Europos duomenų apsaugos priežiūros pareigūno nuomonės dėl bendro Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai komunikato „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“ ir Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti pasiūlymo santrauka

(Visą šios nuomonės tekstą anglų, prancūzų ir vokiečių kalbomis galima rasti EDAPP interneto svetainėje http://www.edps.europa.eu)

(2014/C 32/10)

1. **Įvadas**

1.1. *EDAPP konsultacija*

1. 2013 m. vasario 7 d. Komisija ir Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai priėmė komunikatą Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“ ([1]) (toliau – Bendras komunikatas, Kibernetinio saugumo strategija arba Strategija).

2. Tą pačią dieną Komisija priėmė Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti pasiūlymą ([2]) (toliau – siūloma direktyva arba pasiūlymas). Šis pasiūlymas EDAPP konsultacijai išsiųstas 2013 m. vasario 7 d.

3. Prieš priimant Bendrą komunikatą ir pasiūlymą, EDAPP suteikta galimybė pateikti Komisijai neoficialias pastabas. Jis palankiai vertina tai, kad Bendrame komunikate ir pasiūlyme į kai kurias jo pastabas atsižvelgta.

4. **Išvados**

74. EDAPP palankiai vertina tai, kad Komisija ir Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai pateikė išsamią Kibernetinio saugumo strategiją, kuri papildyta direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų (TIS) saugumo lygiui visoje Sąjungoje užtikrinti pasiūlymu. Šia strategija papildomi politikos veiksmai, kuriuos ES jau yra išplėtojusi tinklų ir informacinio saugumo srityje.

75. EDAPP palankiai vertina tai, kad strategijoje laikomasi ne vien tradicinio požiūrio priešinti saugumą ir privatumą ir kad privatumas ir duomenų apsauga aiškiai pripažįstama pagrindinėmis vertybėmis, kuriomis turėtų būti vadovaujamasi formuojant kibernetinio saugumo politiką ES ir tarptautiniu lygmeniu. EDAPP pažymi, kad kibernetinio saugumo strategija ir siūloma direktyva dėl TIS gali labai padėti užtikrinti asmenų teisių į privatumą ir duomenų apsaugą interneto aplinkoje. Kartu reikia užtikrinti, kad dėl jų neatsirastų priemonių, kuriomis būtų neteisėtai ribojamos asmenų teisės į privatumą ir duomenų apsaugą.

76. EDAPP taip pat palankiai vertina tai, kad keliose strategijos dalyse paminėta duomenų apsauga ir kad į ją atsižvelgta siūlomoje direktyvoje dėl TIS. Tačiau jis apgailestauja, kad strategijoje ir siūlomoje direktyvoje nėra tinkamai pabrėžiamas esamų ir būsimų duomenų apsaugos teisės aktų indėlis į saugumą ir iki galo neužtikrinama, kad bet kokios iš siūlomos direktyvos ar kitų strategijos dalių atsirandančios pareigos papildytų duomenų apsaugos srities pareigas, nesutaptų ir neprieštarautų tarpusavyje.

77. Be to, EDAPP pažymi, kad dėl motyvų stokos ir visapusiai atsižvelgiant į kitas lygiagrečias Komisijos iniciatyvas bei tebevykdomas teisėkūros procedūras, pvz., duomenų apsaugos reformą ir siūlomą reglamentą dėl elektroninės atpažinties ir patikimumo užtikrinimo paslaugų, Kibernetinio saugumo strategijoje neužtikrinamas tikrai visapusis ir holistinis požiūris į kibernetinį saugumą ES, be to, ja gali būti išlaikytas

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

suskaidytas ir nevienodas požiūris. EDAPP taip pat pažymi, kad pagal siūlomą direktyvą dėl TIS visapusis požiūris į saugumą ES dar nėra įmanomas ir kad duomenų apsaugos teisės aktuose nustatyta pareiga yra bene išsamiausia tinklo ir saugumo pareiga pagal ES teisę.

78. EDAPP taip pat apgailestauja, kad nėra tinkamai atsižvelgta į duomenų apsaugos institucijų vaidmenį įgyvendinant saugumo pareigas, užtikrinant jų įgyvendinimą ir stiprinant kibernetinį saugumą.

79. Dėl kibernetinio saugumo strategijos EDAPP pažymi, kad:

— labai svarbu aiškiai apibrėžti sąvokas „kibernetinis atsparumas“, „elektroniniai nusikaltimai“ ir „kibernetinė gynyba“, nes šios sąvokos vartojamos pateisinti tam tikroms specialioms priemonėms, kuriomis gali būti apribotos pagrindinės teisės, įskaitant teisę į privatumą ir duomenų apsaugą. Tačiau strategijoje ir Elektroninių nusikaltimų konvencijoje sąvoka „elektroniniai nusikaltimai“ apibrėžta labai plačiai. Patartina aiškiai ir siaurai, o ne visaapimančiai apibrėžti sąvoką „elektroniniai nusikaltimai“,

— duomenų apsaugos teisės aktai turėtų būti taikomi visiems strategijos veiksmams, jeigu tik jie susiję su priemonėmis, apimančiomis asmens duomenų tvarkymą. Nors duomenų apsaugos teisės aktai nėra konkrečiai paminėti skyriuose, susijusiuose su elektroniniais nusikaltimais ir kibernetine gynyba, EDAPP pabrėžia, kad daugelis toje srityje planuojamų veiksmų apimtų asmens duomenų tvarkymą, taigi, patektų į taikytinų duomenų apsaugos teisės aktų taikymo sritį. Jis taip pat pažymi, kad daugelis veiksmų pasireiškia koordinavimo mechanizmų sukūrimu, o tam reikės įgyvendinti atitinkamas duomenų apsaugos garantijas, susijusias su keitimosi asmens duomenimis ypatumais,

— duomenų apsaugos institucijos (DAI) atlieka svarbų vaidmenį kibernetinio saugumo srityje. Būdamos asmenų privatumo ir duomenų apsaugos teisių sergėtojomis, DAI aktyviai saugo jų asmens duomenis interneto ir ne interneto aplinkoje. Todėl jos pagal savo kaip priežiūros įstaigų kompetenciją turėtų atitinkamai dalyvauti, kalbant apie įgyvendinimo priemones, susijusias su asmens duomenų tvarkymu (pvz., pradedant ES bandomąjį projektą dėl robotų tinklų (botnetų) ir kenkimo programinės įrangos). Kiti kibernetinio saugumo srityje veiklą vykdantys subjektai taip pat turėtų su jomis bendradarbiauti, vykdydami savo užduotis, pvz., keisdamiesi geriausia patirtimi ir organizuodami informuotumo didinimo veiksmus. EDAPP ir nacionalinės DAI taip pat turėtų atitinkamai dalyvauti aukšto lygio konferencijoje 2014 m., kad įvertintų strategijos įgyvendinimo pažangą.

80. Dėl siūlomos TIS direktyvos EDAPP rekomenduoja teisės aktų leidėjams:

— 3 straipsnio 8 dalyje aiškiau ir griežčiau suformuluoti rinkos subjektų, patenkančių į pasiūlymo taikymo sritį, apibrėžtį ir sudaryti išsamų sąrašą, į kurį būtų įtraukti visi atitinkami suinteresuotieji subjektai, siekiant užtikrinti visiškai suderintą ir integruotą požiūrį į saugumą ES,

— siūlomos direktyvos 1 straipsnio 2 dalies c punkte patikslinti, kad ji taikoma ES institucijoms ir įstaigoms, o į pasiūlymo 1 straipsnio 5 dalį įtraukti nuorodą į Reglamentą (EB) Nr. 45/2001,

— pripažinti horizontalesnį šio pasiūlymo vaidmenį saugumo srityje, jo 1 straipsnyje aiškiai nustatant, kad jis turėtų būti taikomas nepažeidžiant esamų ar būsimų išsamesnių konkrečios srities taisyklių (pvz., tų, kurios bus nustatytos patikimumo užtikrinimo paslaugų teikėjams siūlomame reglamente dėl elektroninės atpažinties),

— įtraukti konstatuojamąją dalį, kurioje būtų paaiškintas poreikis diegti pritaikytąją ir numatytąją duomenų apsaugą pasiūlyme numatytu ankstyvuoju mechanizmų projektavimo etapu ir per visą atitinkamų procesų, procedūrų, organizacijų, metodų ir infrastruktūros gyvavimo ciklą, atsižvelgiant į siūlomą Duomenų apsaugos reglamentą,

— patikslinti 3 straipsnio 1 dalyje esančios sąvokos „tinklo ir informacinė sistema“ ir 3 straipsnio 4 dalyje esančios sąvokos „incidentas“ apibrėžtis ir 5 straipsnio 2 dalyje įtvirtintą pareigą nustatyti „rizikos vertinimo planą“ pakeisti pareiga „sukurti ir išlaikyti rizikos valdymo sistemą“,

— 1 straipsnio 6 dalyje nurodyti, kad asmens duomenų tvarkymas būtų pateisinamas pagal Direktyvos 95/46/EB 7 straipsnio e punktą, jeigu jis būtų būtinas siūlomoje direktyvoje numatytiems viešojo intereso tikslams pasiekti. Tačiau būtina užtikrinti tinkamą būtinumo ir proporcingumo principų laikymąsi, kad būtų tvarkomi tik griežtai būtini numatytam tikslui pasiekti reikalingi duomenys,

— 14 straipsnyje nurodyti aplinkybes, kuriomis yra reikalingas pranešimas, taip pat pranešimo turinį ir formą, įskaitant asmens duomenų rūšis, apie kurias reikia pranešti, taip pat ar ir kokiu mastu pranešime ir jo patvirtinamuosiuose dokumentuose bus nurodyti asmens duomenys, susiję su konkrečiu saugumo incidentu (pvz., IP adresai). Būtina atsižvelgti į tai, kad įvykus saugumo incidentui kompetentingoms TIS institucijoms turėtų būti leidžiama rinkti ir tvarkyti atitinkamus asmens duomenis tik jeigu tai yra griežtai būtina. Be to, pasiūlyme derėtų numatyti atitinkamas garantijas kompetentingų TIS institucijų tvarkomų duomenų tinkamai apsaugai užtikrinti,

— 14 straipsnyje patikslinti, kad pagal 14 straipsnio 2 dalį nurodyti pranešimai apie incidentą turėtų būti teikiami nepažeidžiant pareigų teikti pranešimus apie asmens duomenų pažeidimą pagal taikytinus duomenų apsaugos teisės aktus. Pasiūlyme reikėtų nurodyti svarbiausius kompetentingų TIS institucijų ir DAI bendradarbiavimo procedūros aspektus tais atvejais, kai saugumo incidentas susijęs su asmens duomenų pažeidimu,

— pakeisti 14 straipsnio 8 dalį taip, kad pranešimo netaikymo labai mažoms įmonėms taisyklė nebūtų taikoma tiems ūkio subjektams, kurie atlieka esminį vaidmenį teikiant informacinės visuomenės paslaugas, pvz., atsižvelgiant į jų tvarkomos informacijos pobūdį (pvz., biometrinius duomenis arba neskelbtinus duomenis),

— įtraukti į pasiūlymą nuostatas, kuriomis būtų reglamentuotas kompetentingų TIS institucijų būsimas keitimasis asmens duomenimis su kitais gavėjais siekiant užtikrinti, kad: i) asmens duomenys būtų atskleidžiami tik tiems gavėjams, kuriems duomenis būtina tvarkyti dėl jų atliekamų funkcijų remiantis atitinkamu teisiniu pagrindu; ir ii) tokia informacija apimtų tik tai kas yra būtina jų funkcijoms atlikti. Be to, reikėtų atsižvelgti į tai, kaip subjektai, teikiantys duomenis keitimosi informacija tinklui, užtikrina tikslo ribojimo principo laikymąsi,

— nurodyti asmens duomenų saugojimo siūlomoje direktyvoje numatytais tikslais terminą, visų pirma kalbant apie kompetentingų TIS institucijų ir naudojant saugią bendradarbiavimo tinklo infrastruktūrą saugomus duomenis,

— priminti kompetentingoms TIS institucijoms jų pareigą teikti atitinkamą informaciją duomenų subjektams apie asmens duomenų tvarkymą, pvz., jų interneto svetainėje paskelbiant privatumo politiką,

— įtraukti nuostatą dėl renkamos, tvarkomos informacijos ir informacijos, kuria keičiamasi, saugumo lygio, kurį turi užtikrinti kompetentingos TIS institucijos. Kalbant apie kompetentingų TIS institucijų taikomą asmens duomenų apsaugą, reikėtų įtraukti konkrečią nuorodą į Direktyvos 95/46/EB 17 straipsnyje nustatytus saugumo reikalavimus,

— 9 straipsnio 2 dalyje patikslinti, kad kriterijais, nustatančiais valstybių narių dalyvavimo saugioje keitimosi informacija sistemoje tvarką, turėtų būti užtikrinta, jog visi keitimosi informacija sistemų dalyviai visais tvarkymo etapais garantuotų aukštą saugumo ir atsparumo lygį. Tarp šių kriterijų, laikantis Direktyvos 95/46/EB 16 ir 17 straipsnių bei Reglamento (EB) Nr. 45/2001 21 ir 22 straipsnių, turėtų būti atitinkamos konfidencialumo ir saugumo priemonės. Šie dalyvavimo kriterijai turėtų būti aiškiai privalomi Komisijai kaip saugios keitimosi informacija sistemos duomenų valdytojai,

— 9 straipsnyje apibūdinti Komisijos ir valstybių narių vaidmenis ir atsakomybės sritis kuriant, eksploatuojant ir techniškai prižiūrint saugaus keitimosi informacija sistemą ir numatyti, kad sistema turėtų būti projektuojama pagal pritaikytosios ir numatytosios duomenų apsaugos principus, taip pat pagal pritaikytojo saugumo principą, ir

— 13 straipsnį papildyti nuostata, kad bet koks asmens duomenų perdavimas gavėjams, įsikūrusiems ne ES valstybėse narėse, turėtų būti vykdomas laikantis Direktyvos 95/46/EB 25 ir 26 straipsnių bei Reglamento (EB) Nr. 45/2001 9 straipsnio.

Priimta Briuselyje 2013 m. birželio 14 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas