hudih oblik kriminala. V skladu z odobrenim besedilom vprašanja v zvezi z dostopom do teh podatkov presegajo okvir zakonodaje Skupnosti in jih Direktiva morda ne bo mogla sama urejati. Namesto tega bi ta pomembna vprašanja lahko bila predmet nacionalnega prava ali ukrepa v skladu z naslovom VI PEU ([1]).

117. Evropski nadzornik za varstvo podatkov v svojem mnenju o predlogu te direktive zagovarja širšo razlago Pogodbe ES, saj je omejitev dostopa nujna za zagotovitev ustreznega varstva posameznika, na katerega se podatki nanašajo in čigar komunikacijske podatke je treba hraniti. Evropski zakonodajalec v zgoraj navedeno direktivo žal ni vključil pravil o dostopu.

118. Evropski nadzornik za varstvo podatkov v tem mnenju ponovno poudarja, da se močno zavzema za to, da mora zakonodaja EU določiti skupne standarde glede dostopa in nadaljnje uporabe s strani organov kazenskega pregona. Dokler to ne bo obravnavano v okviru prvega stebra, bi lahko potrebno varstvo zagotovil instrument tretjega stebra. To stališče Evropskega nadzornika za varstvo podatkov je podprto tudi z dejstvom, da se med državami članicami na splošno izmenja vse več podatkov, in z nedavnim predlogom v zvezi z načelom dostopnosti. Različna nacionalna pravila glede dostopa in nadaljnje uporabe ne bi bila v skladu s predlaganim „prostim pretokom“ informacij organov kazenskega pregona po vsej EU, kamor sodijo tudi podatki iz zasebnih podatkovnih baz.

119. Evropski nadzornik za varstvo podatkov zato meni, da bi se morali uporabljati skupni standardi za dostop organov kazenskega pregona do osebnih podatkov, ki jih hranijo zasebne stranke, s čimer bi se zagotovilo, da bi bil dostop dovoljen samo na podlagi jasno opredeljenih pogojev in omejitev. Predvsem bi se moral pristojnim organom dostop dovoliti samo za vsak posamezen primer, pod določenimi pogoji in za določene namene ter pod sodnim nadzorom držav članic.

([1]) V skladu z uvodnimi izjavami Direktive „Vprašanja dostopa do podatkov, ki jih nacionalni javni organi hranijo v skladu s to direktivo za dejavnosti iz prve alinee člena 3(2) Direktive 95/46/ES, ne spadajo v področje prava Skupnosti. Lahko pa so predmet nacionalnega prava ali ukrepa v skladu z Naslovom VI Pogodbe o Evropski uniji, pri čemer morajo ti zakoni ali ukrepi vedno v celoti upoštevati temeljne pravice, saj temeljijo na skupnih ustavnih tradicijah držav članic in so zagotovljene z ECHR. Člen 8 ECHR, kakor ga razlaga Evropsko sodišče za človekove pravice…“

## IV.10 **Pravice posameznika, na katerega se podatki nanašajo**

120. Poglavje IV obravnava pravice posameznika, na katerega se podatki nanašajo, in sicer na način, ki je v splošnem skladen z veljavno zakonodajo o varstvu podatkov in členom 8 Listine EU o temeljnih pravicah.

121. Evropski nadzornik za varstvo podatkov te določbe pozdravlja, saj zagotavljajo usklajen niz pravic za posameznike, na katere se podatki nanašajo, hkrati pa upoštevajo posebne značilnosti obdelave s strani organov kazenskega pregona in pravosodnih organov. To predstavlja pomemben napredek, saj trenutne razmere zaznamuje široka paleta pravil in praks, zlasti kar zadeva pravico do dostopa. Nekatere države članice posamezniku, na katerega se podatki nanašajo, ne dopuščajo dostopa do njegovih podatkov, imajo pa sistem „posrednega dostopa“ (ki ga v imenu posameznika, na katerega se podatki nanašajo, izvaja nacionalni organ za varstvo podatkov).

122. V okviru predloga so možna odstopanja od neposredne pravice do dostopa usklajena. To ima vse večji pomen za državljane – katerih podatke pristojni organi različnih držav članic EU vse bolj obdelujejo in si jih izmenjujejo – , ki tako lahko kot posamezniki, na katere se podatki nanašajo, izkoristijo usklajen niz pravic, ne glede na to, v kateri državi članici so podatki zbrani ali obdelani ([2]).

123. Evropski nadzornik za varstvo podatkov dopušča možnost, da se posameznikom, na katere se podatki nanašajo, omeji pravice v primerih, kadar je to potrebno zaradi preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj. Vsekakor pa naj se uporabi strog preskus sorazmernosti, saj je treba te omejitve obravnavati kot izjeme k temeljnim pravicam posameznikov, na katere se podatki nanašajo. To pomeni, da je treba izjeme omejiti in natančno opredeliti, omejitve pa naj bodo, če je to mogoče, delne in časovno omejene.

124. V zvezi s tem želi Evropski nadzornik za varstvo podatkov pozornost zakonodajalca usmeriti k odstavku 2(a) členov 19, 20 in 21, kjer je določena zelo široka in neopredeljena izjema k pravicam posameznikov, na katere se podatki nanašajo, saj navaja, da se smejo te pravice omejiti, če je to potrebno, „da se omogoči upravljavcu ustrezna izpolnitev zakonitih dolžnosti“. Poleg tega se ta izjema prekriva z določbo pod črko (b), ki dopušča omejitve pravic posameznikov, na katere se podatki nanašajo, kadar je to potrebno, „da bi se izognili

([2]) Poglavje IV obravnava predvsem pravico do informacij (člena 19 in 20) in pravico do dostopa, dosege popravka, izbrisa ali zamrznitve (člen 21). Na splošno ti členi posameznikom, na katere se osebni podatki nanašajo, zagotavljajo pravice, ki so običajno zajamčene z zakonodajo EU o varstvu podatkov, hkrati pa določajo vrsto izjem z namenom upoštevanja posebnosti tretjega stebra. Omejitve pravic posameznikov, na katere se osebni podatki nanašajo, posebej dopuščajo skoraj identične določbe, tako kar zadeva pravico do informacij (člena 19.2 in 20.2) kot tudi pravico do dostopa (člen 21.2).

vplivanju na tekoče preiskave, poizvedbe ali postopke ali izpolnjevanje zakonitih dolžnosti pristojnih organov". Medtem ko bi za to zadnjo izjemo sodili, da je upravičena, se za prvo zdi, da predvideva nesorazmerno omejitev pravic posameznikov, na katere se podatki nanašajo. Evropski nadzornik za varstvo podatkov zato priporoča, da se odstavek 2(a) členov 19, 20 in 21 črta.

125. Poleg tega Evropski nadzornik za varstvo podatkov priporoča, da se členi 19, 20 in 21 popravijo, tako da bo:

— določeno, da omejitve pravic posameznikov, na katere se podatki nanašajo, niso obvezne, se ne uporabljajo za nedoločeno časovno obdobje in so dovoljene „samo" v posebnih primerih, navedenih v členih;

— upoštevano, da mora upravljavec informacije zagotoviti sam in ne na podlagi zahteve posameznika, na katerega se podatki nanašajo;

— členu 19(1)(c) dodano, da je treba zagotoviti tudi informacije o „rokih za hrambo podatkov";

— zagotovljeno (s spremembo člena 20(1) v skladu z drugimi instrumenti EU o varstvu podatkov), da so informacije – kadar podatki niso bili pridobljeni od posameznika, na katerega se podatki nanašajo, ali so bili od njega pridobljeni, ne da bi za to vedel – takemu posamezniku na voljo „najpozneje tedaj, ko se podatki prvič posredujejo";

— zagotovljeno, da se mehanizem za pritožbe zoper zavrnitev ali omejitev pravic posameznikov, na katere se podatki nanašajo, uporablja v primerih omejitve pravice do obveščanja; zadnji stavek člena 19(4) pa se ustrezno spremeni.

*Avtomatizirane posamezne odločitve*

126. Evropski nadzornik za varstvo podatkov obžaluje, da predlog ne obravnava pomembnega vprašanja avtomatiziranih posameznih odločitev. Praktične izkušnje dejansko kažejo, da se organi kazenskega pregona vse bolj poslužujejo uporabe avtomatske obdelave podatkov z namenom ovrednotenja nekaterih osebnih vidikov posameznikov, zlasti za oceno njihove zanesljivosti in ravnanja.

127. Evropski nadzornik za varstvo podatkov sicer priznava, da so ti sistemi v nekaterih primerih morda nujni za izboljšanje učinkovitosti pri dejavnostih na področju kazenskega pregona, vendar opozarja, da morajo za odločitve, ki temeljijo zgolj na avtomatski obdelavi podatkov, veljati strogi pogoji in varovala, kadar imajo te za posameznika pravni učinek ali nanj pomembno vplivajo. V okviru tretjega stebra je to še pomembnejše, saj imajo pristojni organi v tem primeru moč javne prisile in lahko tako njihove odločitve ali ukrepi bolj vplivajo na posameznika oziroma bolj posegajo v njegovo življenje kot bi običajno, če bi te odločitve/ukrepe sprejemale zasebne stranke.

128. Take odločitve ali ukrepi naj se zlasti v skladu s splošnimi načeli varstva podatkov dopustijo samo, če to izrecno določa zakon ali odobri pristojni nadzorni organ, hkrati pa morajo biti podvrženi ustreznim ukrepom, namenjenim varovanju zakonitih interesov posameznika, na katerega se podatki nanašajo. Poleg tega morajo biti posamezniku, na katerega se podatki nanašajo, zlahka dostopna sredstva, s katerimi lahko predstavi svoje stališče, in seznanjen mora biti z utemeljitvijo odločitve, razen če je to nezdružljivo z namenom obdelave podatkov.

129. Zaradi tega Evropski nadzornik za varstvo podatkov priporoča uvedbo posebne določbe o avtomatiziranih posameznih odločitvah, ki bi bila v skladu z veljavno zakonodajo EU o varstvu podatkov.

### IV.11 **Varnost obdelave**

130. V zvezi z varnostjo obdelave člen 24 določa obveznost upravljavca, da izvaja ustrezne tehnične in organizacijske ukrepe, ki so v skladu z določbami ostalih instrumentov EU o varstvu podatkov. Poleg tega odstavek 2 podaja podroben in celovit seznam ukrepov, ki se izvajajo v zvezi z avtomatsko obdelavo podatkov.

131. Evropski nadzornik za varstvo podatkov pozdravlja to določbo, vendar zaradi učinkovitejšega nadzora s strani nadzornih organov predlaga, naj se seznamu ukrepov iz odstavka 2 doda naslednji dodatni ukrep: *„k) izvesti ukrepe za sistematično spremljanje in poročanje o učinkovitosti teh varnostnih ukrepov (sistematični samonadzor varnostnih ukrepov)"* ([1]).

*Prijavljanje podatkov*

132. Člen 10 določa, da se vsako avtomatsko pošiljanje ali prejemanje osebnih podatkov prijavi (v primeru avtomatskega pošiljanja) ali dokumentira (v primeru neavtomatskega pošiljanja), s čimer se omogoči naknadno preverjanje zakonitosti pošiljanja in obdelave podatkov. Te informacije so na voljo pristojnemu nadzornemu organu, če to zahteva.

([1]) V tej zvezi glej tudi 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, objavljeno na www.edps.eu.int

133. Evropski nadzornik za varstvo podatkov to določbo pozdravlja. Kljub temu pa ugotavlja, da se zaradi zagotovitve celovitega nadzora in preverjanja pravilne uporabe osebnih podatkov prijavi ali dokumentira tudi „dostop“ do podatkov. Ta informacija je bistvena, saj se mora učinkovito spremljanje pravilne obdelave osebnih podatkov osredotočiti ne le na zakonitost pošiljanja osebnih podatkov med organi, ampak tudi na zakonitost dostopa, ki ga imajo ti organi ([1]). Evropski nadzornik za varstvo podatkov zato priporoča spremembo člena 10, s čimer bi zagotovili, da se prijavi oziroma dokumentira tudi dostop do podatkov.

V.12 **Pravna sredstva, odgovornost in sankcije**

134. Poglavje VI predloga obravnava pravna sredstva (člen 27), odgovornost (člen 28) in sankcije (člen 29). Na splošno so določbe v skladu z veljavno zakonodajo EU o varstvu podatkov.

135. V zvezi s sankcijami Evropski nadzornik za varstvo podatkov zlasti pozdravlja zahtevo, da morajo biti sankcije v primeru kršitev določb, sprejetih v skladu s tem okvirnim sklepom, učinkovite, sorazmerne in odvračilne. Nadalje kazenske sankcije v primeru namerno storjenih kaznivih dejanj, ki pomenijo hude kršitve določb – predvsem določb s ciljem zagotavljanja zaupnosti in varnosti obdelave – za hujše kršitve zakonodaje o varstvu podatkov zagotavljajo večji odvračilni učinek.

IV. 13 **Spremljanje, nadzor in posvetovalne naloge**

136. Določbe predloga v zvezi s spremljanjem in nadzorom obdelave podatkov kot tudi posvetovanjem glede obdelave podatkov so v veliki meri podobne določbam Direktive 95/46/ES. Evropski nadzornik za varstvo podatkov pozdravlja dejstvo, da se je Komisija v svojem predlogu odločila za že preverjene in dobro delujoče mehanizme, ter predvsem poudarja uvedbo (obveznega) sistema predhodnega preverjanja. Takšen sistem predvideva tako Direktiva 95/46/ES kot tudi Uredba 45/2001/ES, izkazal pa se je kot učinkovit instrument, ki je na razpolago Evropskemu nadzorniku za varstvo podatkov pri nadzoru obdelave podatkov s strani institucij in organov Evropskih skupnosti.

137. Drug instrument za spremljanje in nadzor obdelave podatkov, ki se je prav tako izkazal za učinkovitega, je imenovanje uradnih oseb za varstvo podatkov s strani upravljavca. Ta instrument deluje v več državah članicah. V Uredbi 45/2001/ES je določen kot obvezen instrument in igra ključno vlogo na ravni Evropskih skupnosti. Uradne osebe za varstvo podatkov so administratorji znotraj organizacije, ki na neodvisni osnovi zagotavljajo notranjo uporabo določb o varstvu podatkov.

138. Evropski nadzornik za varstvo podatkov priporoča, da se v predlog vključijo določbe o uradnih osebah za varstvo podatkov. Te določbe bi lahko bile oblikovane podobno kot členi 24–26 Uredbe 45/2005/ES.

139. Predlog okvirnega sklepa je naslovljen na države članice. Zato je logično, da člen 30 predloga predvideva nadzor s strani neodvisnih nadzornih organov. Ta člen je zasnovan na podoben način kot člen 28 Direktive 95/46/ES. Ti nacionalni organi morajo sodelovati med seboj, s skupnimi nadzornimi organi, ustanovljenimi v skladu z naslovom VI Pogodbe EU, in z Evropskim nadzornikom za varstvo podatkov. Poleg tega člen 31 predloga predvideva ustanovitev delovne skupine, ki mora igrati podobno vlogo, kot jo ima Delovna skupina iz člena 29 v prvem stebru. Vsi pomembni akterji na področju varstva podatkov so omenjeni v členu 31 predloga.

140. Samoumevno je, da v predlogu, ki predvideva izboljšanje policijskega in pravosodnega sodelovanja med državami članicami, pomembno vlogo igra tudi sodelovanje med vsemi pomembnimi akterji na področju varstva podatkov. Zato Evropski nadzornik za varstvo podatkov pozdravlja dejstvo, da je velik poudarek v predlogu namenjen sodelovanju med nadzornimi organi.

141. Poleg tega poudarja pomen doslednega pristopa do vprašanj glede varstva podatkov, ki se lahko okrepi s spodbujanjem komunikacije med obstoječo Delovno skupino iz člena 29 in delovno skupino, ustanovljeno v skladu z zadevnim predlogom okvirnega sklepa. Evropski nadzornik za varstvo podatkov predlaga spremembo člena 31(2) predloga, tako da bi imel tudi predsednik Delovne skupine iz člena 29 pravico sodelovati in biti zastopan na sestankih nove delovne skupine.

142. Besedilo člena 31 zadevnega predloga vsebuje eno občutno razliko v primerjavi s členom 29 Direktive 95/46/ES. Evropski nadzornik za varstvo podatkov je polnopraven član Delovne skupine iz člena 29. Članstvo vključuje tudi pravico do glasovanja. Zadevni predlog Evropskega nadzornika za varstvo podatkov prav tako imenuje za člana delovne skupine (na podlagi člena 31), vendar zanj ne predvideva pravice do glasovanja. Razlogi, zakaj zadevni predlog odstopa od člena 29 Direktive 95/46/ES, niso jasni. Po mnenju Evropskega nadzornika za varstvo podatkov je predlagano besedilo dvoumno glede njegove vloge, kar bi lahko oviralo učinkovitost njegovega sodelovanja pri delu delovne skupine. Zato Evropski nadzornik za varstvo podatkov priporoča, da se ohrani skladnost z besedilom Direktive.

([1]) To je v skladu z določbami iz člena 18 predloga, ki določa, da se organ, ki je poslal ali dal na voljo zadevne podatke, obvesti o zahtevi za njihovo nadaljnjo uporabo, in določbami iz člena 24 o izvajanju varnostnih ukrepov, tudi v luči predlaganega sistematičnega samonadzora teh ukrepov.

### IV.14 **Druge določbe**

143. Poglavje VIII predloga vsebuje nekatere končne določbe o spremembi Schengenske konvencije in drugih instrumentov v zvezi z obdelovo in varstvom osebnih podatkov.

*Schengenska konvencija*

144. Člen 33 predloga določa, da se členi 126 do 130 Schengenske konvencije s tem sklepom nadomestijo v zvezi z zadevami, ki spadajo v področje uporabe Pogodbe EU. Členi 126 do 130 Schengenske konvencije vsebujejo splošne predpise o varstvu podatkov glede obdelave podatkov, ki se sporočajo v skladu s Konvencijo (vendar zunaj Schengenskega informacijskega sistema).

145. Evropski nadzornik za varstvo podatkov pozdravlja to nadomestitev, saj pomeni večjo doslednost sistema varstva podatkov v tretjem stebru in v nekaterih pogledih znatno izboljšanje varstva osebnih podatkov, na primer s tem, da dobijo nadzorni organi večja pooblastila. Vendar ima ponekod nenamerno in neugodno posledico zmanjšanja stopnje varstva podatkov. Nekatere določbe Schengenske konvencije so dejansko strožje kot določbe okvirnega sklepa.

146. Evropski nadzornik za varstvo podatkov zlasti omenja člen 126(3)(b) Schengenske konvencije, ki navaja, da lahko podatke uporabljajo samo sodni organi ter službe in organi, ki izvajajo naloge ali dolžnosti v zvezi z nameni, določenimi s Konvencijo. Zdi se, da ta določba izključuje pošiljanje zasebnim strankam, medtem ko bi predlagani okvirni sklep to dopuščal. Poleg tega se določbe o varstvu podatkov iz Schengenske konvencije uporabljajo tudi za *vse* podatke, ki so vključeni v *neavtomatiziranih* podatkovnih zbirkah ali se iz njih sporočajo (člen 127), medtem ko so nestrukturirane podatkovne zbirke izključene iz področja uporabe predlaganega okvirnega sklepa.

*Konvencija o medsebojni pravni pomoči v kazenskih zadevah med državami članicami Evropske unije*

147. Člen 34 določa, da se člen 23 Konvencije o medsebojni pravni pomoči v kazenskih zadevah med državami članicami Evropske unije nadomesti z okvirnim sklepom. Evropski nadzornik za varstvo podatkov opozarja, da čeprav bi ta nadomestitev na splošno zagotovila boljše varstvo osebnih podatkov, ki se izmenjajo v okviru Konvencije, bi hkrati lahko povzročila določene težave glede združljivosti obeh instrumentov.

148. Konvencija posebej obravnava medsebojno pravno pomoč pri prestrezanju telekomunikacij. V tem primeru zaprošena država članica lahko da soglasje za prestrezanje ali prenos snemanj telekomunikacij ob upoštevanju morebitnih pogojev, ki jih je treba spoštovati v podobnem domačem primeru. V skladu s členom 23(4) Konvencije ti dodatni pogoji prevladajo nad predpisi o varstvu podatkov iz člena 23, kadar se nanašajo na uporabo osebnih podatkov. Podobno člen 23(5) določa prednost dodatnih predpisov o varovanju informacij, ki jih zberejo skupne preiskovalne skupine. Evropski nadzornik za varstvo podatkov opozarja, da v primeru zamenjave člena 23 z zadevnim predlogom ne bi bilo jasno, ali zgoraj navedeni dodatni predpisi še vedno veljajo. Zaradi tega Evropski nadzornik za varstvo podatkov priporoča, da se ta točka razjasni in da se posledice popolne nadomestitve člena 23 Konvencije s tem okvirnim sklepom temeljito preučijo.

*Konvencija 108 Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov*

149. Člen 34(2) določa, da se kakršno koli sklicevanje na Konvencijo 108 šteje kot sklicevanje na ta okvirni sklep. Razlaga in praktična uporaba te določbe sta zelo nejasni. V vsakem primeru Evropski nadzornik za varstvo podatkov domneva, da se ta določba nanaša le na področje uporabe *ratione materiae* tega okvirnega sklepa.

*Druga vprašanja*

150. V zvezi s sistematično doslednostjo besedila Evropski nadzornik za varstvo podatkov meni, da bi se lahko nekateri členi v besedilu predloga prerazporedili.

Zato Evropski nadzornik za varstvo podatkov predlaga:

4. člen 16 („Odbor“) iz poglavja III („Posebne oblike obdelave“) naj se prestavi v novo poglavje;

5. člen 25 („Evidenca“) in člen 26 („Predhodno preverjanje“) iz poglavja V („Zaupnost in varnost obdelave“) naj se prestavita v novo poglavje.

## V. **SKLEPI**

*Znaten napredek*

a) Sprejetje tega predloga bi predstavljalo velik napredek na področju varstva osebnih podatkov; to je pomembno področje, ki na ravni Evropske unije zahteva usklajen in učinkovit mehanizem za varstvo osebnih podatkov.

b) Učinkovito varstvo osebnih podatkov ni pomembno le za posameznike, na katere se podatki nanašajo, temveč prispeva tudi k uspešnemu policijskemu in pravosodnemu sodelovanju. Z več vidikov ta dva javna interesa sovpadata.

*Skupni standardi*

c) Evropski nadzornik za varstvo podatkov meni, da bi moral novi okvir za varstvo podatkov spoštovati načela varstva podatkov – pomembno je zagotoviti skladnost varstva podatkov v Evropski uniji – kot tudi zagotoviti dodaten sklop predpisov, ki bi upoštevali posebno naravo področja kazenskega pregona.

d) Zadevni predlog te pogoje izpolnjuje: zagotavlja namreč, da se bodo obstoječa načela varstva podatkov iz Direktive 95/46/ES uporabljala v okviru tretjega stebra, saj večina določb predloga odraža druge pravne instrumente EU o varstvu osebnih podatkov in se z njimi sklada. Poleg tega določa skupne standarde, ki natančno opredeljujejo ta načela z vidika njihove uporabe na tem področju in na splošno zagotavljajo ustrezna varovala za varstvo podatkov v tretjem stebru.

*Veljavno za vso obdelavo*

e) Da bi okvirni sklep dosegel svoj namen, mora zajemati vse policijske in pravosodne podatke, tudi če pristojni organi drugih držav članic zadevnih podatkov niso posredovali ali dali na voljo.

f) Člena 30(1)(b) in 31(1)(c) PEU zagotavljata pravno podlago za predpise o varstvu podatkov, ki niso omejeni na varstvo osebnih podatkov, ki se dejansko izmenjajo med pristojnimi organi držav članic, temveč se uporabljajo tudi za domače primere.

g) Predlog se ne nanaša na obdelavo v okviru drugega stebra Pogodbe EU (skupna zunanja in varnostna politika) niti na obdelavo podatkov s strani obveščevalnih služb ali na njihov dostop do teh podatkov, kadar jih obdelujejo pristojni organi ali druge stranke (to izhaja iz člena 33 PEU). Na teh področjih mora ustrezno varstvo posameznikov, na katere se podatki nanašajo, zagotoviti nacionalna zakonodaja. Ta neenakost v varstvu na ravni EU zahteva še učinkovitejše varstvo na področjih, ki so dejansko zajeta v predlogu.

h) Evropski nadzornik za varstvo podatkov pozdravlja dejstvo, da predlog vključuje tudi osebne podatke, ki jih obdelujejo pravosodni organi.

*V zvezi z drugimi pravnimi instrumenti*

i) Kadar koli kakšen drug poseben pravni instrument iz naslova VI Pogodbe EU predvideva natančnejše pogoje ali omejitve za obdelavo ali dostop do podatkov, naj se poseben pravni instrument uporablja kot *lex specialis*.

j) Zadevni predlog okvirnega sklepa Sveta o varstvu podatkov ima določene prednosti in je zato potreben, tudi če ne bo sprejet pravni instrument v zvezi z dostopnostjo (kakor je predlagala Komisija 12. oktobra 2005).

k) Ker je Evropski parlament odobril direktivo o hrambi komunikacijskih podatkov, je postala vzpostavitev pravnega okvira za varstvo podatkov v tretjem stebru še bolj nujna.

*Struktura predloga*

l) Dodatni predpisi v poglavju II (poleg splošnih načel Direktive 95/46/ES) bi morali nuditi dodatno varstvo posameznikov, na katere se podatki nanašajo, glede na specifičen okvir tretjega stebra, vendar ne smejo povzročiti nižje stopnje varstva.

m) Poglavje III o posebnih oblikah obdelave (kamor je vključena tretja raven varstva) ne sme odstopati od poglavja II: določbe poglavja III bi morale nuditi dodatno varstvo posameznikov, na katere se podatki nanašajo, kadar so vpleteni pristojni organi več držav članic, vendar te določbe ne smejo povzročiti nižje stopnje varstva.

n) Določbe, ki se nanašajo na preverjanje kakovosti podatkov (člen 9(1) in (6)) in ki urejajo nadaljnjo obdelavo osebnih podatkov (člen 11(1)), bi se morale prestaviti v poglavje II in se uporabljati za vso obdelavo podatkov s strani organov kazenskega pregona, tudi če osebne podatke ni poslala ali dala na voljo druga država članica. Zlasti je pomembno – tako v interesu posameznikov, na katere se podatki nanašajo, kot tudi pristojnih organov –, da se zagotovi primerno preverjanje kakovosti v zvezi z vsemi osebnimi podatki.

*Omejitev namena*

o) Predlog ne obravnava v zadostni meri ene situacije, ki lahko nastane pri policijskem delu: potrebe po nadaljnji uporabi podatkov za namen, ki se šteje kot nezdružljiv z namenom, za katerega so se podatki dejansko zbrali.

p) V skladu z zakonodajo EU o varstvu podatkov se morajo osebni podatki zbirati v posebne in izrecne namene, ne pa nadalje obdelovati na način, ki je nezdružljiv s temi nameni. Glede nadaljnje uporabe je potrebna določena mera prožnosti. Omejitev zbiranja se bo verjetno bolj spoštovala, če organi, odgovorni za notranjo varnost, vedo, da se lahko z ustreznimi varovali zanesejo na odstopanje od omejitev nadaljnje uporabe.

q) Okvirni sklep bi moral v poglavju II določiti, da je treba državam članicam omogočiti, da sprejmejo zakonodajne ukrepe, ki bi dopuščali nadaljnjo obdelavo, kadar je ta ukrep potreben za:

— preprečevanje nevarnosti za javno varnost, obrambo ali nacionalno varnost;

— zaščito pomembnega gospodarskega ali finančnega interesa države članice;

— varstvo posameznika, na katerega se podatki nanašajo.

Te pristojnosti držav članic bi lahko vključevale obdelavo, ki posega v zasebnost, in bi jih torej morali spremljati zelo strogi pogoji.

*Nujnost in sorazmernost*

r) Načeli nujnosti in sorazmernosti bi morali v predlogu v celoti odražati sodno prakso Evropskega sodišča za človekove pravice in torej zagotoviti, da se obdelava osebnih podatkov šteje za potrebno, samo kadar lahko pristojni organi jasno dokažejo to potrebo in pod pogojem, da ukrepi, ki bi manj posegali v zasebnost, niso na voljo.

*Izmenjave osebnih podatkov s tretjimi državami*

s) Če bi bilo možno podatke poslati v tretjo državo brez zagotovitve varstva posameznika, na katerega se podatki nanašajo, bi to resno škodovalo varstvu, ki je predvideno v zadevnem predlogu na ozemlju Evropske unije. Evropski nadzornik za varstvo podatkov priporoča spremembo zadevnega predloga, s katero se zagotovi, da se člen 15 uporablja za izmenjavo *vseh* osebnih podatkov s tretjimi državami. To priporočilo ne velja za člen 15(1)(c).

t) Ko se osebni podatki pošiljajo iz tretjih držav, je treba skrbno presoditi njihovo kakovost z vidika spoštovanja človekovih pravic in standardov za varstvo podatkov, še preden se ti podatki uporabijo.

*Izmenjave osebnih podatkov z zasebnimi strankami in organi, ki niso organi kazenskega pregona*

u) Prenos podatkov zasebnim strankam in drugim javnim organom je lahko v posameznih primerih nujen za namen preprečevanja kriminala in boja proti njemu, vendar se morajo uporabljati posebni in strogi pogoji. Evropski nadzornik za varstvo podatkov priporoča, da se zadevni predlog spremeni tako, da bo zagotovljena uporaba členov 13 in 14 pri izmenjavi *vseh* osebnih podatkov, tudi tistih, ki jih ne prejme ali da na voljo druga država članica. To priporočilo ne velja za člena 13(c) in 14(c).

v) Uporabljati bi se morali skupni standardi za dostop organov kazenskega pregona do osebnih podatkov, ki jih hranijo zasebne stranke, s čimer bi se zagotovilo, da bi bil dostop dovoljen samo na podlagi jasno opredeljenih pogojev in omejitev.

*Posebne kategorije podatkov*

w) Treba je zagotoviti posebna varovala, zlasti da se zagotovi:

— da se biometrični podatki in profili DNK uporabljajo le na podlagi dobro vzpostavljenih in interoperabilnih tehničnih standardov,

— da se stopnja njihove točnosti skrbno upošteva in da jo lahko posameznik, na katerega se podatki nanašajo, spodbija s pomočjo zlahka dostopnih sredstev in

— da se v celoti zagotovi spoštovanje dostojanstva ljudi.

*Razlikovanje med različnimi kategorijami podatkov*

x) Osebni podatki v zvezi z različnimi kategorijami oseb (osumljeni, obsojeni, žrtve, priče itd.) bi se morali obdelovati v skladu z različnimi ustreznimi pogoji in varovali. Zato Evropski nadzornik za varstvo podatkov predlaga, da se členu 4 doda nov odstavek, ki vsebuje naslednje elemente:

— obveznost držav članic, da določijo pravne posledice v zvezi z razlikami, ki naj se uvedejo za osebne podatke različnih kategorij oseb;

— dodatne določbe, ki omejijo namen obdelave, določijo natančne roke, in omejijo dostop do podatkov, če gre za osebe, ki niso osumljenci.

*Avtomatizirane posamezne odločitve*

y) Za odločitve, ki temeljijo zgolj na avtomatski obdelavi podatkov, morajo veljati strogi pogoji, kadar imajo te za posameznika pravni učinek ali nanj pomembno vplivajo. Zato Evropski nadzornik za varstvo podatkov priporoča, da se uvedejo posebne določbe o avtomatiziranih posameznih odločitvah, ki bi bile podobne določbam iz Direktive 95/46/ES.

*Izbor ostalih priporočil*

z) Evropski nadzornik za varstvo podatkov priporoča:

— preoblikovanje prve alinee člena 4(4), da se zagotovi upoštevanje sodne prakse glede člena 8 ECHR, saj predlagano besedilo člena 4(4) ne izpolnjuje meril, ki jih določa sodna praksa Evropskega sodišča za človekove pravice v zvezi s členom 8 ECHR;

— črtanje širokega odstopanja iz člena 7(1) ali vsaj izrecno omejitev javnih interesov, ki državam članicam opravičujejo uporabo tega odstopanja;

— spremembo člena 10, s čimer se zagotovi, da se prijavi oziroma dokumentira tudi dostop do podatkov;

— črtanje odstavka 2(a) členov 19, 20 in 21;

— vključitev določb o uradnih osebah za varstvo podatkov v predlog. Te določbe bi lahko bile oblikovane podobno kot členi 24–26 Uredbe 45/2005/ES;

— spremembo člena 31(2) predloga, tako da bi imel tudi predsednik Delovne skupine iz člena 29 pravico sodelovati in biti zastopan na sestankih nove delovne skupine.

V Bruslju, 19. decembra 2005,

Peter HUSTINX

*Evropski nadzornik za varstvo podatkov*