Eiropas Datu aizsardzības uzraudzītāja atzinuma kopsavilkums par Komisijas un Eiropas Savienības Augstā pārstāvja ārlietās un drošības politikas jautājumos kopīgu paziņojumu "Eiropas Savienības kiberdrošības stratēģija – atvērta un droša kibertelpa" un par Komisijas priekšlikumu direktīvai par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā

(Šā atzinuma pilns teksts angļu, franču un vācu valodā ir pieejams EDAU tīmekļa vietnē http://www.edps.europa.eu)

(2014/C 32/10)

1. **Ievads**

1.1. *Apspriešanās ar EDAU*

1. Komisija un Eiropas Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos 2013. gada 7. februārī pieņēma kopīgu paziņojumu Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Eiropas Savienības kiberdrošības stratēģija – atvērta un droša kibertelpa" ([1]) (turpmāk tekstā "kopīgais paziņojums", "kiberdrošības stratēģija" vai "stratēģija").

2. Tajā pašā dienā Komisija pieņēma priekšlikumu Eiropas Parlamenta un Padomes direktīvai par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā ([2]) (turpmāk tekstā "piedāvātā direktīva" vai "priekšlikums"). Šo priekšlikumu nosūtīja EDAU apspriešanai 2013. gada 7. februārī.

3. Pirms kopīgā paziņojuma un priekšlikuma pieņemšanas EDAU tika dota iespēja sniegt neoficiālas atsauksmes Komisijai. Viņš atzinīgi novērtē to, ka dažas no šīm atsauksmēm ir ņemtas vērā kopīgajā paziņojumā un priekšlikumā.

4. **Secinājumi**

74. EDAU atzinīgi novērtē to, ka Komisija un Augstais pārstāvis ārlietās un drošības politikas jautājumos ir izstrādājuši visaptverošu kiberdrošības stratēģiju, ko papildina priekšlikums direktīvai par pasākumiem, kas nodrošinātu augsta līmeņa tīklu un informācijas drošību (TID) visā Savienībā. Stratēģija papildina ES jau izstrādātās politikas darbības tīklu un informācijas drošības jomā.

75. EDAU atzinīgi novērtē to, ka stratēģija ir plašāka par tradicionālo pieeju, kurā drošība tiek pretstatīta privātumam, paredzot precīzi formulētu privātuma un datu aizsardzības atzīšanu par pamatvērtību, kam ES un starptautiskajā mērogā būtu jābūt kiberdrošības politikas pamatā. EDAU atzīmē, ka kiberdrošības stratēģijai un piedāvātajai direktīvai par TID var būt būtiska nozīme, cenšoties nodrošināt privātpersonu tiesību uz privātumu aizsardzību un datu aizsardzību tiešsaistes vidē. Tajā pašā laikā ir jānodrošina, lai ar stratēģiju un direktīvu netiktu ieviesti pasākumi, kas nozīmētu nelikumīgu iejaukšanos privātpersonu tiesībās uz privātumu un datu aizsardzību.

76. EDAU arī atzinīgi novērtē to, ka datu aizsardzība ir pieminēta vairākās stratēģijas daļās un ir ņemta vērā piedāvātajā direktīvā par TID. Taču viņš pauž nožēlu par to, ka stratēģijā un piedāvātajā direktīvā nav labāk uzsvērts esošo un gaidāmo datu aizsardzības tiesību aktu devums attiecībā uz drošību un ka tās pilnībā nenodrošina, lai jebkādas saistības, kas izriet no piedāvātās direktīvas, vai citi stratēģijas elementi papildinātu datu aizsardzības saistības un nedublētu viens otru, vai arī nebūtu pretrunīgi.

77. Turklāt EDAU atzīmē, ka sakarā ar to, ka līdz galam nav apsvērtas un ņemtas vērā citas paralēlās Komisijas iniciatīvas un pašreiz notiekošie likumdošanas procesi, piemēram, datu aizsardzības reforma un piedāvātā regula par elektronisko identifikāciju un uzticamības pakalpojumiem, kiberdrošības stratēģija nenodrošina patiešām visaptverošu un kopīgu ainu attiecībā uz kiberdrošību ES un riskē iemūžināt

([1]) JOIN(2013) 1 *final.*
([2]) COM(2013) 48 *final.*

fragmentāru un saskaldītu pieeju. EDAU arī atzīmē, ka piedāvātā direktīva par TID arī vēl nepieļauj visaptverošu pieeju saistībā ar drošību ES un ka saistības, kas noteiktas datu aizsardzības tiesību aktos, iespējams, ir visaptverošākās tīklu un informācijas drošības saistības ES tiesību aktos.

78. EDAU pauž nožēlu arī par to, ka nav pienācīgi apsvērta arī datu aizsardzības iestāžu nozīme ar drošību saistīto saistību īstenošanā un izpildīšanā, ka arī kiberdrošības palielināšanā.

79. Attiecībā uz kiberdošības stratēģiju EDAU atzīmē, ka:

— ļoti svarīgi ir skaidri definēt terminus "kiberelastīgums", "kibernoziedzība" un "kiberaizsardzība", jo šie termini tiek izmantoti kā attaisnojums noteiktiem īpašiem pasākumiem, kas varētu aizskart pamattiesības, tostarp tiesības uz privātumu un datu aizsardzību. Taču stratēģijā un Konvencijā par kibernoziedzību "kibernoziedzības" definīcijas joprojām ir pārāk plašas. Būtu ieteicams izstrādāt skaidru un *ierobežojošu* "kibernoziedzības" definīciju, nevis tādu, kurā ir ietverts pārāk daudz,

— datu aizsardzības tiesību akti būtu jāpiemēro visām darbībām stratēģijas ietvaros, ja tās attiecas uz pasākumiem, kas saistīti ar personas datu apstrādi. Lai gan datu aizsardzības tiesību akti nav konkrēti minēti nodaļās, kas attiecas uz kibernoziegumiem un kiberaizsardzību, EDAU uzsver, ka daudzas šajās jomās plānotās darbības varētu būt saistītas ar personas datu apstrādi un tāpēc uz tām būtu jāattiecina datu aizsardzības tiesību akti. Viņš atzīmē arī, ka daudzas darbības sastāv no saskaņošanas mehānismu izveides, kas prasīs ieviest attiecīgas datu aizsardzības garantijas saistībā ar personas datu apmaiņas kārtību,

— datu aizsardzības iestādēm (DAI) ir liela nozīme saistībā ar kiberdrošību. Kā privātpersonu privātuma un datu aizsardzības tiesību sargātājas datu aizsardzības iestādes ir aktīvi iesaistītas privātpersonu personas datu aizsardzībā gan bezsaistes, gan tiešsaistes režīmā. Tāpēc tām atbilstoši savam uzraudzības iestāžu statusam būtu jābūt pienācīgi iesaistītām īstenošanas pasākumos, kas saistīti ar personas datu apstrādi (piemēram, ES pilotprojektā par robottīklu un destruktīvu programmatūru apkarošanu). Arī citiem kiberdrošības nozares pārstāvjiem, pildot savus pienākumus, būtu jāsadarbojas ar DAI, piemēram, apmainoties ar labākajām praksēm un organizējot informētības paaugstināšanas pasākumus. EDAU un valstu datu aizsardzības iestādēm būtu pienācīgi jāiesaistās augsta līmeņa konferencē, kas tiks sasaukta 2014. gadā, lai novērtētu stratēģijas īstenošanas gaitu.

80. Attiecībā uz piedāvāto TID direktīvu EDAU iesaka likumdevējiem:

— nodrošināt vairāk skaidrības un noteiktības 3. panta 8. punktā par to tirgus dalībnieku definīciju, uz kuriem attiecas priekšlikums, un izveidot izsmeļošu sarakstu, kurā ietvertas visas attiecīgās ieinteresētās personas, lai nodrošinātu pilnībā saskaņotu un vienotu pieeju attiecībā uz drošību visā ES,

— izskaidrot 1. panta 2. punkta c) apakšpunktā, ka piedāvātā direktīva attiecas uz visām ES iestādēm un struktūrām, un priekšlikuma 1. panta 5. punktā iekļaut atsauci uz Regulu (EK) Nr. 45/2001,

— atzīt, ka šā priekšlikuma nozīme attiecībā uz drošību ir horizontālāka, 1. pantā skaidri paredzot tā piemērošanu, neskarot esošos vai turpmākos sīki izstrādātos noteikumus konkrētās jomās (piemēram, tādās, kas minētas saistībā ar uzticamības pakalpojumu sniedzējiem piedāvātajā regulā par elektronisko identifikāciju),

— pievienot apsvērumu, lai paskaidrotu nepieciešamību nostiprināt integrētu un automātisku datu aizsardzību, jau sākot no priekšlikumā noteikto mehānismu projektēšanas sākumstadijas, un visā saistīto procesu, procedūru, organizāciju, tehniku un infrastruktūru dzīves ciklā, ņemot vērā piedāvāto datu aizsardzības regulu,

— izskaidrot 3. panta 1. punktā "tīklu un informācijas sistēmas" un 3. panta 4. punktā "incidenta" definīciju un 5. panta 2. punktā aizstāt pienākumu izveidot "risku novērtēšanas plānu" ar "izveidot un uzturēt riska pārvaldības regulējumu",

— noteikt 1. panta 6. punktā, ka saskaņā ar Direktīvas 95/46/EK 7. panta e) punktu personas datu apstrāde ir pamatota tiktāl, cik tas nepieciešams piedāvātajā direktīvā izvirzīto sabiedrībai svarīgo mērķu sasniegšanai. Taču, tā kā ir jānodrošina nepieciešamības un proporcionalitātes principu ievērošana, tad apstrādāti tiek tikai tie dati, kas patiešām ir nepieciešami nolūka sasniegšanai,

— noteikt 14. pantā apstākļus, kad ir nepieciešams paziņojums, kā arī paziņojuma saturu un formātu, tostarp tos personas datu veidus, kas būtu jāpaziņo, un to, vai paziņojumā un to atbalstošos dokumentos būtu vai nebūtu jāiekļauj, un ja būtu, tad kādā apjomā, personas datu sīka informācija (piemēram, IP adreses), ko var ietekmēt kāds noteikts drošības incidents. Jāņem vērā fakts, ka TID jomas kompetentajām iestādēm būtu jāļauj savākt un apstrādāt personas datus drošības incidenta ietvaros tikai tad, ja tas ir patiešām nepieciešams. Priekšlikumā būtu jāparedz arī piemērotas garantijas, lai nodrošinātu TID jomas kompetento iestāžu apstrādāto datu attiecīgu aizsardzību,

— izskaidrot 14. pantā, ka paziņošana par incidentiem saskaņā ar 14. panta 2. punktu būtu jāpiemēro, neskarot piemērojamajos datu aizsardzības tiesību aktos paredzētos paziņošanas pienākumus par personas datu aizsardzības pārkāpumiem. Priekšlikumā būtu jāparedz galvenie procedūras aspekti TID kompetento iestāžu sadarbībai ar datu aizsardzības iestādēm gadījumos, kad drošības incidents ietver personas datu aizsardzības pārkāpumu,

— grozīt 14. panta 8. punktu tā, ka paziņošanas neattiecināšana uz mikrouzņēmumiem neattiektos uz tiem tirgus dalībniekiem, kam ir izšķiroša nozīme informācijas sabiedrības pakalpojumu sniegšanā, piemēram, ņemot vērā to apstrādātās informācijas raksturu (piemēram, biometriskos datus vai sensitīvos datus),

— pievienot priekšlikumā noteikumus, kas regulētu turpmāko TID kompetento iestāžu veikto personas datu apmaiņu ar citiem saņēmējiem, lai nodrošinātu, ka i) tiek atklāti tikai tie personas dati, kuru apstrāde ir nepieciešama viņu pienākumu izpildei ar attiecīgu tiesisko pamatu, un ii) šāda informācija tiek ierobežota tikai līdz tai, kas ir nepieciešama viņu pienākumu izpildei. Ir jāņem vērā arī tas, kā iestādes, kas sniedz datus informācijas apmaiņas tīklam, nodrošina atbilstību datu izmantošanas mērķa ierobežojuma principam,

— noteikt laika ierobežojumu personas datu uzglabāšanai nolūkos, kas noteikti piedāvātajā direktīvā, jo īpaši attiecībā uz tādu datu uzglabāšanu, ko veic TID kompetentās iestādes, un kas notiek sadarbības tīkla drošas infrastruktūras ietvaros,

— atgādināt TID kompetentajām iestādēm par to pienākumu sniegt attiecīgu informāciju datu subjektiem par personas datu apstrādi, piemēram, ievietojot privātuma politiku savā tīmekļa vietnē,

— pievienot noteikumu attiecībā uz drošības līmeni, kas TID kompetentajām iestādēm ir jāievēro attiecībā uz savākto, apstrādāto un apmainīto informāciju. Būtu speciāli jāiekļauj atsauce uz Direktīvas 95/46/EK 17. panta drošības prasībām attiecībā uz personas datu aizsardzību, ko nodrošina TID kompetentās iestādes Izskaidrot 9. panta 2. punktā, ka kritērijiem par dalībvalstu piedalīšanos drošā informācijas apmaiņas sistēmā būtu jānodrošina, ka visi dalībnieki informācijas apmaiņas sistēmās visos apstrādes posmos garantē augsta līmeņa drošību un stabilitāti. Saskaņā ar Direktīvas 95/46/EK 16. un 17. pantu un Regulas (EK) Nr. 45/2001 21. un 22. pantu šiem kritērijiem būtu jāietver attiecīgi konfidencialitātes un drošības pasākumi. Šie kritēriji būtu skaidri jāattiecina uz Komisijas līdzdalību drošas informācijas apmaiņas sistēmas pārziņa statusā,

— pievienot 9. pantā Komisijas un dalībvalstu uzdevumus un atbildību saistībā ar drošas informācijas apmaiņas sistēmas izveidi, darbību un uzturēšanu un noteikt, ka sistēmas izveidei jānotiek saskaņā ar integrētas datu aizsardzības, automātiskas datu aizsardzības un integrētas drošības principiem, un

— minēt 13. pantā, ka jebkādai personas datu pārsūtīšanai saņēmējiem, kuri atrodas ārpus ES, jānotiek saskaņā ar Direktīvas 95/46/EK 25. un 26. pantu un Regulas (EK) Nr. 45/2001 9. pantu.

Briselē, 2013. gada 14. jūnijā

Eiropas Datu aizsardzības uzraudzītājs

Peter HUSTINX