I

(Resolucije, priporočila in mnenja)

MNENJA

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o predlogu direktive Evropskega parlamenta in Sveta o spremembi direktiv 89/666/EGS, 2005/56/ES in 2009/101/ES glede povezovanja centralnih in trgovinskih registrov ter registrov družb

(2011/C 220/01)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 16 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah ter zlasti členov 7 in 8 Listine,

ob upoštevanju Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov [1],

ob upoštevanju prošnje za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov [2] –

SPREJEL NASLEDNJE MNENJE:

I. **UVOD**

1. Evropska komisija je 24. februarja 2011 sprejela predlog direktive Evropskega parlamenta in Sveta o spremembi direktiv 89/666/EGS, 2005/56/ES in 2009/101/ES glede povezovanja centralnih in trgovinskih registrov ter registrov družb [3] (v nadaljnjem besedilu: predlog) ter se naknadno posvetovala z Evropskim nadzornikom za varstvo podatkov (v nadaljnjem besedilu: ENVP).

2. ENVP je zadovoljen, da je bil v skladu s členom 28(2) Uredbe št. 45/2001 zaprošen za mnenje in da je sklic na to mnenje vključen v preambulo predloga.

1.1 **Cilji predloga**

3. Cilj predloga je lajšati in krepiti čezmejno sodelovanje in izmenjavo informacij med poslovnimi registri v evropskem gospodarskem prostoru, s čimer naj bi se povečali preglednost in zanesljivost čezmejno razpoložljivih infomacij. Učinkoviti postopki upravnega sodelovanja v zvezi s poslovnimi registri so ključni za povečanje zaupanja v enotni evropski trg z zagotavljanjem varnejšega poslovnega okolja za potrošnike, upnike in druge poslovne partnerje, z zmanjšanjem upravne obremenitve in povečanjem pravne varnosti. Izboljšanje postopkov upravnega sodelovanja v zvezi s poslovnimi registri v Evropi je zlasti pomembno v postopkih čezmejnih združitev, prenosov sedeža in posodabljanja registracije tujih podružnic, kjer mehanizmov sodelovanja ni ali pa so omejeni.

4. Za ta namen je cilj predloga spremeniti tri veljavne direktive, kot sledi:

[1] UL L 281, 23.11.1995, str. 31.
[2] UL L 8, 12.1.2001, str. 1.
[3] Zaradi jedrnatosti se v nadaljevanju tega mnenja namesto izraza „centralni in trgovinski registri ter registri družb“ uporablja izraz „poslovni registri“.

— cilj sprememb Direktive 2009/101/ES ([1]) je z (i) vzpostavitvijo elektronskega omrežja poslovnih registrov in z (ii) določitvijo skupnega minimalnega niza najnovejših informacij, ki morajo biti elektronsko dostopne tretjim osebam prek enotnega evropskega večjezičnega vmesnika/točke dostopa, olajšati čezmejni dostop do uradnih poslovnih informacij,

— namen sprememb Direktive 89/666/EGS ([2]) je zagotoviti, da poslovni register družbe poslovnemu registru tujih podružnic v vsej Evropi zagotavlja najnovejše informacije o položaju družbe, in, končno,

— cilj sprememb Direktive 2005/56/ES ([3]) je izboljšati postopke upravnega sodelovanja med poslovnimi registri v postopkih čezmejnih združitev.

1.2 **Ozadje predloga**

5. Poslovne registre imajo vse države članice in so organizirani na nacionalni, regionalni ali lokalni ravni. Leta 1968 so bila sprejeta skupna pravila za oblikovanje minimalnih standardov za razkritje (vpis in objavo) poslovnih informacij ([4]). Države članice morajo od 1. januarja 2007 voditi tudi elektronske poslovne registre ([5]) in tretjim stranem omogočati spletni dostop do vsebine registra.

6. Nekateri evropski pravni instrumenti izrecno zahtevajo sodelovanje v zvezi s poslovnimi registri iz različnih držav članic za lajšanje čezmejnih združitev kapitalskih družb ([6]) ter čezmejnega prenosa sedeža evropske družbe (SE) ([7]) in evropske zadruge (SCE) ([8]).

7. V zvezi s poslovnimi registri v Evropi je bil leta 1992 oblikovan mehanizem prostovoljnega sodelovanja. Tako imenovani evropski poslovni register (v nadaljnjem besedilu: EBR) ([9]) zdaj združuje uradne poslovne registre iz 19 držav članic in šestih drugih evropskih jurisdikcij. EBR je med letoma 2006 in 2009 sodeloval v raziskovalnem projektu, imenovanem BRITE ([10]), katerega cilj je bil razviti tehnološki vmesnik za interoperabilnost poslovnih registrov po vsej Evropi. V oceni učinka, priloženi predlogu, pa je pojasnjeno, da se EBR spopada s pomembnimi izzivi v zvezi s širitvijo, financiranjem in upravljanjem: glede na oceno učinka mehanizem sodelovanja v svoji zdajšnji obliki ni v celoti zadovoljiv za morebitne uporabnike.

1.3 **Sinergije z drugimi pobudami**

8. V obrazložitvenem memorandumu, priloženem predlogu, je navedeno, da bo evropski portal e-pravosodja ([11]) postal ključna točka dostopa do pravnih informacij, pravnih in upravnih ustanov, registrov, zbirk podatkov in drugih storitev v EU. Poleg tega je v njem potrjeno, da predlog dopolnjuje projekt e-pravosodja in naj bi prispeval k lažjemu dostopu tretjih strani do poslovnih informacij prek portala.

9. V skladu z oceno učinka je drug pomemben projekt z mogočimi sinergijami informacijski sistem za notranji trg (v nadaljnjem besedilu: IMI) ([12]). IMI je elektronsko orodje, načrtovano za podporo tekočemu upravnemu sodelovanju med javnimi upravami v okviru direktive o storitvah (2006/123/ES) in direktive o poklicnih kvalifikacijah (2005/36/ES). Orodje IMI je trenutno v postopku širitve in bi lahko v skladu z oceno učinka pripomoglo tudi k izvrševanju drugih direktiv, vključno na področju prava gospodarskih družb.

II. **POMEMBNE DOLOČBE PREDLOGA**

10. Člen 3 predloga spreminja Direktivo 2009/101/ES v več pogledih. Od teh sta dve spremembi zelo pomembni za varstvo podatkov.

([1]) Direktiva 2009/101/ES Evropskega parlamenta in Sveta z dne 16. septembra 2009 o uskladitvi zaščitnih ukrepov za varovanje interesov družbenikov in tretjih oseb, ki jih države članice zahtevajo od gospodarskih družb v skladu z drugim pododstavkom člena 48 Pogodbe, zato da se oblikujejo zaščitni ukrepi z enakim učinkom v vsej Skupnosti (UL L 258, 1.10.2009, str. 11).

([2]) Enajsta direktiva Sveta 89/666/EGS z dne 21. decembra 1989 o razkritjih podružnic, ki jih v državi članici odprejo nekatere oblike družb, za katere velja zakonodaja druge države (UL L 395, 30.12.1989, str. 36).

([3]) Direktiva Evropskega parlamenta in Sveta 2005/56/ES z dne 26. oktobra 2005 o čezmejnih združitvah kapitalskih družb (UL L 310, 25.11.2005, str. 1).

([4]) Direktiva 2009/101/ES, v celoti navedena zgoraj. V členu 1 Direktive je področje uporabe določb Direktive omejeno na „companies incorporated with limited liability".

([5]) Direktiva 2003/58/ES Evropskega parlamenta in Sveta z dne 15. julija 2003 o spremembah Direktive Sveta 68/151/EGS glede zahtev za objavo nekaterih vrst družb (UL L 221, 4.9.2003, str. 13).

([6]) Direktiva 2005/56/ES, v celoti navedena zgoraj.

([7]) Uredba (ES) št. 2157/2001 z dne 8. oktobra 2001 o statutu evropske družbe (UL L 294, 10.11.2001, str. 1).

([8]) Uredba (ES) št. 1435/2003 z dne 18. avgusta 2003 o statutu evropske zadruge (UL L 207, 18.8.2003, p. 1).

([9]) http://www.ebr.org/

([10]) http://www.briteproject.eu

([11]) https://e-justice.europa.eu/home.do

([12]) http://ec.europa.eu/internal_market/imi-net/index_en.html

2.1 **Objava informacij prek enotnega evropskega elektronskega vmesnika/točke dostopa**

11. Člen 2 veljavne Direktive 2009/101/ES že zahteva, da se v poslovnem registru v vsaki državi članici objavijo nekatere minimalne informacije, da tretje strani lahko preverijo informacije o družbah. Kot je pojasnjeno v oddelku 1.2 zgoraj, morajo države članice voditi tudi elektronske poslovne registre in tretjim stranem omogočiti spletni dostop do vsebine teh registrov.

12. V členu 2 je naštetih enajst osnovnih informacij o družbah, ki jih je treba objaviti, vključno s/z:

— aktom o ustanovitvi, statutom ter vsemi spremembami akta o ustanovitvi in statuta,

— vpisanim kapitalom,

— računovodskimi listinami,

— spremembo registriranega sedeža družbe,

— prenehanjem družbe, izjavo o ničnosti, imenovanjem likvidacijskih upraviteljev, ustavitvijo postopka likvidacije in izbrisom družbe iz registra.

13. Z vidika varstva podatkov je pomembno, da člen 2 zahteva tudi razkritje „imenovanja, odpoklica in podatkov“ (dodan poudarek) o osebah, ki so (i) pooblaščene za zastopanje družbe in/ali (ii) kako drugače udeležene pri „upravljanju, nadzoru ali obvladovanju“.

14. Seznam informacij, ki jih je treba razkriti v skladu s členom 2, je v predlogu ostal nespremenjen. Nova ni niti zahteva, da mora vsaka država članica omogočiti javni elektronski dostop do teh informacij. Novost predloga je, da bodo informacije, ki so bile doslej na voljo razdrobljeno, pogosto le v lokalnih jezikih in prek lokalnih spletnih strani, zdaj zlahka dostopne prek enotnega evropskega vmesnika/točke dostopa v večjezičnem okolju.

15. Zato bi predlog vstavil nov člen 3a v direktivo, s čimer bi določil, da „[d]ržave članice zagotovijo, da vlagatelj lahko na zahtevo v elektronski obliki prek enotnega evropskega elektronskega vmesnika, ki je dostopen iz vsake države članice, dobi dokumente in podatke iz člena 2, ki so bili vpisani v njihov register“. Predlog prepušča vse nadaljnje podrobnosti delegiranim aktom.

2.2 **Interoperabilnost in povezovanje poslovnih registrov: vzpostavitev elektronskega omrežja**

16. Predlog bi poleg tega vstavil nov člen 4a v isto Direktivo 2009/101/ES, s čimer bi določil, da „[d]ržave članice sprejmejo potrebne ukrepe za zagotovitev, da so [poslovni registri] interoperabilni in tvorijo elektronsko omrežje“. Predlog spet prepušča nadaljnje podrobnosti delegiranim aktom.

2.3 **Določbe o varstvu podatkov**

17. Predlog bi za obravnavo pomislekov v zvezi z varstvom podatkov v besedilo vseh treh direktiv, ki jih je treba spremeniti, vstavil poseben člen o varstvu podatkov, ki določa, da „[z]a obdelavo osebnih podatkov, ki se opravlja v okviru te direktive, velja Direktiva 95/46/ES“.

III. **PRIPOMBE IN PRIPOROČILA EVROPSKEGA NADZORNIKA ZA VARSTVO PODATKOV**

3.1 **Uvod: izpolnjevanje potreb po preglednosti in zasebnosti**

18. ENVP se strinja s Komisijo, da (i) lahko uporaba informacijskih in komunikacijskih tehnologij prispeva k učinkovitejšemu sodelovanju v zvezi s poslovnimi registri ter (ii) da lahko večja dostopnost informacij iz poslovnega registra omogoča večjo preglednost. Zato podpira cilje predloga. Njegove pripombe je treba ovrednotiti z vidika tega konstruktivnega pristopa.

19. ENVP hkrati še poudarja, da večja dostopnost osebnih podatkov vodi tudi k večjim tveganjem za osebne podatke. Medtem ko bi bila na primer ustrezna identifikacija zastopnika družbe lažja, če bi bil razkrit njegov zasebni naslov, bi lahko razkritje tudi negativno vplivalo na pravico tega posameznika do varstva osebnih podatkov. To še zlasti drži za osebne podatke, ki so široko dostopni na svetovnem spletu v digitalni obliki v več jezikih in prek zlahka dostopnega evropskega vmesnika/točke dostopa.

20. Še do pred kratkim so se osebni podatki iz poslovnih registrov (npr. ime, naslov in vzorčni podpis direktorja) razkrivali javnosti v papirni obliki in v lokalnem jeziku, pogosto le po tem, ko se je vlagatelj osebno oglasil na lokalnem registrskem uradu. Treba je priznati, da se ta položaj kvalitativno razlikuje od javnega razkritja podatkov v digitalni

obliki prek nacionalne elektronske točke dostopa. Javno razkrivanje osebnih podatkov prek zlahka dostopnega evropskega vmesnika/točk dostopa ta položaj še stopnjuje ter dodatno krepi dostopnost informacij in tveganja za varstvo osebnih podatkov zadevnih posameznikov.

21. Zdajšnja tveganja za zasebnost (zaradi preproste razpoložljivosti podatkov v digitalni obliki prek enotne elektronske točke dostopa) vključujejo krajo identitete in druge kriminalne dejavnosti ter tveganje, da bodo družbe po profiliranju zadevnih posameznikov razkrite informacije nezakonito zajemale in uporabljale za komercialne namene, ki niso bili prvotno predvideni. Brez ustreznih zaščitnih ukrepov se lahko informacije prodajajo drugim ali se združujejo z drugimi informacijami in se prodajajo nazaj vladam za uporabo za nepovezane in nerazkrite namene (npr. za izvrševanje davčne zakonodaje ali druge kazenske ali upravne preiskave) brez ustrezne pravne podlage ([1]).

22. Zato je treba skrbno pretehtati, katere osebne informacije je treba dati na voljo prek enotnega evropskega vmesnika/točke dostopa in katere dodatne zaščitne ukrepe za varstvo podatkov – vključno s tehničnimi ukrepi za omejitev zmogljivosti iskanja ali prenašanja in podatkovnega rudarjenja – je treba uporabljati.

3.2 **Poglavitne zaščitne ukrepe za varstvo podatkov je treba opredeliti v samem predlogu in jih ne bi smeli prepustiti delegiranim aktom**

23. Kot je navedeno v oddelkih 2.1 in 2.2 zgoraj, sta predlagana člena 3a in 4a Direktive 2009/101/ES zelo splošna in številna ključna vprašanja prepuščata delegiranim aktom.

24. Čeprav ENVP priznava potrebo po prožnosti in s tem tudi potrebo po delegiranih aktih, poudarja, da so potrebni zaščitni ukrepi za varstvo podatkov poglavitni elementi, ki jih je treba jasno in izrecno predvideti neposredno v besedilu samega predloga Direktive. V tej zvezi jih ni mogoče šteti za „nepoglavitne elemente“, ki se lahko vključijo v naknadne delegirane akte, sprejete na podlagi člena 290 Pogodbe o delovanju Evropske unije.

25. ENVP zato priporoča, da morajo biti določbe predloga o varstvu podatkov bolj specifične in ne vključujejo le sklica na Direktivo 95/46/ES (glej oddelke od 3.4 do 3.13). V delegirane akte se nato lahko vključijo dodatne določbe v zvezi z izvajanjem posebnih zaščitnih ukrepov na podlagi posvetovanja z Evropskim nadzornikom za varstvo podatkov in po potrebi z nacionalnimi organi za varstvo podatkov (glej oddelke 3.5, 3.6, 3.8, 3.9, 3.10, 3.12 in 3.13 spodaj).

3.3 **V samem predlogu je treba pojasniti tudi druge poglavitne elemente predlaganih ukrepov**

26. V predlogu niso obravnavani le ključni zaščitni ukrepi za varstvo podatkov, ampak je predlog tudi zelo nedorečen v drugih pogledih. Predlog delegiranim aktom zlasti prepušča določitev poglavitnih elementov, kako izvesti predlagano (i) povezovanje poslovnih registrov in (ii) javno razkritje podatkov.

27. Pojasnitev teh drugih poglavitnih elementov predloga je nujen pogoj za sprejetje ustreznih zaščitnih ukrepov za varstvo podatkov. ENVP zato priporoča, da morajo biti ti poglavitni elementi opredeljeni v samem predlogu direktive (glej oddelka 3.4 in 3.5 spodaj).

3.4 **Upravljanje: vloge, pristojnosti in odgovornosti je treba pojasniti v predlogu direktive**

28. Predlog za zdaj delegiranim aktom prepušča določitev pravil o upravljanju, vodenju, delovanju in zastopanju elektronskega omrežja ([2]).

29. Čeprav so v oceni učinka in obrazložitvenem memorandumu opredeljene nekatere sinergije z orodjem IMI in portalom e-pravosodja, besedilo predloga direktive pušča odprta vrata različnim možnostim, da se omogoči uresničitev katere koli sinergije ali vseh sinergij, vključno s preoblikovanjem evropskega poslovnega registra (EBR), z uporabo orodja IMI za nekatere izmenjave podatkov in/ali z uporabo portala e-pravosodja kot vmesnika/točke dostopa za zagotavljanje informacij iz poslovnih registrov javnosti.

30. Izključene niso niti druge možnosti, kot so objava razpisa za dodelitev pravice za načrtovanje in upravljanje elektronskega omrežja ali da Komisija prevzame neposredno vlogo pri načrtovanju in upravljanju sistema. V upravljavsko strukturo elektronskega omrežja so lahko vključeni tudi predstavniki držav članic.

([1]) Dejansko obstaja razvijajoči se trg, ki se ukvarja s prodajo tovrstnih poslovnih informacij. Izvajalci storitev na tem trgu točkujejo zanesljivost družb/posameznikov na podlagi informacij iz številnih virov, vključno s poslovnimi registri, sodnimi registri, registri plačilne nesposobnosti itd.

([2]) Glej predlagano besedilo za člena 4(a)(3)(a) Direktive 2009/101/ES.

31. Še več, čeprav je v sedanji obliki predloga predviden „enotni evropski elektronski vmesnik“ (dodan poudarek), ni izključena možnost, da bo pozneje v zakonodajnem postopku besedilo spremenjeno za določitev bolj decentralizirane strukture.

32. ENVP še ugotavlja, da čeprav sedanji predlog ne obravnava posebej vprašanja povezovanja poslovnih registrov z drugimi podatkovnimi zbirkami (kot so na primer zemljiške knjige ali civilni registri), je to nedvomno tehnična možnost in nekaj, kar se že dogaja v nekaterih državah članicah ([1]).

33. Izbira ene ali druge možnosti lahko privede do popolnoma različne strukture upravljanja elektronskega omrežja in elektronskega orodja, ki ju je treba uporabljati za javno razkritje. To nato pripelje do različnih vlog in odgovornosti vključenih strani, posledica pa so tudi različne vloge in odgovornosti z vidika varstva podatkov.

34. ENVP v zvezi s tem poudarja, da je pri vsakršni obdelavi osebnih podatkov ključno pravilno opredeliti, kdo je „upravljavec“. To je poudarila tudi Delovna skupina iz člena 29 v Mnenju 1/2010 o pojmih „upravljavec“ in „obdelovalec“ ([2]). Glavni razlog, zakaj je jasna in nedvoumna opredelitev upravljavca tako pomembna, je, da ta opredelitev določa, kdo je odgovoren za skladnost s pravili o varstvu podatkov, pomembna pa je tudi za opredelitev prava, ki se uporablja ([3]).

35. Kot je bilo ugotovljeno v mnenju Delovne skupine iz člena 29, „[č]e ni dovolj jasno, kaj se od koga zahteva – npr. nihče ni odgovoren ali je veliko mogočih upravljavcev –, je očitno tveganje, da se bo dogajalo le malo ali nič in da bodo pravne določbe ostale neučinkovite“.

36. ENVP poudarja, da je jasnost še zlasti potrebna v primerih, kadar je v sodelovanje vključenih več akterjev. To pogosto drži za informacijske sisteme EU, ki se uporabljajo za javne namene, kjer je namen obdelave opredeljen v pravu EU.

37. ENVP zato priporoča, naj se v besedilu samega predloga direktive izrecno, jasno in nedvoumno opredeli:

— ali bo elektronsko omrežje upravljala Komisija ali tretja stran in ali bo njegova struktura centralizirana ali decentralizirana,

— naloge in odgovornosti vseh strani, vključenih v obdelavo podatkov in upravljanje elektronskega omrežja, vključno s Komisijo, predstavniki držav članic, nosilci poslovnih registrov v državah članicah in vsemi tretjimi stranmi, ter

— razmerje med elektronskim sistemom, predvidenim v predlogu, in drugimi pobudami, kot so orodje IMI, portal e-pravosodja in register EBR.

38. Z vidika varstva podatkov morajo biti ta pojasnila tudi izrecna in nedvoumna, da se na podlagi samega predloga direktive opredeli, ali je treba posebnega akterja šteti za „upravljavca“ ali „obdelovalca“.

39. Predlog naj bi načeloma izrecno prispeval k opredelitvi – kot se zdi na podlagi sedanjega osnutka kot celote –, da je treba vse nosilce poslovnih registrov in upravljavca(-e) sistema v zvezi z njihovimi dejavnosti šteti za upravljavce podatkov. Glede na navedeno ter to, da zdaj v predlogu ni opisana upravljavska struktura in ni opredeljeno, kdo bo(-do) upravljavec(-vci) elektronskega sistema, ni mogoče izključiti, da bodo nekateri subjekti, ki bodo na koncu upravljali sistem na praktični ravni, delovali kot obdelovalci, ne kot upravljavci. To lahko še zlasti drži, če se ta dejavnost dodeli v zunanje izvajanje tretji strani, ki bo dosledno delovala na podlagi navodil. Vsekakor se zdi, da je še vedno več upravljavcev podatkov, vsaj eden v vsaki državi članici: subjekti, ki vodijo poslovne registre. Tega vidika ne spremeni niti to, da so lahko kot upravljavci, „distributerji“ ali kako drugače vključeni drugi (zasebni) subjekti. Vsekakor je treba zaradi jasnosti in pravne varnosti to navesti v predlogu direktive.

([1]) Ker v predlogu povezovanje zdaj ni predvideno, ENVP v tej fazi v svojem mnenju o tem vprašanju ne bo razpravljal. Kljub temu opozarja, da lahko morebitni razmislek o povezovanju zahteva ločeno analizo sorazmernosti in sprejetje dodatnih ustreznih zaščitnih ukrepov za varstvo podatkov.

([2]) Glej člen 2(d) in (e) Direktive 95/46/ES in Uredbe (ES) št. 45/2001 ter Mnenje 1/2010 Delovne skupine iz člena 29 z dne 16. februarja 2010 o pojmih „upravljavec“ in „obdelovalec“ (WP 169).

([3]) Glede na to, da predpisi s področja varstva podatkov v Evropi niso popolnoma usklajeni, je identiteta upravljavca pomembna za določitev, katera nacionalna zakonodaja se uporablja. Poleg tega je pomembno še opredeliti, ali se uporablja Direktiva 95/46/ES ali Uredba (ES) št. 45/2001: če je Komisija (tudi) upravljavec, se bo uporabljala (tudi) Uredba (ES) št. 45/2001, kot je pojasnjeno v oddelku 3.11 spodaj.

40. Ne nazadnje, v predlogu je treba bolj specifično in celoviteje opisati odgovornosti, ki izhajajo iz teh vlog. Tako je treba na primer v predlog vključiti vlogo upravljavca(-cev) pri zagotavljanju, da je sistem načrtovan tako, da upošteva zasebnost, in usklajevalno vlogo upravljavca v zvezi z vprašanji glede varstva podatkov.

41. ENVP ugotavlja, da bodo vse te pojasnitve pomembne tudi za opredelitev, kateri organi za nadzor varstva podatkov so pristojni in za katero obdelavo osebnih podatkov.

3.5 **V predlogu direktive je treba opredeliti okvir in pravno podlago za pretok podatkov/postopke upravnega sodelovanja**

42. Zdi se, da elektronsko omrežje v sedanji obliki ni predvideno za zagotavljanje samodejne razpoložljivosti vseh informacij, ki se hranijo v poslovnih registrih, vsem drugim poslovnim registrom v vseh drugih državah članicah: predlog zahteva le povezovanje in interoperabilnost poslovnih registrov in tako določa pogoje, ki omogočajo izmenjave informacij in dostop v prihodnosti. Za zagotovitev pravne varnosti je treba v predlogu pojasniti, ali je to razumevanje pravilno.

43. Poleg tega v predlogu ni navedeno, kateri pretok podatkov/postopki upravnega sodelovanja lahko potekajo prek povezanih poslovnih registrov ([1]). ENVP razume, da bo morda potrebna neka raven prožnosti za zagotovitev izpolnjevanja potreb, ki bi se lahko pojavile v prihodnosti. Glede na to ENVP meni, da je poglavitno, da se v predlogu opredelijo okvir za pretok podatkov in postopki upravnega sodelovanja, ki lahko potekajo v prihodnosti z uporabo elektronskega omrežja. To je še zlasti pomembno za zagotovitev, da (i) imajo vse izmenjave podatkov trdno pravno podlago in (ii) so določeni ustrezni zaščitni ukrepi za varstvo podatkov.

44. ENVP meni, da morajo vsi prenosi podatkov ali druge dejavnosti obdelave podatkov prek elektronskega omrežja (npr. javno razkritje osebnih podatkov prek enotnega vmesnika/točke dostopa) temeljiti na zavezujočem aktu EU, sprejetem na trdni pravni podlagi. To je treba jasno določiti v predlogu direktive ([2]).

([1]) To velja z izjemo, do neke mere, izmenjav podatkov v primeru čezmejnih združitev, prenosov sedeža in posodobitvah informacij o podružnicah, o katerih se v predlogu posebej razpravlja.

([2]) Če v zvezi s tem obstaja morebitna potreba po obdelavi podatkov na območju notranjega trga, ki ni zajeta v posebnem aktu Unije, ENVP poziva k nadaljnjemu premisleku o modalitetah pravnega okvira, ki bi omogočil – morda skupaj s splošnimi določbami Pogodbe – posebne določbe v predlagani direktivi in naknadnih delegiranih aktih za zagotovitev ustrezne pravne podlage z vidika varstva podatkov. V predlagani direktivi je treba še navesti, ali lahko poslovni registri uporabljajo elektronsko omrežje in enotno točko dostopa za izmenjavo ali javno razkritje osebnih podatkov, ki ni predvideno v aktu Unije, vendar je dovoljeno ali zahtevano na podlagi nacionalne zakonodaje.

3.6 **V predlogu direktive je treba obravnavati tudi druga ključna vprašanja, prepuščena delegiranim aktom**

45. V predlogu je poleg tega določeno, da se v delegiranih aktih opredelijo naslednja vprašanja ([3]):

— pogoji udeležbe v elektronskem omrežju za države zunaj evropskega gospodarskega prostora,

— minimalni varnostni standardi za elektronsko omrežje ter

— opredelitev standardov oblike zapisa, vsebine in omejitve za shranjevanje in pridobivanje dokumentov in podatkov, ki omogoča samodejno izmenjavo podatkov.

46. ENVP v zvezi s prvo in drugo alineo meni, da je treba nekatere poglavitne zaščitne ukrepe določiti v samem predlogu direktive (glej oddelka 3.12 in 3.13 spodaj). Nadaljnje podrobnosti se nato lahko opredelijo v delegiranih aktih.

47. V zvezi s samodejnimi izmenjavami podatkov je ENVP zadovoljen, da so v predlogu zahtevani delegirani akti za določitev „opredelitve standardov oblike zapisa, vsebine in omejitve za shranjevanje in priklic dokumentov in podatkov, ki omogoča samodejno izmenjavo podatkov“.

48. Za zagotovitev večje jasnosti v zvezi s tem ENVP priporoča, naj se v samem predlogu direktive jasno navede, da elektronsko omrežje omogoča (i) posebne ročne izmenjave podatkov med poslovnimi registri v vsakem primeru posebej (kot je določeno v aktu EU na primer v primeru združitve ali prenosa sedeža) in (ii) samodejne prenose podatkov (kot je določeno v aktu EU na primer v primeru posodobitve informacij v registru tujih podružnic).

([3]) Glej predlagano besedilo za člen 4(a)(3) Direktive 2009/101/ES.

49. ENVP za dodatno povečanje jasnosti poleg tega priporoča spremembo predlaganega besedila za zadevni člen 4(a)(3)(i) Direktive 2009/101/ES za zagotovitev, da (i) bodo delegirani akti celovito pokrivali ročne in samodejne izmenjave podatkov, da (ii) so zajeti vsi postopki obdelave, ki lahko vključujejo osebne podatke (ne le shranjevanje in pridobivanje), in da (iii) bodo posebne določbe o varstvu podatkov v delegiranih aktih zagotavljale tudi praktično izvajanje ustreznih zaščitnih ukrepov za varstvo podatkov.

50. V ponazoritev, člen 4(a)(3)(i) bi se lahko spremenil tako:

„(i) obliko zapisa, vsebine in omejitve za vse ročne ali samodejne postopke obdelave podatkov, ki potekajo z uporabo omrežja, vključno s prenosom, shranjevanjem in pridobivanjem informacij, ter posebne ukrepe, ki so lahko potrebni za zagotavljanje praktičnega izvajanja ustreznih zaščitnih ukrepov za varstvo podatkov."

3.7 **V predlogu direktive je treba dodatno pojasniti kategorije osebnih podatkov, ki se obdelujejo**

51. ENVP v uvodni pripombi poudarja, da čeprav so imena (in po možnosti drugi podrobni podatki, kot so zasebni naslovi) zastopnikov družb (in drugih posameznikov, ki sodelujejo pri upravljanju družb) nedvomno najočitnejši osebni podatki, ki jih lahko obdeluje elektronsko omrežje in/ali jih je mogoče javno razkriti prek enotnega elektronskega vmesnika/točke dostopa, to nikakor niso edine osebne informacije, ki se hranijo v poslovnih registrih.

52. Prvič, tudi nekateri dokumenti iz člena 2 Direktive 2009/101/ES (npr. akt o ustanovitvi, statut in računovodske listine) lahko vključujejo osebne podatke drugih posameznikov. Ti podatki lahko med drugim vključujejo imena, naslove, po možnosti številke osebnih izkaznic in rojstne datume ter celo skenirane lastnoročne podpise različnih posameznikov, vključno s posamezniki, ki so ustanovili družbo, delničarji družbe, odvetniki, računovodji, zaposlenimi ali notarji.

53. Drugič, podatke o družbi, kadar so povezani z imenom posameznika (kot je direktor), je mogoče šteti tudi za osebne podatke, povezane s tem posameznikom. Če na primer podatki iz poslovnega registra kažejo, da je neki posameznik član upravnega odbora družbe v postopku likvidacije, je ta informacija pomembna tudi za zadevnega posameznika.

54. Za zagotovitev jasnosti, kateri osebni podatki se obdelujejo, in za zagotovitev, da je razpon podatkov, ki se obdelujejo, sorazmeren s cilji predloga, ENVP priporoča pojasnitve, opredeljene v nadaljevanju tega oddelka 3.7.

V predlogu direktive je treba pojasniti besedno zvezo „podatki o osebah"

55. V členu 2 Direktive 2009/101/ES ni opredeljeno, katere „podatke" o zadevnih posameznikih (zastopnikih družb in drugih osebah, ki sodelujejo pri upravljanju družb) je treba razkriti.

56. Dejansko različne jezikovne različice predloga kažejo na velike razlike celo v zvezi s prevodom besedne zveze „podatki o osebah". Tako je ta na primer v francoščini „l'identité des personnes" (tj. identiteta oseb), v italijanščini „le generalità delle persone" (tj. osebni podatki, kot sta ime in priimek), v madžarščini „személyek adatai" (tj. podatki o posameznikih), v nizozemščini „de identiteit van de personen" (tj. identiteta oseb) in v romunščini „identitatea persoanelor" (tj. identiteta oseb).

57. Poleg tega so v nekaterih državah članicah zasebni naslovi direktorjev družb in/ali drugih posameznikov, kot so nekateri delničarji, rutinsko na voljo javnosti na svetovnem spletu. V nekaterih drugih državah članicah poslovni register, ki so mu bile informacije predložene, ohranja zaupnost teh informacij zaradi pomislekov v zvezi z zaupnostjo, vključno zaradi strahu pred krajo identitete.

58. ENVP priporoča spremembo člena 2 Direktive 2009/101/ES za pojasnitev, katere – če sploh katere – osebne podatke je treba razkriti poleg imen zadevnih posameznikov (zastopnikov družb in drugih oseb, ki sodelujejo pri upravljanju družbe). Pri tem je treba skrbno preučiti potrebo po preglednosti in natančni identifikaciji teh posameznikov ter jo ovrednotiti glede na druge konkurenčne pomisleke, kot je potreba po varstvu zasebnosti zadevnih posameznikov ([1]).

59. Če zaradi razlik v nacionalnih praksah ne bo dosežen sporazum, je treba člen 2 spremeniti vsaj tako, da določa, da je treba razkriti „polno ime zadevnih posameznikov in – če to posebej zahteva nacionalna zakonodaja – dodatne podatke, potrebne za njihovo identifikacijo". Nato bo jasno, da lahko države članice v nacionalni zakonodaji same

([1]) Oceno sorazmernosti je treba opraviti zlasti ob upoštevanju meril, ki jih je opredelilo Sodišče Evropske unije v zadevi *Schecke in Eifert* (sodba Sodišča z dne 9. novembra 2010 v združenih zadevah C-92/09 in C-93/09; glej zlasti odstavke 81, 65 in 86). Sodišče je v zadevi *Schecke* poudarilo, da je treba odstopanja in omejitve v zvezi z varstvom osebnih podatkov uporabljati le, če je to nujno potrebno. Sodišče je poleg tega menilo, da morajo institucije preučiti različne načine objave za opredelitev, kateri način je v skladu z namenom objave, hkrati pa najmanj posega v pravico osebe, na katero se podatki nanašajo, do zasebnega življenja na splošno in posebej varstva osebnih podatkov.

določijo, katere – če sploh katere – „podrobnosti“ je treba razkriti poleg imen in da bo treba dodatne osebne podatke razkriti le, če je to potrebno za identifikacijo zadevnih posameznikov.

60. Druga možnost in ob upoštevanju tega, da so v členu 2 navedene „minimalne informacije“, ne popolna uskladitev vsebine poslovnih registrov v Evropi, bi bilo mogoče besedno zvezo „podrobnosti o osebah“ preprosto nadomestiti z besedno zvezo „polna imena oseb“. Nato bi države članice same odločile, katere – če sploh katere – dodatne informacije želijo razkriti.

Treba je pojasniti besedno zvezo „upravljanje, nadzor ali obvladovanje“

61. V členu 2 Direktive 2009/101/ES se poleg tega zahteva razkritje informacij o osebah, udeleženih pri „upravljanju, nadzoru ali obvladovanju“ družbe. Na podlagi te široke ubeseditve ni popolnoma jasno, ali je treba razkriti informacije o delničarjih: zlasti informacije o delničarjih, (i) ki imajo velik, vpliven ali kontrolni delež nad določenim pragom ali (ii) zaradi zlatega deleža, posebne pogodbene ureditve ali drugačnega dejanskega nadzora/vpliva nad družbo.

62. ENVP razume, da je široka ubeseditev potrebna za zajetje najrazličnejših struktur upravljanja družb, ki v zvezi z družbami z omejeno odgovornostjo obstajajo v različnih državah članicah. Glede na to je z vidika varstva podatkov ključna pravna varnost v zvezi s kategorijami posameznikov, katerih podatke je mogoče razkriti. ENVP zato priporoča spremembo člena 2 Direktive 2009/101/ES za pojasnitev, katere – če sploh katere – osebne podatke o delničarjih je treba razkriti. Pri tem je treba opraviti tudi analizo sorazmernosti na podlagi zadeve *Schecke* (kot je bilo navedeno zgoraj).

Razkritje informacij, ki presegajo minimalne zahteve; črni seznami

63. Čeprav predlog ne zahteva izmenjave ali javnega razkritja osebnih podatkov, ki presega minimalne zahteve iz člena 2 Direktive 2009/101/ES, ni izključeno, da lahko države članice zahtevajo, če se tako odločijo, da njihovi poslovni registri obdelujejo ali razkrivajo dodatne osebne podatke in dajejo take podatke na voljo prek enotnega evropskega vmesnika/točke dostopa in/ali izmenjujejo take podatke s poslovnimi registri v drugih državah članicah.

64. To je posebej občutljivo vprašanje v zvezi s „črnimi seznami“. V nekaterih državah elektronski register dejansko deluje tudi kot nekakšen „črni seznam“, na katerem lahko katere koli tretje strani prek elektronskega vmesnika iščejo informacije o zastopnikih družb, ki jim je bilo prepovedano opravljanje dejavnosti.

65. ENVP za obravnavo tega vprašanja priporoča, naj se v predlogu pojasni, ali in v kolikšnem obsegu lahko države članice morebiti javno razkrijejo več informacij prek enotnega portala in/ali morebitno izmenjujejo več informacij na podlagi nacionalne zakonodaje, če to želijo. V tem primeru mora dosledna ocena sorazmernosti (glej zgoraj navedeno zadevo *Schecke*) temeljiti na nacionalni zakonodaji in upoštevati tudi cilje notranjega trga.

66. Poleg tega predlaga, naj te pristojnosti postanejo zavezujoče za vlogo, ki jo bodo imeli nacionalni organi za varstvo podatkov, na primer s posvetovanjem.

67. Ne nazadnje, ENVP poudarja, da je – če bo predvidena evropska shema, ki bo posebej zahtevala take „črne sezname“ – to treba posebej opredeliti v predlogu direktive ([1]).

3.8 **Jamstva za zagotavljanje omejitve namena, zaščitni ukrepi za preprečevanje zajemanja podatkov, podatkovnega rudarjenja, kombiniranja podatkov in čezmernega iskanja**

68. ENVP priporoča, naj se v predlogu direktive izrecno navede, da je treba v vseh primerih, v katerih so osebni podatki javno razkriti ali jih drugače souporabljajo poslovni registri, določiti ustrezne zaščitne ukrepe za preprečevanje zlasti zajemanja podatkov, podatkovnega rudarjenja, kombiniranja podatkov in čezmernega iskanja, da se zagotovi, da osebni podatki, ki so zaradi preglednosti dani na voljo, ne bodo zlorabljeni za dodatne nepovezane namene ([2]).

69. ENVP poudarja zlasti potrebo po razmisleku o tehnoloških in organizacijskih ukrepih na podlagi načela vgrajene zasebnosti (glej oddelek 3.14 spodaj). Praktično izvajanje teh zaščitnih ukrepov je mogoče prepustiti delegiranim aktom. Vendar je treba načela opredeliti v samem predlogu direktive.

([1]) Ker v predlogu to ni predvideno, ENVP v tej fazi v svojem mnenju o tem vprašanju ne bo razpravljal. Kljub temu opozarja, da lahko morebitni razmislek o tem zahteva ločeno analizo sorazmernosti in sprejetje dodatnih ustreznih zaščitnih ukrepov za varstvo podatkov.

([2]) Glej člen 6(b) Direktive 95/46/ES in Uredbe (ES) št. 45/2001.

3.9 **Zagotavljanje informacij osebam, na katere se podatki nanašajo, in preglednost**

70. ENVP priporoča, naj predlog direktive vsebuje posebno določbo, ki zahteva, da je treba osebam, na katere se podatki nanašajo, informacije iz členov 10 in 11 Direktive 95/46/ES (in ustreznih določb Uredbe (ES) št. 45/2001, če je primerno) zagotoviti učinkovito in celovito. Poleg tega in glede na upravljavsko strukturo, o kateri se je treba dogovoriti, ter vloge in odgovornosti različnih vključenih strani je mogoče v predlogu direktive izrecno zahtevati, da upravljavec sistema prevzame proaktivno vlogo pri zagotavljanju obvestil in drugih informacij osebam, na katere se podatki nanašajo, na svoji spletni strani, tudi „v imenu“ poslovnih registrov. Nadaljnje podrobnosti se lahko po potrebi vključijo v delegirane akte ali opredelijo v politiki o varstvu podatkov.

3.10 **Pravice do dostopa, popravka in izbrisa**

71. Predlog mora vključevati vsaj sklic na zahtevo za razvoj modalitet ureditve (v delegiranih aktih), da se osebam, na katere se podatki nanašajo, omogoči uveljavljanje njihovih pravic. Treba se je tudi sklicevati na možnost oblikovanja modula za varstvo podatkov in možnost rešitev vgrajene zasebnosti za sodelovanje med organi v zvezi s pravicami do dostopa ter „krepitve vloge oseb, na katere se podatki nanašajo“, če je primerno.

3.11 **Pravo, ki se uporablja**

72. Ker je mogoče, da tudi Komisija ali druga institucija/organ EU obdeluje osebne podatke v elektronskem omrežju (npr. v vlogi upravljavca omrežja ali s pridobivanjem osebnih podatkov iz omrežja), se je treba sklicevati tudi na Uredbo (ES) št. 45/2001.

73. Poleg tega je treba pojasniti, da se Direktiva 95/46/ES uporablja za poslovne registre in druge strani, ki delujejo v državah članicah na podlagi nacionalne zakonodaje, medtem ko se Uredba (ES) št. 45/2001 uporablja za Komisijo ter druge institucije in organe EU.

3.12 **Prenos osebnih podatkov tretjim državam**

74. V zvezi s prenosom osebnih podatkov, ki ga nosilec poslovnega registra v EU opravi za nosilca poslovnega registra v tretji državi, ki ne zagotavlja ustrezne ravni varstva osebnih podatkov, ENVP najprej poudarja, da je treba razlikovati med dvojimi primeri:

— primeri, v katerih so osebni podatki že na voljo v javnem registru (na primer prek enotnega evropskega vmesnika/točke dostopa), in

— primeri, v katerih osebni podatki niso javno dostopni.

75. V prvem primeru člen 26(1)(f) Direktive 95/46/ES ob upoštevanju nekaterih pogojev dopušča izjemo, kadar „se prenos opravi iz [javnega] registra“. Če želi na primer nosilec poslovnega registra v neki evropski državi prenesti poseben niz osebnih podatkov (npr. v zvezi z registracijo tujih podružnic) nosilcu poslovnega registra v tretji državi in bi bili zadevni podatki v vsakem primeru že dostopni javnosti, bi moral biti prenos mogoč tudi, če zadevna tretja država ne zagotavlja ustrezne ravni varstva.

76. V zvezi z drugim primerom ENVP priporoča, naj se v predlogu pojasni, da lahko prenosi podatkov, ki niso javno dostopni, potekajo le subjektom ali posameznikom v tretji državi, ki ne zagotavlja ustreznega varstva, če upravljavec navede ustrezne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic. Taki zaščitni ukrepi lahko izhajajo zlasti iz ustreznih pogodbenih klavzul, oblikovanih na podlagi člena 26(2) Direktive 95/46/ES ([1]). V primerih, v katerih taki prenosi podatkov tretjim državam sistematično vključujejo podatke, ki so skupni poslovnim registrom v dveh ali več državah EU, ali v katerih je ukrepanje na ravni EU kako drugače zaželeno, lahko pogajanja o pogodbenih klavzulah potekajo tudi na ravni EU (člen 26(4)).

77. ENVP poudarja, da se druga odstopanja, kot je tisto, v katerem (člen 26(d)) „je prenos potreben oziroma ga zahteva zakon na temelju pomembnega javnega interesa ali pa za uveljavitev, izvajanje ali obdržanje pravice do pravnih zahtevkov“, ne smejo uporabiti za utemeljitev sistematičnih prenosov podatkov tretjim državam prek elektronskega omrežja.

([1]) Če je mogoče, da je v nekaterih primerih Komisija med akterji, ki lahko prenašajo podatke tretjim državam, je treba vključiti tudi sklic na člen 9(1) in 9(7) Uredbe (ES) št. 45/2001.

3.13 **Odgovornost in vgrajena zasebnost**

78. ENVP priporoča, naj se v predlogu izrecno sklicuje in prizadeva za izvajanje načela odgovornosti ([1]) ter opredeli jasen okvir za ustrezne notranje mehanizme in kontrolne sisteme za zagotavljanje skladnosti z določbami o varstvu podatkov ter dokazov o njej, kot so:

— izvedba ocene učinka na zasebnost (vključno z analizo tveganja glede varnosti) pred načrtovanjem sistema,

— po potrebi sprejetje in posodobitev formalne politike varstva podatkov (izvedbena pravila), tudi v zvezi z varnostnim načrtom,

— izvedba rednih revizij za ocenjevanje stalne ustreznosti politike varstva in varnosti podatkov ter skladnosti z njo,

— javna objava (vsaj delno) izsledkov teh revizij, da se delničarjem dokaže skladnost z določbami o varstvu podatkov, ter

— uradna obvestila o kršitvah varstva podatkov in drugih varnostnih incidentih.

79. V zvezi z vgrajeno zasebnostjo ([2]) se mora predlog izrecno sklicevati na to načelo, poleg tega mora tudi to zavezo uresničiti v konkretnih ukrepih. V predlogu je treba zlasti določiti, da mora biti elektronsko omrežje zgrajeno varno in trdno, kar omogoča privzeto vgrajenost raznovrstnih zaščitnih ukrepov glede zasebnosti. Mogoči primeri zaščitnih ukrepov glede vgrajene zasebnosti vključujejo:

— decentraliziran pristop, v okviru katerega so podatki shranjeni le v „glavnem“ viru in vsak „distributer“ le pridobi podatke iz tega „glavnega“ vira (za zagotavljanje, da so podatki posodobljeni),

— samodejne postopke, ki iščejo nedosledne in nenatančne informacije,

— omejene zmogljivosti iskanja za razvrščanje le tistih podatkov, ki so sorazmerni in ustrezajo namenu,

— druge zaščitne ukrepe za preprečevanje/omejevanje množičnih prenosov, podatkovnega rudarjenja in čezmernega iskanja ter zagotavljanje ustrezne omejitve namena; zaščitne ukrepe za preprečevanje ali omejevanje možnosti tretjih strani, da uporabljajo iskalni vmesnik za zajemanje podatkov in profiliranje posameznikov (npr. „captcha“ ([3]) ali registracijska zahteva za plačilo),

— vgrajeno sistemsko funkcionalnost, ki osebam, na katere se podatki nanašajo, lajša učinkovito uveljavljanje pravic; vgrajene funkcionalnosti za poslovne registre za medsebojno usklajevanje v zvezi z zahtevki za dostop oseb, na katere se podatki nanašajo,

— postopke za obravnavo informacij o vlagateljih, ki so prenesli informacije iz javnega registra na način, ki je varen in upošteva zasebnost, ter

— revizijske/sledilne mehanizme.

IV. **SKLEPNE UGOTOVITVE**

80. ENVP podpira cilje predloga. Njegove pripombe je treba ovrednotiti z vidika tega konstruktivnega pristopa.

81. ENVP poudarja, da je treba neposredno v besedilu direktive jasno in izrecno določiti potrebne zaščitne ukrepe za varstvo podatkov, saj jih šteje za poglavitne elemente. Dodatne določbe v zvezi z izvajanjem posebnih zaščitnih ukrepov je nato mogoče opredeliti v delegiranih aktih.

82. V predlogu direktive je treba obravnavati vprašanja upravljanja, vlog, pristojnosti in odgovornosti. Za ta namen je treba v predlogu direktive opredeliti:

— ali bo elektronsko omrežje upravljala Komisija ali tretja stran in ali bo njegova struktura centralizirana ali decentralizirana,

— naloge in odgovornosti vseh strani, vključenih v obdelavo podatkov in upravljanje elektronskega omrežja, vključno s Komisijo, predstavniki držav članic, nosilci poslovnih registrov v državah članicah in vsemi tretjimi stranmi,

([1]) Glej oddelek 7 Mnenja Evropskega nadzornika za varstvo podatkov o sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – „Celovit pristop k varstvu osebnih podatkov v Evropski uniji“, izdanega 14. januarja 2011, na spletni strani http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

([2]) Prav tam.

([3]) „Captcha“ je vrsta preizkusa izziv-odziv, ki se v računalništvu uporablja za zagotavljanje, da odziv ni računalniško ustvarjen.

— razmerje med elektronskim sistemom, predvidenim v predlogu, in drugimi pobudami, kot so orodje IMI, portal e-pravosodja in register EBR, ter

— specifične in nedvoumne elemente za opredelitev, ali je treba nekega akterja šteti za „upravljavca“ ali „obdelovalca“.

83. Vse dejavnosti obdelave podatkov prek elektronskega omrežja morajo temeljiti na zavezujočem pravnem instrumentu, kot je poseben akt Unije, sprejet na trdni pravni podlagi. To je treba jasno opredeliti v predlogu direktive.

84. Pojasniti je treba določbe o pravu, ki se uporablja, in vključiti sklic na Uredbo (ES) št. 45/2001.

85. V zvezi s prenosom osebnih podatkov tretjim državam je treba v predlogu pojasniti, da lahko načeloma in z izjemo primerov, ki jih zajema člen 26(1)(f) Direktive 95/46/ES, prenosi potekajo le subjektom ali posameznikom v tretji državi, ki ne zagotavlja ustreznega varstva, če upravljavec navede ustrezne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic. Taki zaščitni ukrepi lahko izhajajo zlasti iz ustreznih pogodbenih klavzul, oblikovanih na podlagi člena 26 Direktive 95/46/ES.

86. Poleg tega mora Komisija skrbno pretehtati, katere tehnične in organizacijske ukrepe je treba sprejeti za zagotavljanje, da sta zasebnost in varstvo podatkov „vgrajena“ v strukturo elektronskega omrežja (v nadaljnjem besedilu: vgrajena zasebnost) in da so vzpostavljeni ustrezni pregledi za zagotavljanje skladnosti z določbami o varstvu podatkov ter dokazov o njej (v nadaljnjem besedilu: odgovornost).

87. Druga priporočila ENVP vključujejo:

— v predlogu direktive je treba jasno navesti, da mora elektronsko omrežje omogočati (i) posebne ročne izmenjave podatkov med poslovnimi registri po eni strani in (ii) samodejne prenose podatkov po drugi strani. Predlog je treba spremeniti tudi za zagotavljanje, da (i) bodo delegirani akti celovito pokrivali ročne in samodejne izmenjave podatkov ter (ii) vse postopke obdelave, ki lahko vključujejo osebne podatke (ne le shranjevanje in pridobivanje), in da (iii) bodo posebne določbe o varstvu podatkov v delegiranih aktih zagotavljale tudi praktično izvajanje ustreznih zaščitnih ukrepov za varstvo podatkov,

— predlog mora spremeniti člen 2 Direktive 2009/101/ES za pojasnitev, katere – če sploh katere – osebne podatke je treba razkriti poleg imen zadevnih posameznikov. Poleg tega je treba pojasniti, ali je treba razkriti podatke o delničarjih. Pri tem je treba skrbno preučiti potrebo po preglednosti in natančni identifikaciji teh posameznikov, vendar jo je treba ovrednotiti tudi glede na druge konkurenčne pomisleke, kot so potreba po zaščiti pravice do varstva osebnih podatkov zadevnih posameznikov,

— v predlogu je treba pojasniti, ali lahko države članice morebiti javno razkrijejo več informacij prek enotnega portala (in/ali izmenjujejo več informacij) na podlagi nacionalne zakonodaje in ob upoštevanju dodatnih zaščitnih ukrepov za varstvo podatkov,

— v predlogu direktive je treba izrecno navesti, da osebni podatki, ki so zaradi preglednosti dani na voljo, ne bodo zlorabljeni za dodatne nepovezane namene, ter da je treba za ta namen izvajati tehnološke in organizacijske ukrepe na podlagi načela vgrajene zasebnosti,

— v predlog je treba vključiti tudi posebne zaščitne ukrepe v zvezi s posredovanjem obvestil osebam, na katere se podatki nanašajo, in zahtevo za razvoj modalitet ureditve, da se osebam, na katere se podatki nanašajo, omogoči uveljavljanje njihovih pravic v delegiranih aktih.

V Bruslju, 6. maja 2011

Giovanni BUTTARELLI

Pomočnik Evropskega nadzornika za varstvo podatkov