EUROPOS KOMISIJA

Briuselis, 2010.11.4
KOM(2010) 609 galutinis

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje

1. NAUJI UŽDAVINIAI ASMENS DUOMENŲ APSAUGOS SRITYJE

1995 m. Duomenų apsaugos direktyva[1] – labai svarbus teisės aktas Europos Sąjungos asmens duomenų apsaugos istorijoje. Direktyvoje įtvirtinti du seni ir vienodai svarbūs Europos integracijos proceso užmojai: viena vertus, apsaugoti asmenų pagrindines teises ir laisves, visų pirma pagrindinę teisę į duomenų apsaugą, kita vertus, sukurti vidaus rinką, o šiuo atveju tai reiškia – užtikrinti laisvą asmens duomenų judėjimą.

Praėjus penkiolikai metų, šis dvejopas tikslas tebėra aktualus, o direktyvoje įtvirtinti principai pagrįsti. **Tačiau sparčiai plėtojant technologijas ir vykstant globalizacijai pasaulis iš esmės pasikeitė, todėl asmens duomenų apsaugos srityje kilo naujų uždavinių.**

Šiandien asmenys, naudodamiesi technologijomis, gali lengvai dalytis informacija apie savo elgseną bei pomėgius ir labai plačiu mastu viešai skelbti ją visame pasaulyje. Šimtus milijonų narių visame pasaulyje turinčių socialinių tinklų svetainės – tikriausiai pats akivaizdžiausias, tačiau ne vienintelis šio reiškinio pavyzdys. Uždavinių duomenų apsaugos srityje taip pat gali kilti plėtojant tinklo kompiuteriją (angl. *cloud computing*): t. y. interneto kompiuterija, kurioje naudojama programinė įranga, bendri ištekliai ir informacija yra saugomi nuotoliniuose serveriuose (tinkle), todėl gali būti, kad įvedę savo duomenis į kitų subjektų techninę įrangą įrašytas programas asmenys nebegalės kontroliuoti galimai neskelbtinos informacijos. Neseniai atliktas tyrimas patvirtino, kad duomenų apsaugos institucijų, įmonių asociacijų ir vartotojų organizacijų nuomonė – kad internetinės veiklos grėsmės privatumui ir asmens duomenų saugumui didėja – iš esmės sutampa[2].

Be to, **asmens duomenų rinkimo būdai tapo gerokai sudėtingesni ir sunkiau atsekami**. Pavyzdžiui, naudodamiesi moderniomis priemonėmis ūkinės veiklos vykdytojai gali stebėti asmenų elgseną ir teikti jiems tikslingesnę informaciją. Vis plačiau naudojant technologijas, kuriomis galima automatiškai rinkti duomenis, pvz., išduodant elektroninius transporto bilietus ir renkant kelių mokesčius, ar geografinės vietos nustatymo prietaisus, asmenų buvimo vietą nustatyti lengviau paprasčiausiai todėl, kad jie pasinaudoja mobiliuoju prietaisu. Viešosios institucijos, naudodamosi e. valdžios taikomosiomis programomis ir kt. priemonėmis, taip pat naudoja vis daugiau asmens duomenų įvairiais tikslais, pavyzdžiui, kad galėtų atsekti asmenis užkrečiamų ligų protrūkio atveju, užkirsti kelią terorizmui bei nusikaltimams ir veiksmingiau su jais kovoti, valdyti socialinės apsaugos sistemas, vykdyti mokesčių politiką.

---

1 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995 11 23, p. 31).

2 Žr. 2010 m. liepos mėn. „London Economics“ parengtą *Privatumo didinimo technologijų ekonominės naudos tyrimą* (angl. *Study on the economic benefits of privacy enhancing technologies*), p. 14 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf).

Atsižvelgiant į tai, neišvengiamai kyla klausimas, ar ES duomenų apsaugos teisės aktais vis dar įmanoma visapusiškai ir veiksmingai įgyvendinti šiuos uždavinius.

Siekdama atsakyti šį klausimą, Komisija ėmėsi dabartinės teisės sistemos peržiūros, kurią 2009 m. gegužės mėn. pradėjo aukšto lygio konferencija, po to iki 2009 m. pabaigos vyko viešos konsultacijos[3]. Be to, pradėta keletas tyrimų[4].

Iš nustatytų faktų matyti, kad pagrindiniai direktyvos principai tebėra aktualūs ir kad jos technologinį neutralumą reikėtų išlaikyti. Tačiau nustatyta keletas sudėtingų problemų, kurioms išspręsti būtina įgyvendinti tam tikrus uždavinius. Uždaviniai:

- *Išspręsti naujų technologijų poveikio problemas*

Iš per konsultacijas pateiktų privačių asmenų ir organizacijų atsakymų matyti, kad reikia aiškiau ir konkrečiau reglamentuoti duomenų apsaugos principų taikymą naujoms technologijoms ir taip užtikrinti, kad asmenų asmens duomenys būtų realiai veiksmingai saugomi, neatsižvelgiant į tai, kokia technologija naudojama jų duomenims tvarkyti, ir kad duomenų valdytojai būtų visapusiškai informuoti apie naujų technologijų poveikį duomenų apsaugai. Šis klausimas iš dalies sprendžiamas Direktyva 2002/58/EB (toliau – E. privatumo direktyva)[5], kurioje konkrečiau išdėstomos ir papildomos bendrosios Duomenų apsaugos direktyvos nuostatos, taikomos elektroninių ryšių sektoriui[6].

- *Stiprinti duomenų apsaugos vidaus rinkos aspektą*

Viena pagrindinių suinteresuotosioms šalims, visų pirma tarptautinėms bendrovėms, susirūpinimą keliančių problemų – nors nustatyta bendra ES teisės sistema, valstybių narių duomenų apsaugos teisės aktai nepakankamai suderinti. Jos pabrėžė, kad reikia padidinti teisinį tikrumą, sumažinti administracinę naštą ir užtikrinti vienodas sąlygas ūkinės veiklos vykdytojams ir kitiems duomenų valdytojams.

---

3 Žr. per Komisijos viešas konsultacijas pateiktus atsakymus (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm). Konkretesnės konsultacijos su suinteresuotosiomis šalimis vyko 2010 m. Be to, 2010 m. spalio 5 d. aukšto lygio susitikimui su suinteresuotosiomis šalimis Briuselyje pirmininkavo Komisijos pirmininko pavaduotoja Viviane Reding. Komisija konsultavosi ir su 29 straipsnio darbo grupe, kuri visapusiškai prisidėjo prie 2009 m. konsultacijų (WP 168) ir 2010 m. liepos mėn. priėmė specialią nuomonę dėl atskaitomybės sąvokos (WP 173).

4 Be Privatumo didinimo technologijų ekonominės naudos tyrimo (minėto 2 išnašoje), žr. 2010 m. sausio mėn. parengtą Skirtingų požiūrių į naujus privatumo srities uždavinius lyginamąją analizę, visų pirma atsižvelgiant į technologijų plėtrą (angl. *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*) (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). Be to, tebevyksta būsimos ES asmens duomenų apsaugos teisės sistemos poveikio vertinimo tyrimas.

5 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių; OL L 201, 2002 7 31, p. 37).

6 Duomenų apsaugos direktyvoje 95/46/EB nustatomi duomenų apsaugos standartai, taikomi visiems ES teisės aktams, įskaitant E. privatumo direktyvą 2002/58/EB (su pakeitimais, padarytais Direktyva 2009/136/EB; OL L 337, 2009 12 18, p. 11). E. privatumo direktyva susijusi su asmens duomenų tvarkymu viešaisiais ryšių tinklais teikiant viešai prieinamas elektroninių ryšių paslaugas. Joje teikiamos konkrečios elektroninių ryšių sektoriui taikomos taisyklės, pagrįstos Duomenų apsaugos direktyvoje išdėstytais principais. Direktyva 95/46/EB, be kita ko, taikoma neviešųjų ryšių paslaugoms.

- *Išspręsti su globalizacija susijusias problemas ir pagerinti tarptautinį duomenų perdavimą*

Kelios suinteresuotosios šalys pabrėžė, kad tvarkymo paslaugos vis dažniau užsakomos, labai dažnai ES nepriklausančiose šalyse, todėl kyla problemų dėl tvarkymui taikytinos teisės ir susijusios atsakomybės pasidalijimo. Daugelis organizacijų manė, kad esamos tarptautinio duomenų perdavimo sistemos nėra visiškai tinkamos ir turi būti peržiūrėtos ir supaprastintos, kad perduoti duomenis būtų paprasčiau ir lengviau.

- *Sustiprinti institucines priemones veiksmingam duomenų apsaugos taisyklių įgyvendinimui užtikrinti*

Suinteresuotosios šalys sutaria, kad siekiant užtikrinti geresnį duomenų apsaugos taisyklių įgyvendinimą būtina sustiprinti duomenų apsaugos institucijų įgaliojimus. Kai kurios organizacijos taip pat nurodė, kad 29 straipsnio darbo grupės darbas turėtų būti skaidresnis (*žr. 2.5 punktą*), o jos užduotys ir įgaliojimai – aiškesni.

- *Pagerinti duomenų apsaugos teisės sistemos suderinamumą*

Per viešas konsultacijas visos suinteresuotosios šalys pabrėžė, kad reikia visuotinės priemonės, kuri būtų taikoma duomenų tvarkymo operacijoms visuose sektoriuose ir visose Sąjungos politikos srityse ir kuria būtų užtikrinamas integruotas požiūris ir vientisa, nuosekli bei veiksminga apsauga[7].

Kad išspręstų minėtus uždavinius, **ES turi parengti visapusišką ir nuoseklų požiūrį** ir taip užtikrinti, kad **pagrindinės asmenų teisės į duomenų apsaugą būtų visapusiškai laikomasi ES ir už jos ribų**. Lisabonos sutartimi ES suteiktos papildomos priemonės šiam tikslui pasiekti – ES pagrindinių teisių chartija, kurios 8 straipsnyje išskirtinai pripažįstama teisė į asmens duomenų apsaugą, tapo teisiškai privaloma, be to, nustatytas naujas teisinis pagrindas[8], kuriuo sudarytos galimybės priimti visapusišką ir nuoseklų Sąjungos teisės aktą dėl asmenų apsaugos tvarkant jų asmens duomenis ir laisvo tokių duomenų judėjimo. Visų pirma, vadovaudamasi naujuoju teisiniu pagrindu ES gali priimti bendrą teisės priemonę duomenų apsaugai reguliuoti, be kita ko, policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje. Bendros užsienio ir saugumo politikos sričiai SESV 16 straipsnis taikomas tik iš dalies, nes konkrečios valstybių narių duomenų tvarkymo taisyklės turi būti nustatytos Tarybos sprendimu, remiantis kitu teisiniu pagrindu[9].

Išnaudodama šias naujas teisines galimybes, Komisija pirmiausia sieks užtikrinti, kad visoje Sąjungos teritorijoje ir visose jos politikos srityse būtų laikomasi pagrindinės teisės į duomenų apsaugą, ir kartu stiprinti vidaus rinkos aspektą ir palengvinti laisvą asmens duomenų judėjimą. Taigi, užtikrinant pagrindinę teisę į asmens duomenų apsaugą, taip pat būtina visapusiškai atsižvelgti į kitas chartijoje įtvirtintas pagrindines teises ir kitus sutartyse nustatytus tikslus.

Šio komunikato tikslas – išdėstyti Komisijos požiūrį siekiant atnaujinti ES asmens duomenų apsaugos visose Sąjungos veiklos srityse teisės sistemą, visų pirma atsižvelgiant į su globalizacija ir naujomis technologijomis susijusius uždavinius, kad toliau būtų užtikrinamas

---

[7] Pasibaigus viešoms konsultacijoms Europolas ir Eurojustas atskiruose pareiškimuose paprašė bet kokiu atveju atsižvelgti į jų darbo specifiką koordinuojant teisėsaugos ir nusikaltimų prevencijos veiklą.

[8] Žr. Sutarties dėl Europos Sąjungos veikimo (SESV) 16 straipsnį.

[9] Žr. SESV 16 straipsnio 2 dalies paskutinę pastraipą ir Europos Sąjungos sutarties (ESS) 39 straipsnį.

aukštas asmenų apsaugos lygis tvarkant jų asmens duomenis visose Sąjungos veiklos srityse. Taip ES galės toliau aktyviai propaguoti aukštus duomenų apsaugos standartus visame pasaulyje.

2. PAGRINDINIAI VISAPUSIŠKO POŽIŪRIO Į DUOMENŲ APSAUGĄ TIKSLAI

2.1. Asmenų teisių stiprinimas

2.1.1. Užtikrinti tinkamą asmenų apsaugą visomis aplinkybėmis

Dabartiniuose ES duomenų apsaugos teisės aktuose nustatytomis taisyklėmis siekiama **saugoti fizinių asmenų pagrindines teises, visų pirma teisę į asmens duomenų apsaugą**, kaip nustatyta ES pagrindinių teisių chartijoje[10].

Sąvoka „asmens duomenys“ – viena pagrindinių asmenų apsaugos sąvokų dabartiniuose ES duomenų apsaugos teisės aktuose – tai duomenų valdytojų ir duomenų tvarkytojų[11] įpareigojimų taikymo pagrindas. Sąvokos „asmens duomenys“ apibrėžtimi siekta įtraukti visą informaciją, tiesiogiai ar netiesiogiai susijusią su asmeniu, kurio tapatybė nustatyta arba gali būti nustatyta. Kad būtų galima nuspręsti, ar galima nustatyti asmens tapatybę, reikėtų atsižvelgti į „visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens tapatybei nustatyti“[12]. Šio požiūrio, kurį teisės leidėjas pasirinko apgalvotai, privalumas – jo lankstumas; jį galima taikyti įvairiose su pagrindinėmis teisėmis susijusiose situacijose ir įvairiomis aplinkybėmis, įskaitant tas, kurių priimant direktyvą nebuvo įmanoma numatyti. Tačiau tokio plataus ir lankstaus požiūrio rezultatas – daugeliu atvejų įgyvendinant direktyvą ne visuomet aišku, kokios pozicijos laikytis, ar asmenys naudojasi duomenų apsaugos teisėmis ir ar duomenų valdytojai turėtų laikytis direktyvoje nustatytų įpareigojimų[13].

Yra tokių atvejų, kai tvarkant specialią informaciją pagal Sąjungos teisę reikėtų imtis papildomų priemonių. Tokios priemonės tam tikrais atvejais jau nustatytos. Pavyzdžiui, informaciją galiniame įrenginyje (pvz., mobiliajame telefone) galima išsaugoti, tik jei tas asmuo davė sutikimą. Šį klausimą taip pat gali tekti spręsti ES lygmeniu, pvz., tais atvejais, kai tvarkomi raktu užkoduoti duomenys bei buvimo vietos duomenys ir naudojamos duomenų gavybos technologijos, kuriomis sudaromos galimybės sujungti įvairių šaltinių duomenis, arba tais atvejais, kai būtina užtikrinti informacinių technologijų sistemų konfidencialumą ir patikimumą[14].

Todėl visus minėtus klausimus būtina nuodugniai išnagrinėti.

---

10 Žr. Europos Teisingumo Teismo 2003 m. Sprendimo *Bodil Lindqvist*, C-101/01, Rink. p. I-1297, 96 ir 97 punktus ir 2008 m. Sprendimą *Productores de Música de España (Promusicae) prieš Telefónica de España SAU*, C-275/06, Rink. p. I-271. Žr. taip pat Europos Žmogaus Teisių Teismo sprendimus, pvz., 2008 m. gruodžio 4 d. Sprendimą *S. ir Marper prieš Jungtinę Karalystę* (peticijų Nr. 30562/04 ir 30566/04) ir 2000 m. gegužės 4 d. Sprendimą *Rotaru prieš Rumuniją* (Nr. 28341/95, § 55, EˇTT 2000–V).

11 Sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ apibrėžtys pateiktos Direktyvos 95/46/EB 2 straipsnio d ir e punktuose.

12 Žr. Direktyvos 95/46/EB 26 konstatuojamąją dalį.

13 Žr., pvz., 29 straipsnio darbo grupės nuomonėje Nr. 4/2007 dėl asmens duomenų sąvokos (WP 136) nagrinėjamą IP adresų atvejį.

14 Žr., pvz., 2008 m. vasario 27 d. Vokietijos Federalinio Konstitucinio Teismo (vok. *Bundesverfassungsgericht*) Sprendimą 1 *BvR* 370/07.

Komisija svarstys, **kaip užtikrinti nuoseklų duomenų apsaugos taisyklių taikymą, atsižvelgdama į naujų technologijų poveikį asmenų teisėms ir laisvėms ir į siekį užtikrinti laisvą asmens duomenų judėjimą vidaus rinkoje**.

2.1.2. Didinti duomenų subjektų skaidrumą

Skaidrumas – būtina sąlyga, kad asmenys galėtų kontroliuoti savo duomenis ir kad būtų galima užtikrinti veiksmingą asmens duomenų apsaugą. Todėl labai svarbu, kad duomenų valdytojai **gerai, aiškiai ir skaidriai informuotų** asmenis apie tai, kaip ir kas renka ir tvarko jų duomenis, kokiais tikslais, kokiam laikotarpiui ir kokios jų teisės, jei jie nori susipažinti su savo duomenimis, juos ištaisyti ar ištrinti. Atitinkamų nuostatų dėl duomenų subjektui teiktinos informacijos[15] nepakanka.

Pagrindiniai skaidrumo reikalavimai: **informacija turi būti lengvai prieinama ir lengvai suprantama, pateikiama aiškia ir paprasta kalba**. Tai ypač svarbu teikiant informaciją internete, kuriame privatumo pranešimai gana dažnai yra neaiškūs, sunkiai prieinami, neskaidrūs[16] ir kartais neatitinka galiojančių taisyklių. Toks atvejis galimas vartotojų elgsena grindžiamos internetinės reklamos srityje, nes tiek dėl vis didėjančio subjektų, dalyvaujančių teikiant tokią reklamą, skaičiaus, tiek dėl naudojamų technologijų sudėtingumo asmenims sunku nustatyti ir suprasti, ar jų asmens duomenys yra renkami, kas juos renka ir kokiais tikslais.

Tokiomis aplinkybėmis **vaikai** turi būti ypač saugomi, nes jie gali nevisiškai suprasti su asmens duomenų tvarkymu susijusias grėsmes, padarinius, apsaugos priemones ir teises[17].

Komisija svarstys, ar:

- į teisės sistemą įtraukti **bendrąjį skaidraus asmens duomenų tvarkymo principą**;

- nustatyti **konkrečius įpareigojimus** duomenų valdytojams dėl teiktinos informacijos pobūdžio ir jos teikimo **būdų**, įskaitant informacijos teikimą **vaikams**;

- parengti vieną ar kelias **ES standartines formas** (**informacinius privatumo pranešimus**), kuriomis turėtų naudotis duomenų valdytojai.

Be to, svarbu informuoti asmenis tuo atveju, jei jų duomenys buvo atsitiktinai ar neteisėtai sunaikinti, prarasti, pakeisti, su jų duomenimis susipažino neįgalioti asmenys arba tie duomenys buvo jiems atskleisti. Neseniai peržiūrėjus E. privatumo direktyvą įtraukta **privalomo pranešimo apie asmens duomenų saugumo pažeidimą** nuostata, tačiau ji taikoma tik telekomunikacijų sektoriui. Kadangi duomenų saugumo pažeidimai gali būti vykdomi ir kituose, pvz., finansų, sektoriuose, Komisija nagrinės galimybes įpareigojimą pranešti apie asmens duomenų saugumo pažeidimus nustatyti ir kituose sektoriuose, atsižvelgdama į savo 2009 m. deklaraciją dėl pranešimo apie duomenų saugumo pažeidimą,

---

15 Žr. Direktyvos 95/46/EB 10 ir 11 straipsnius.

16 Iš 2009 m. Eurobarometro atliktos apklausos matyti, kad maždaug pusė respondentų manė, jog privatumo pranešimai svetainėse yra labai arba gana neaiškūs (žr. greitąją Eurobarometro apklausą Nr. 282 http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

17 Žr. kokybinį tyrimą „Saugesnis internetas vaikams“ (angl. *Safer Internet for Children*) apie 9–10 ir 12–14 metų vaikus, iš kurio matyti, kad vaikai nepakankamai suvokia su interneto naudojimu susijusias grėsmes ir sumenkina savo rizikingo elgesio padarinius (galima rasti adresu http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

pateiktą Europos Parlamentui siekiant pertvarkyti elektroninių ryšių reguliavimo sistemą[18]. Šis nagrinėjimas nesusijęs su E. privatumo direktyvos nuostatomis, kurias į nacionalinę teisę būtina perkelti iki 2011 m. gegužės 25 d.[19]. Sprendžiant šį klausimą būtina laikytis nuoseklaus ir visapusiško požiūrio.

Komisija

- nagrinės galimybes į bendrąją teisės sistemą įtraukti **bendrąją pranešimo apie asmens duomenų saugumo pažeidimą nuostatą**, įskaitant tokių pranešimų adresatus ir įpareigojimo pranešti kriterijus.

2.1.3. Didinti duomenų subjektų galimybes kontroliuoti savo duomenis

Siekiant užtikinti, kad asmenų duomenys būtų tinkamai saugomi, būtina įvykdyti šias dvi svarbias sąlygas: **duomenų valdytojai gali tvarkyti duomenis tik numatytais tikslais (duomenų kiekio mažinimo principas)**, o duomenų subjektai toliau **veiksmingai kontroliuoja savo duomenis**. Chartijos 8 straipsnio 2 dalyje nustatyta, kad „kiekvienas turi teisę susipažinti su surinktais jo asmens duomenimis bei į tai, kad jie būtų ištaisomi“. Asmenys turi visada galėti susipažinti su savo duomenimis, juos ištaisyti, ištrinti ar sustabdyti jų tvarkymą, nebent yra įstatymais nustatytų teisėtų priežasčių to neleisti. Šios teisės jau įtvirtintos dabartinėje teisės sistemoje. Tačiau naudojimosi šiomis teisėmis priemonės nesuderintos, todėl kai kuriose valstybėse narėse jomis pasinaudoti praktiškai yra lengviau, kitose – sunkiau. Be to, dabar tai ypač sudėtinga internete, nes duomenys dažnai išsaugomi nepranešus susijusiam asmeniui ir (arba) be jo sutikimo.

Internetiniai socialiniai tinklai – ypač aktualus pavyzdys, nes jų nariai, norėdami veiksmingai kontroliuoti savo asmens duomenis, patiria didelių sunkumų. Komisija yra gavusi įvairių užklausų iš asmenų, kuriems kartais nepavykdavo atgauti savo asmens duomenų iš interneto paslaugų teikėjų, pavyzdžiui, nuotraukų, taigi, jie negalėjo pasinaudoti teisėmis susipažinti su duomenimis, juos ištaisyti ir ištrinti.

Todėl šias teises reikėtų reglamentuoti aiškiau ir tiksliau, o galbūt ir sustiprinti.

Todėl Komisija nagrinės, kaip:

- sustiprinti **duomenų kiekio mažinimo principą**;

- **pagerinti galimybes** faktiškai naudotis **teisėmis susipažinti su duomenimis, juos ištaisyti, ištrinti ar sustabdyti jų tvarkymą** (pvz., nustatyti atsakymų į asmenų prašymus terminą, leisti naudotis teisėmis elektroninėmis priemonėmis arba įtvirtinti principą, kad teisė susipažinti su duomenimis turėtų būti užtikrinama nemokamai);

---

[18] „Komisija atkreipia dėmesį į Europos Parlamento norą pareigą pranešti apie asmens duomenų saugumo pažeidimus taikyti ne tik elektroninių ryšių sektoriuje, bet ir įstaigoms, pavyzdžiui, informacinės visuomenės paslaugų teikėjams […]. Todėl Komisija nedelsdama pradės tinkamus parengiamuosius darbus, įskaitant konsultacijas su suinteresuotais subjektais, siekdama prireikus ne vėliau kaip 2011 m. pabaigoje pateikti pasiūlymus šioje srityje […].“ Galima rasti adresu http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009–0360+0+DOC+XML+V0//LT. Žr. taip pat Direktyvos 2009/136/EB, kuria iš dalies keičiama E. privatumo direktyva 2002/58/EB, 59 konstatuojamąją dalį: „Paslaugų gavėjų interesas būti informuotiems aiškiai neapsiriboja vien tik elektroninių ryšių sektoriumi, todėl Bendrijos lygmeniu prioritetine tvarka turėtų būti nustatyti aiškūs, privalomi reikalavimai dėl pranešimo, taikomi visuose sektoriuose“.

[19] Direktyvos 2009/136/EB 4 straipsnis.

- aiškiau reglamentuoti vadinamąją „**teisę būti pamirštam**“, t. y. asmenų teisę į tai, kad jų duomenys nebebūtų tvarkomi ir būtų ištrinti, jei tų duomenų nebereikia siekiant teisėtų tikslų. Pavyzdžiui, jei duomenys tvarkomi remiantis asmens sutikimu, o tas asmuo atšaukia savo sutikimą, arba pasibaigus duomenų saugojimo laikotarpiui;

- papildyti duomenų subjektų teises užtikrinant **duomenų perkeliamumą**, t. y. aiškiai nustatyti asmens teisę duomenų valdytojui netrukdant atšaukti savo duomenis (pvz., nuotraukas ar draugų sąrašą) iš vienos programos ar paslaugos, kad atšauktus duomenis būtų galima perkelti į kitą programą ar paslaugą, kiek tai techniškai įmanoma.

2.1.4. Didinti informuotumą

Skaidrumas – būtina sąlyga, tačiau taip pat reikia geriau informuoti plačiąją visuomenę, visų pirma jaunimą, apie asmens duomenų tvarkymo grėsmes ir susijusias teises. Per 2008 m. Eurobarometro apklausą nustatyta, kad labai daug ES valstybių narių gyventojų mano, jog jų šalies visuomenė nedaug žino apie asmens duomenų apsaugą[20]. Todėl įvairūs subjektai – valstybių narių institucijos, visų pirma duomenų apsaugos institucijos ir švietimo įstaigos, duomenų valdytojai ir pilietinės visuomenės asociacijos – turėtų skatinti ir propaguoti informuotumo didinimo veiklą. Jie turėtų imtis ir neteisinių priemonių, pvz., rengti informavimo kampanijas spaudoje ir elektroninėje žiniasklaidoje, taip pat aiškiai teikti informaciją interneto svetainėse, tiksliai išdėstyti duomenų subjektų teises ir duomenų valdytojų atsakomybę.

Komisija tirs, ar:

- galima iš Sąjungos biudžeto **bendrai finansuoti informuotumo didinimo veiklą duomenų apsaugos srityje**;

- reikia ir ar būtų galima į teisės sistemą įtraukti **įpareigojimą vykdyti informuotumo didinimo veiklą** šioje srityje.

2.1.5. Užtikrinti informuoto duomenų subjekto savanorišką sutikimą

Jei reikia informuoto duomenų subjekto sutikimo, galiojančiose taisyklėse nustatyta, kad asmens sutikimas tvarkyti jo asmens duomenis – tai „savanoriškai ir žinomai duotas konkretus duomenų subjekto pareiškimas“, kuriuo jis nurodo savo sutikimą, kad būtų tvarkomi jo duomenys[21]. Tačiau šiuo metu šios sąlygos valstybėse narėse vertinamos skirtingai: kai kuriose valstybėse narėse nustatytas bendras rašytinio sutikimo reikalavimas, kai kuriose – užtenka netiesioginio sutikimo.

Be to, dėl privatumo politikos skaidrumo stokos internete asmenys dažnai prasčiau žino apie savo teises ir informuoto duomenų subjekto sutikimą duoti yra sunkiau. Padėtis yra dar sudėtingesnė dėl to, kad kai kuriais atvejais neaišku, kas yra savanoriškai duotas konkretus informuoto duomenų subjekto sutikimas tvarkyti duomenis, pvz., vartotojų elgsena grindžiamos reklamos atveju vieni, priešingai nei kiti, mano, kad naudotojo sutikimas gaunamas interneto naršyklės nustatymais.

---

[20] Žr. greitąją Eurobarometro apklausą Nr. 225 „Duomenų apsauga Europos Sąjungoje“ http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[21] Žr. Direktyvos 95/46/EB 2 straipsnio h punktą.

Todėl reikėtų aiškiau išdėstyti duomenų subjekto sutikimo sąlygas, kad būtų visada užtikrinamas informuoto duomenų subjekto sutikimas, o asmuo visiškai suprastų, kad duoda sutikimą ir kaip jo duomenys bus tvarkomi, kaip nustatyta ES pagrindinių teisių chartijos 8 straipsnyje. Jei pagrindinės sąvokos būtų aiškios, gali būti lengviau imtis savireguliavimo iniciatyvų, kuriomis siekiama ieškoti praktinių ES teisę atitinkančių sprendimų.

Komisija nagrinės, kaip **aiškiau išdėstyti ir sugriežtinti su sutikimu susijusias taisykles**.

2.1.6. Saugoti neskelbtinus duomenis

Apskritai dabar jau draudžiama tvarkyti neskelbtinus duomenis, t. y. duomenis, susijusius su rasine ar etnine kilme, politiniais, religiniais ir filosofiniais įsitikinimais, naryste profesinėje sąjungoje, taip pat informaciją apie asmens sveikatą ar intymų gyvenimą, tačiau numatyta keletas išimčių, taikomų įvykdžius tam tikras sąlygas ir laikantis tam tikrų apsaugos priemonių[22]. Tačiau atsižvelgiant į technologijų ir visuomenės raidą, būtina peržiūrėti galiojančias neskelbtinų duomenų nuostatas, išnagrinėti, ar reikėtų įtraukti kitų duomenų kategorijų, ir aiškiau reglamentuoti jų tvarkymo sąlygas. Tai susiję, pavyzdžiui, su genetiniais duomenimis, kurie šiuo metu aiškiai nepriskirti neskelbtinų duomenų kategorijai.

Komisija svarstys:

- ar prie **neskelbtinų duomenų** reikėtų priskirti kitų kategorijų duomenis, pavyzdžiui, **genetinius** duomenis;

- galimybes dar aiškiau reglamentuoti ir **suderinti sąlygas**, kurias įvykdžius leidžiama tvarkyti neskelbtinų duomenų kategorijų duomenis.

2.1.7. Didinti taisomųjų priemonių ir sankcijų veiksmingumą

Kad būtų užtikrintas duomenų apsaugos taisyklių įgyvendinimas, būtina įtvirtinti **veiksmingas taisomųjų priemonių ir sankcijų nuostatas**. Daugeliu atvejų, jei dėl duomenų apsaugos taisyklių pažeidimo daromas poveikis vienam asmeniui, toks poveikis daromas ir daugeliui kitų panašioje padėtyje esančių asmenų.

Todėl Komisija:

- svarstys galimybę **suteikti** duomenų apsaugos institucijoms, pilietinės visuomenės asociacijoms ir **kitoms duomenų subjektų interesus ginančioms asociacijoms įgaliojimą kreiptis į nacionalinius teismus**;

- vertins, ar reikia **sugriežtinti galiojančias sankcijų nuostatas**, pavyzdžiui, aiškiai nustatant baudžiamąsias sankcijas už sunkius duomenų apsaugos pažeidimus, siekiant padidinti jų veiksmingumą.

[22] Žr. Direktyvos 95/46/EB 8 straipsnį.

2.2. Vidaus rinkos aspekto stiprinimas

2.2.1. Didinti teisinį tikrumą ir užtikrinti vienodas sąlygas duomenų valdytojams

Duomenų apsaugai ES **labai svarbus vidaus rinkos aspektas**, t. y. būtinybė užtikrinti laisvą asmens duomenų judėjimą tarp valstybių narių vidaus rinkoje. Taigi, direktyva siekiama ne minimaliai, bet iš esmės visiškai suderinti nacionalinius duomenų apsaugos teisės aktus[23].

Tačiau kartu direktyvoje nustatyta, kad valstybės narės tam tikrais atvejais gali veikti laisvai ir išlaikyti ar nustatyti konkrečioms situacijoms taikomas specialias taisykles[24]. Dėl šios priežasties, taip pat dėl to, kad valstybės narės kartais neteisingai įgyvendinimo direktyvos nuostatas, **direktyvą įgyvendinantys nacionaliniai teisės aktai skiriasi, o tai neatitinka vieno iš pagrindinių direktyvos tikslų – užtikrinti laisvą asmens duomenų judėjimą vidaus rinkoje**. Tai taikoma daugeliui sektorių ir daugelyje situacijų, pvz., tvarkant asmens duomenis įdarbinimo ar visuomenės sveikatos tikslais. Nepakankamai suderintos nuostatos iš tiesų yra nuolatinė svarbi privačių suinteresuotųjų subjektų, ypač ūkinės veiklos vykdytojų, iškelta problema, nes dėl to jie patiria papildomų išlaidų ir padidėja jų administracinė našta. Tai ypač aktualu keliose valstybėse narėse įsikūrusiems duomenų valdytojams, kurie privalo laikytis kiekvienos šalies reikalavimų ir praktikos. Be to, kadangi valstybės narės skirtingai įgyvendina direktyvą, teisinio netikrumo problemą patiria ne tik duomenų valdytojai, bet ir duomenų subjektai, todėl gali būti iškreiptas vienodas apsaugos lygis, kurio siekiama ir kuris turėtų būti užtikrintas įgyvendinus direktyvą.

Komisija nagrinės galimybes **dar labiau suderinti duomenų apsaugos taisykles ES lygmeniu**.

2.2.2. Mažinti administracinę naštą

Užtikrinus vienodas sąlygas, sumažės poreikis laikytis skirtingų nacionalinių reikalavimų, taigi, duomenų valdytojų administracinė našta taip pat gerokai sumažės. Kitas svarbus žingsnis siekiant palengvinti duomenų valdytojų administracinę naštą ir sumažinti išlaidas – **peržiūrėti ir supaprastinti dabartinę pranešimo sistemą**[25]. Duomenų valdytojai iš esmės sutaria, kad galiojanti bendroji pareiga pranešti apie visas duomenų tvarkymo operacijas duomenų apsaugos institucijoms apsunkina jų darbą ir asmens duomenų apsaugos požiūriu realiai neduoda jokios papildomos naudos. Be to, tai vienas iš atvejų, kai valstybėms narėms pagal direktyvą suteikiama tam tikra veikimo laisvė, todėl jos gali laisvai spręsti dėl galimų išimčių, supaprastintos tvarkos ir taikytinų procedūrų.

Suderinus ir supaprastinus sistemą, sumažėtų duomenų valdytojų, ypač keliose valstybėse narėse įsikūrusių tarptautinių bendrovių, išlaidos ir administracinė našta.

Komisija svarstys įvairias galimybes, kaip **supaprastinti ir suderinti galiojančią pranešimo sistemą**, įskaitant galimybę parengti **bendrąją ES registracijos formą**.

---

[23] 2003 m. Europos Teisingumo teismo Sprendimas *Bodil Lindqvist*, C-101/01, Rink. p. I-1297, 96 ir 97 punktai.

[24] Ten pat, 97 punktas. Žr. taip pat Direktyvos 95/46/EB 9 konstatuojamąją dalį.

[25] Žr. Direktyvos 95/46/EB 18 straipsnį.

2.2.3. Aiškiau išdėstyti taikytinos teisės ir valstybių narių atsakomybės taisykles

Jau 2003 m. pirmojoje Duomenų apsaugos direktyvos įgyvendinimo ataskaitoje[26] Komisija pabrėžė, kad taikytinos teisės nuostatos[27] buvo „keliais atvejais nepakankamos, todėl galėjo kilti tokio pobūdžio teisės kolizijų, kurių šiuo straipsniu siekiama išvengti“. Padėtis nuo tada nepagerėjo, todėl duomenų valdytojai ir duomenų apsaugos priežiūros institucijos kartais negali aiškiai nustatyti, kokia valstybė narė yra atsakinga ir kokia teisė turėtų būti taikoma, jei atvejis susijęs su keliomis valstybėmis narėmis. Tokie atvejai ypač dažni, jei duomenų valdytojas turi laikytis kelių valstybių narių skirtingų reikalavimų, jei tarptautinė bendrovė įsikūrusi daugiau nei vienoje valstybėje narėje arba jei duomenų valdytojas įsikūręs ne ES, tačiau teikia paslaugas ES gyventojams.

Sudėtingumas taip pat didėja dėl globalizacijos ir technologijų raidos – duomenų valdytojai vis dažniau veikia keliose valstybėse narėse bei jurisdikcijose ir teikia paslaugas bei pagalbą visą parą. Naudodamiesi internetu duomenų valdytojai, įsikūrę Europos ekonominei erdvei (EEE)[28] nepriklausančioje šalyje, gali gerokai paprasčiau teikti paslaugas nuotoliniu būdu ir tvarkyti asmens duomenis internetu; taigi, dažnai sunku nustatyti asmens duomenų ir naudojamos įrangos vietą tam tikru metu (pvz., tinklo kompiuterijos programų ir paslaugų atveju).

Tačiau Komisija mano, kad apsaugos, į kurią asmenys turi teisę pagal ES pagrindinių teisių chartiją ir ES duomenų apsaugos teisės aktus, jie neturėtų netekti dėl to, kad jų asmens duomenis tvarko trečiojoje šalyje įsikūręs duomenų valdytojas.

Komisija nagrinės, kaip **peržiūrėti ir aiškiau išdėstyti galiojančias taikytinos teisės nuostatas**, įskaitant dabartinius nustatymo kriterijus, ir taip padidinti teisinį tikrumą, aiškiau išdėstyti valstybių narių atsakomybę taikant duomenų apsaugos taisykles ir, galiausiai, užtikrinti vienodą ES duomenų subjektų apsaugą neatsižvelgiant į geografinę duomenų valdytojo vietą.

2.2.4. Didinti duomenų valdytojų atsakomybę

Supaprastinus administracines procedūras, **duomenų valdytojų atsakomybė užtikrinant veiksmingą duomenų apsaugą apskritai neturėtų sumažėti**. Priešingai, Komisija mano, kad jų įpareigojimai turėtų būti aiškiau išdėstyti teisės sistemoje, įskaitant vidaus kontrolės mechanizmų ir bendradarbiavimo su duomenų apsaugos priežiūros institucijomis įpareigojimus. Be to, reikėtų užtikrinti, kad tokia atsakomybė būtų taip pat taikoma duomenų valdytojams, kurie privalo laikytis profesinės paslapties prievolių (pvz., advokatai), ir tais vis dažniau pasitaikančiais atvejais, kai duomenų valdytojai duomenų tvarkymą paveda kitiems subjektams (pvz., duomenų tvarkytojams).

Todėl Komisija nagrinės, kaip **užtikrinti, kad duomenų valdytojai įgyvendintų veiksmingą politiką ir mechanizmus, skirtus duomenų apsaugos taisyklių laikymuisi užtikrinti**. Nagrinėdama šį klausimą, Komisija atsižvelgs į dabartines diskusijas dėl galimo atskaitomybės (angl. *accountability*) principo nustatymo[29]. Ji nesiektų didinti duomenų

---

[26] Komisijos ataskaita – Pirmoji Duomenų apsaugos direktyvos (95/46/EB) įgyvendinimo ataskaita, COM (2003) 265.

[27] Žr. Direktyvos 95/46/EB 4 straipsnį.

[28] Europos ekonominei erdvei taip pat priklauso Norvegija, Lichtenšteinas, Islandija.

[29] Žr. visų pirma liepos 13 d. 29 straipsnio darbo grupės priimtą nuomonę Nr. 3/2010.

valdytojų administracinės naštos; tokiomis priemonėmis ji pirmiausia siektų nustatyti apsaugos priemones ir mechanizmus, kuriais veiksmingiau laikomasi duomenų apsaugos taisyklių, ir kartu sumažinti ir supaprastinti tam tikrus administracinius formalumus, pvz., pranešimo tvarką (*žr. 2.2.2 punktą*).

Siekiant šio tikslo ir, be kita ko, užtikrinant duomenų saugumą, svarbu skatinti naudotis privatumo didinimo technologijomis, kaip jau nustatyta susijusiame 2007 m. Komisijos komunikate, ir laikytis principo „privatumo apsauga visą ciklą“[30].

Siekdama didinti duomenų valdytojų atsakomybę, Komisija nagrinės šiuos klausimus:

– nustatyti privalomą nepriklausomo **duomenų apsaugos pareigūno** paskyrimą ir atsižvelgiant į reikiamas ribas, kad būtų išvengta netinkamos administracinės naštos, visų pirma mažoms ir labai mažoms įmonėms, suderinti su jo užduotimis ir kompetencija susijusias taisykles[31];

– į teisės sistemą įtraukti duomenų valdytojų įpareigojimą tam tikrais atvejais atlikti **duomenų apsaugos poveikio vertinimą**, pavyzdžiui, jei tvarkomi neskelbtini duomenys, jei kitaip dėl tvarkymo pobūdžio, visų pirma naudojant tam tikras technologijas, mechanizmus ar procedūras, įskaitant profiliavimą ar vaizdo stebėjimo sistemas, galėtų kilti tam tikra grėsmė;

– toliau skatinti naudotis privatumo didinimo technologijomis ir galimybes praktiškai įgyvendinti sąvoką **„privatumo apsauga visą ciklą“**.

2.2.5. Skatinti savireguliavimo iniciatyvas ir nagrinėti ES sertifikavimo sistemas

Komisija tebemano, kad duomenų valdytojų **savireguliavimo iniciatyvos** gali būti **naudingos siekiant veiksmingiau įgyvendinti duomenų apsaugos taisykles**. Privačios suinteresuotosios šalys iki šiol retai naudojosi galiojančiomis Duomenų apsaugos direktyvos savireguliavimo nuostatomis, visų pirma elgesio kodeksų rengimo srityje[32], ir mano, kad jos yra nepatenkinamos.

Be to, Komisija tirs galimybes sukurti privatumo reikalavimus atitinkančių procesų, technologijų, produktų ir paslaugų ES **sertifikavimo sistemas (pvz., privatumo apsaugos ženklų sistema)**[33]. Taigi, asmenys – tokių technologijų, produktų ir paslaugų naudotojai – būtų geriau informuoti, be to, duomenų valdytojams būtų lengviau spręsti atsakomybės klausimą: duomenų valdytojams, pasirinkusiems sertifikuotas technologijas, produktus ar paslaugas, būtų lengviau įrodyti, kad įvykdė įpareigojimus (*žr. 2.2.4 punktą*). Žinoma, būtų labai svarbu **užtikrinti tokių privatumo apsaugos ženklų patikimumą** ir išsiaiškinti, kaip jie dera su teisiniais įsipareigojimais ir tarptautiniais techniniais standartais.

---

30 Dėl privatumo didinimo technologijų žr. Komisijos komunikatą Europos Parlamentui ir Tarybai dėl duomenų apsaugos stiprinimo naudojant privatumo didinimo technologijas, COM (2007) 228. Principas „privatumo apsauga visą ciklą“ reiškia, kad privatumas ir duomenys yra saugomi visą technologijų būvio ciklą – nuo jų pradinio kūrimo etapo iki jų diegimo, naudojimo ir atsisakymo. Šis principas, be kita ko, minimas Komisijos komunikate „Europos skaitmeninė darbotvarkė“, COM (2010) 245.

31 Dabartine galimybe duomenų valdytojui paskirti duomenų apsaugos pareigūną, kad būtų nepriklausomai užtikrinamas ES ir nacionalinių duomenų apsaugos taisyklių laikymasis ir padedama asmenims, jau pasinaudojo kelios valstybės narės (žr., pvz., „Beauftragter für den Datenschutz“ Vokietijoje ir „correspondant informatique et libertés (CIL)“ Prancūzijoje).

32 Žr. Direktyvos 95/46/EB 27 straipsnį.

33 Dėl šio klausimo taip pat žr. 30 išnašoje minėtą Komunikatą dėl privatumo didinimo technologijų.

Komisija:

- nagrinės galimybes **toliau skatinti savireguliavimo iniciatyvas**, įskaitant aktyvų elgesio kodeksų skatinimą;

- tirs, ar įmanoma sukurti **ES sertifikavimo sistemas** privatumo ir duomenų apsaugos srityse.

2.3. Duomenų apsaugos taisyklių, taikomų policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje, peržiūra

Duomenų apsaugos direktyva taikoma visai asmens duomenų tvarkymo veiklai valstybėse narėse, tiek viešajame, tiek privačiajame sektoriuose. Tačiau ji netaikoma tvarkant asmens duomenis, „kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį“, pvz., policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje[34]. Tačiau Lisabonos sutartimi buvo panaikinta ankstesnė ES ramsčių struktūra ir nustatytas naujas visapusiškas asmens duomenų apsaugos visose Sąjungos politikos srityse teisinis pagrindas[35]. Atsižvelgiant į tai ir į ES pagrindinių teisių chartiją, Komisijos komunikatuose dėl Stokholmo programos ir Stokholmo veiksmų plano[36] pabrėžiama, kad būtina sukurti „išsamią apsaugos sistemą“ ir „sustiprinti ES poziciją dėl asmens duomenų apsaugos visų sričių ES politikoje, įskaitant teisėsaugą ir nusikaltimų prevenciją“.

ES asmens duomenų apsaugos policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje priemonė – **Pamatinis sprendimas 2008/977/TVR**[37]. Šis pamatinis sprendimas – svarbi pažangos priemonė šioje srityje, kur bendri duomenų apsaugos standartai buvo labai reikalingi. Tačiau reikia dirbti toliau.

Pamatinis sprendimas taikomas tik tarpvalstybiniu mastu keičiantis asmens duomenimis ES, o ne vykdant nacionalinio lygmens duomenų tvarkymo operacijas valstybėse narėse. Praktiškai tai sunku atskirti, todėl pamatinį sprendimą įgyvendinti ir taikyti faktiškai gali būti sudėtinga[38].

Be to, **pamatiniame sprendime numatyta pernelyg plati tikslų apribojimo principo išimtis**. Kitas trūkumas – nenustatyta, kad reikėtų skirti skirtingas duomenų kategorijas pagal jų tikslumą ir patikimumą, kad reikėtų skirti faktais pagrįstus duomenis nuo nuomonėmis ir asmeniniu vertinimu pagrįstų duomenų[39] ir kad reikėtų skirti įvairias duomenų subjektų kategorijas (nusikaltėliai, įtariamieji, nukentėjusieji, liudininkai ir t. t.), numatant specialias su neįtariamais asmenimis susijusiems duomenims taikomas garantijas[40].

---

34 Žr. Direktyvos 95/46/EB 3 straipsnio 2 dalies pirmą įtrauką.

35 Žr. SESV 16 straipsnį.

36 Žr. COM (2009) 262, 2009 6 10, ir COM (2010) 171, 2010 4 20.

37 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (OL L 350, 2008 12 30, p. 60). Pamatiniame sprendime numatyta duomenų apsaugos standartus derinti tik minimaliai.

38 Tai neskiriama atitinkamuose Europos Tarybos dokumentuose, pvz., Konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Europos Tarybos sutarčių sąrašo Nr. 108), jos Papildomame protokole dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų (Europos Tarybos sutarčių sąrašo Nr. 181) ir 1987 m. rugsėjo 17 d. Europos Tarybos Ministrų Komiteto rekomendacijoje valstybėms narėms Nr. R (87) 15, reglamentuojančioje asmens duomenų naudojimą policijos sektoriuje.

39 Kaip reikalaujama pagal Rekomendacijos Nr. R (87) 15 3.2 principą.

40 Prieštaraujama Rekomendacijos Nr. R (87) 15 2 principui ir susijusioms vertinimo ataskaitoms.

Be to, **šiuo pamatiniu sprendimu nepakeičiamos įvairios ES lygmeniu priimtos konkrečiai šiam sektoriui skirtos teisėkūros priemonės dėl policijos ir teisminio bendradarbiavimo baudžiamosiose bylose**[41], visų pirma priemonės, kuriomis reglamentuojamas Europolo, Eurojusto, Šengeno informacinės sistemos (SIS) ir Muitinės informacinės sistemos (MIS)[42] veikimas ir kuriose paprastai nustatoma speciali duomenų apsaugos tvarka ir (arba) remiamasi Europos Tarybos duomenų apsaugos dokumentais. Policijos ir teisminio bendradarbiavimo veiklai reguliuoti visos valstybės narės įsipareigojo įgyvendinti Europos Tarybos rekomendaciją Nr. R (87) 15, kurioje išdėstyti policijos sektoriui skirti 108-osios konvencijos principai. Tačiau tai nėra teisiškai privalomas dokumentas.

Todėl gali būti tiesiogiai ribojamos asmenų galimybės naudotis savo duomenų apsaugos teisėmis šioje srityje (pvz., sužinoti, kokie asmens duomenys tvarkomi ir kokiais duomenimis keičiamasi, kas tvarko tuos duomenis ir kokiu tikslu, kaip pasinaudoti savo teisėmis, pvz., teise susipažinti su savo duomenimis).

Siekiant sukurti visapusišką ir nuoseklią sistemą ES, taikomą ir trečiųjų šalių atžvilgiu, būtina **svarstyti galimybę peržiūrėti galiojančias duomenų apsaugos taisykles policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje**. Komisija pabrėžia, kad remiantis visapusiškos duomenų apsaugos sistemos sąvoka neatmetama galimybė konkrečias duomenų apsaugos policijos ir teismų sektoriuje taisykles įtraukti į bendrąją sistemą, tinkamai atsižvelgiant į specifinį šios srities pobūdį, kaip nurodyta prie Lisabonos sutarties pridėtoje deklaracijoje Nr. 21. Todėl būtina, pavyzdžiui, nustatyti, kiek asmeniui naudojantis tam tikromis duomenų apsaugos teisėmis gali būti trukdoma vykdyti nusikalstamų veikų prevenciją, jas tirti, nustatyti, o jų vykdytojus patraukti baudžiamojon atsakomybėn arba tam tikrais atvejais – vykdyti bausmes.

Komisija visų pirma:

- svarstys galimybę **bendrąsias duomenų apsaugos taisykles pradėti taikyti policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje**, be kita ko, tvarkant duomenis nacionaliniu lygmeniu, prireikus nustatant tam tikrų duomenų apsaugos teisių, pvz., teisės susipažinti ar skaidrumo principo, **apribojimus**;

- svarstys, ar į naująją bendrąją duomenų apsaugos sistemą būtina įtraukti **konkrečias ir suderintas nuostatas**, pavyzdžiui, dėl duomenų apsaugos tvarkant **genetinius duomenis** baudžiamosios teisės tikslais ar skiriant įvairias duomenų subjektų kategorijas (liudininkus, įtariamuosius ir t. t.) policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje;

- 2011 m. pradės **konsultacijas** su visomis susijusiomis suinteresuotosiomis šalimis apie tai, kaip geriausia **peržiūrėti dabartinę priežiūros sistemą policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje** ir užtikrinti veiksmingą ir nuoseklią duomenų apsaugos priežiūrą visose sąjungos institucijose, įstaigose, tarnybose ir agentūrose;

- įvertins, ar būtina ilgainiui **suderinti galiojančias įvairias šiam sektoriui skirtas taisykles, nustatytas konkrečiuose ES lygmeniu priimtuose dokumentuose policijos ir teisminiam bendradarbiavimui baudžiamosiose bylose reglamentuoti**, su nauja bendrąja duomenų apsaugos teisės sistema.

---

41 Šių priemonių apžvalga pateikta Komisijos komunikate „Informacijos valdymo laisvės, saugumo ir teisingumo erdvėje apžvalga“, COM (2010) 385.

42 Be Europos duomenų apsaugos priežiūros pareigūno (EDAPP), kuriam suteikti bendrieji Sąjungos institucijų, įstaigų, tarnybų ir agentūrų priežiūros įgaliojimai remiantis Reglamentu (EB) Nr. 45/2001, atitinkamais teisės aktais įsteigtos bendros priežiūros institucijos duomenų apsaugos priežiūrai užtikrinti.

2.4. Pasaulinė duomenų apsauga

2.4.1. Aiškiau išdėstyti ir supaprastinti tarptautinio duomenų perdavimo taisykles

Viena iš priemonių, kuria sudaromos galimybės perduoti asmens duomenis už ES ir EEE ribų, yra **tinkamumo vertinimas**. Šiuo metu trečiosios šalies tinkamumą, t. y. ar trečioji šalis užtikrina tokį apsaugos lygį, kurį ES laiko tinkamu, gali nustatyti Komisija ir valstybės narės.

Jei Komisija nustato, kad trečiosios šalies apsaugos lygis yra tinkamas, asmens duomenis galima laisvai perduoti iš 27 ES valstybių narių ir trijų EEE valstybių narių į tą šalį, nesiimant jokių papildomų apsaugos priemonių. Tačiau galiojančioje Duomenų apsaugos direktyvoje nepakankamai tiksliai išdėstyti konkretūs reikalavimai, kuriais vadovaudamasi Komisija pripažįsta apsaugos tinkamumą. Be to, pamatiniame sprendime toks Komisijos sprendimas nenumatytas.

Kai kuriose valstybėse narėse tinkamumą pirmiausia įvertina duomenų valdytojas, perduodantis duomenis į trečiąją šalį, kartais duomenų apsaugos priežiūros institucijai atliekant *ex post* priežiūrą. Todėl trečiųjų šalių ar tarptautinių organizacijų tinkamumo lygiui įvertinti gali būti taikomi skirtingi metodai, be to, **valstybės narės gali skirtingai vertinti trečiojoje šalyje užtikrinamą duomenų subjektų apsaugos lygį**. Galiojančiuose teisės dokumentuose nenustatyti tikslūs, suderinti reikalavimai, kurių laikantis perdavimą galima laikyti teisėtu. Todėl valstybių narių praktika skiriasi.

Be to, kalbant apie duomenų perdavimą į trečiąją šalį, neužtikrinančią tinkamo apsaugos lygio, dabartinės Komisijos nustatytos standartinės asmens duomenų perdavimo duomenų valdytojams[43] ir duomenų tvarkytojams[44] sąlygos nepritaikytos nesutartiniams atvejams ir, pavyzdžiui, jomis negali naudotis viena kitai duomenis perduodančios viešojo administravimo institucijos.

ES ar jos valstybių narių sudaromuose tarptautiniuose susitarimuose taip pat dažnai reikalaujama įtraukti duomenų apsaugos principus ir konkrečias nuostatas. Todėl susitarimų tekstai gali skirtis, nuostatos ir teisės gali būti išdėstytos nenuosekliai, taigi, jie gali būti aiškinami skirtingai, pažeidžiant duomenų subjekto interesus. Taigi, Komisija paskelbė nagrinėsianti teisėsaugos tikslais sudarytų Sąjungos ir trečiųjų šalių susitarimų pagrindines asmens duomenų apsaugos sudedamąsias dalis[45].

Kitos parengtos savireguliavimo priemonės, pavyzdžiui, įmonių vidaus elgesio kodeksai, žinomi kaip įmonėms privalomos taisyklės[46], taip pat gali būti naudingos įmonėms,

---

[43] 2001 m. birželio 15 d. Komisijos sprendimas 2001/497/EB dėl sutarčių, susijusių su asmens duomenų perdavimu trečiosioms šalims, tipinių punktų, atsižvelgiant į Direktyvą 95/46/EB (OL L 181, 2001 7 4, p. 19); 2001 m. gruodžio 27 d. Komisijos sprendimas 2002/16/EB dėl sutarčių standartinių sąlygų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Direktyvos 95/46/EB nuostatas (OL L 6, 2002 1 10, p. 52); 2004 m. gruodžio 27 d. Komisijos sprendimas 2004/915/EB, iš dalies keičiantis Sprendimą 2001/497/EB dėl sutarčių, susijusių su asmens duomenų perdavimu trečiosioms šalims, tipinių punktų (OL L 385, 2004 12 29, p. 74).

[44] 2010 m. vasario 5 d. Komisijos sprendimas dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas (OL L 39, 2010 2 12, p. 5).

[45] 36 išnašoje minėtas Stokholmo veiksmų planas.

[46] Įmonėms privalomos taisyklės – Europos duomenų apsaugos standartais grindžiami veiklos kodeksai, kuriuos tarptautinės organizacijos rengia ir kurių savanoriškai laikosi, kad užtikrintų tinkamas apsaugos priemones, taikomas įmonėms, priklausančioms tai pačiai įmonių grupei ir besilaikančioms šių

priklausančioms tai pačiai įmonių grupei, viena kitai teisėtai perduodant asmens duomenis. Tačiau suinteresuotosios šalys pastebėjo, kad būtų galima dar labiau pagerinti šį mechanizmą ir palengvinti jo įgyvendinimą.

Siekiant išspręsti iškeltus klausimus, **būtina iš esmės gerinti dabartinius tarptautinio asmens duomenų perdavimo mechanizmus** ir kartu užtikrinti, kad už ES ir EEE ribų perduodami ir tvarkomi asmens duomenys būtų tinkamai saugomi.

Komisija planuoja nagrinėti, kaip:

- **pagerinti ir supaprastinti galiojančias** tarptautinio duomenų perdavimo **procedūras**, įskaitant teisiškai privalomus dokumentus ir įmonėms privalomas taisykles, ir užtikrinti **vienodesnį ir darnesnį ES požiūrį** trečiųjų šalių ir organizacijų atžvilgiu;

- **aiškiau išdėstyti Komisijos tinkamumo procedūrą** ir nustatyti tikslesnius duomenų apsaugos lygio, užtikrinamo trečiojoje šalyje ar tarptautinėje organizacijoje, vertinimo **kriterijus ir reikalavimus**;

- nustatyti **pagrindines ES duomenų apsaugos sudedamąsias dalis**, kuriomis būtų galima naudotis sudarant bet kurio pobūdžio tarptautinius susitarimus.

2.4.2. Propaguoti universaliuosius principus

Duomenys tvarkomi pasauliniu mastu, todėl reikėtų nustatyti universaliuosius asmenų apsaugos tvarkant asmens duomenis principus.

ES duomenų apsaugos teisės sistema **trečiosioms šalims** dažnai buvo **duomenų apsaugos reguliavimo pavyzdys**. Jos įtaka ir poveikis Sąjungoje ir už jos ribų ypač svarbūs. Todėl **Europos Sąjunga turi toliau aktyviai skatinti tarptautinių teisės ir techninių asmens duomenų apsaugos standartų rengimą ir įgyvendinimą** remiantis atitinkamais ES ir kitais Europos duomenų apsaugos dokumentais. Tai ypač svarbu įgyvendinant ES plėtros politiką.

Kalbant apie standartizavimo organizacijų rengiamus tarptautinius techninius standartus, Komisija mano, kad labai svarbu suderinti būsimą teisės sistemą su tokiais standartais ir taip užtikrinti, kad duomenų valdytojai nuosekliai įgyvendintų duomenų apsaugos taisykles praktikoje.

įmonėms skirtų taisyklių, perduodant viena kitai asmens duomenis ar vykdant tam tikros rūšies asmens duomenų perdavimą. Žr. http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

Komisija:

- toliau **skatins rengti aukšto lygio teisės ir techninius duomenų apsaugos standartus** trečiosiose šalyse ir tarptautiniu lygmeniu;

- sieks įgyvendinti **apsaugos abipusiškumo principą** Sąjungos tarptautinėje veikloje, visų pirma duomenų subjektų, kurių duomenys perduodami iš ES į trečiąsias šalis, atžvilgiu;

- **stiprins bendradarbiavimą šiuo klausimu su trečiosiomis šalimis ir tarptautinėmis organizacijomis**, pvz., EBPO, Europos Taryba, Jungtinėmis Tautomis ir kitomis regioninėmis organizacijomis;

- **atidžiai stebės, kaip standartizavimo organizacijos**, pvz., Europos standartizacijos komitetas (CEN) ir Tarptautinė standartizacijos organizacija (ISO), **rengia tarptautinius techninius standartus**, ir užtikrins, kad jie būtų naudingi ir papildytų teisės taisykles ir kad pagrindiniai duomenų apsaugos reikalavimai būtų veiksmingai įgyvendinti.

2.5. Institucinių priemonių stiprinimas siekiant geriau įgyvendinti duomenų apsaugos taisykles

Siekiant užtikrinti asmenų teisių laikymąsi būtina įgyvendinti duomenų apsaugos principus ir taisykles ir jų laikytis.

Atsižvelgiant į tai, labai svarbus **vaidmuo** įgyvendinant duomenų apsaugos taisykles tenka **duomenų apsaugos institucijoms**. Šios institucijos – nepriklausomos pagrindinių su asmens duomenų apsauga susijusių teisių ir laisvių sergėtojos, patikimai užtikrinančios asmenims jų asmens duomenų apsaugą ir tvarkymo operacijų teisėtumą. Todėl Komisija mano, kad reikėtų sustiprinti jų vaidmenį, visų pirma atsižvelgiant į neseniai priimtą ETT sprendimą dėl jų nepriklausomumo[47], ir suteikti joms būtinus įgaliojimus ir išteklius, kad jos galėtų tinkamai vykdyti savo užduotis nacionaliniu lygmeniu ir bendradarbiaudamos tarpusavyje.

Komisija taip pat mano, kad **duomenų apsaugos institucijos turėtų glaudžiau bendradarbiauti ir geriau koordinuoti savo veiklą**, ypač spręsdamos tarpvalstybinio pobūdžio klausimus. Tai ypač svarbu tais atvejais, kai tarptautinės bendrovės yra įsikūrusios keliose valstybėse narėse ir vykdo veiklą kiekvienoje iš jų arba kai reikia koordinuoti priežiūrą su Europos duomenų apsaugos priežiūros pareigūnu (EDAPP)[48].

Šioje srityje **svarbus vaidmuo gali tekti 29 straipsnio darbo grupei**[49], kuriai, be patariamosios funkcijos[50], jau priskirta užduotis padėti vienodai taikyti ES duomenų apsaugos taisykles nacionaliniu lygmeniu. Nors duomenų apsaugos problemos visoje ES yra tokios pačios, duomenų apsaugos institucijos toliau skirtingai taiko ir aiškina ES taisykles, todėl reikia sustiprinti šios darbo grupės vaidmenį koordinuojant duomenų apsaugos institucijų pozicijas, užtikrinant vienodesnį nacionalinį taikymą ir vienodą duomenų apsaugos lygį.

---

47 2010 m. kovo 9 d. ETT Sprendimas *Komisija prieš Vokietiją*, C-518/07.

48 Šiuo metu tą reikia daryti didelių IT sistemų, pvz., antrosios kartos Šengeno informacinės sistemos SIS II (žr. Reglamento (EB) Nr. 1987/2006 46 straipsnį, OL L 318, 2006 12 28, p. 4) ir Vizų informacinės sistemos VIS (žr. Reglamento (EB) Nr. 767/2008 43 straipsnį, OL L 218, 2008 8 13, p. 60), atveju.

49 29 straipsnio darbo grupė – patariamoji grupė, į kurią po vieną atstovą siunčia valstybės narės, duomenų apsaugos institucijos, Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) ir Komisija (be balsavimo teisės), kuri taip pat teikia jai sekretoriato paslaugas. Žr. http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

50 29 straipsnio darbo grupė pataria Komisijai dėl apsaugos lygio ES bei trečiosiose šalyse ir bet kokių kitų su asmens duomenų tvarkymu susijusių priemonių.

Komisija nagrinės, kaip:

- naująja teisės sistema **sustiprinti, aiškiau išdėstyti ir suderinti nacionalinių duomenų apsaugos institucijų statusą ir įgaliojimus**, įskaitant visapusišką visiško nepriklausomumo sąvokos įgyvendinimą[51];

- **pagerinti duomenų apsaugos institucijų bendradarbiavimą ir koordinavimą**;

- užtikrinti nuoseklesnį ES duomenų apsaugos taisyklių taikymą vidaus rinkoje. Galimi veiksmai šioje srityje: **nacionalinių duomenų apsaugos priežiūros pareigūnų vaidmens stiprinimas, geresnis jų darbo koordinavimas per 29 straipsnio darbo grupę (kuri turėtų tapti skaidresne) ir (arba) nuoseklų taikymą vidaus rinkoje užtikrinančio mechanizmo sukūrimas vadovaujant Europos Komisijai**.

3. IŠVADA. TOLESNI VEIKSMAI

Asmens duomenų naudojimo ir keitimosi jais būdai, kaip ir technologijos, nuolat keičiasi. Teisės aktų leidėjų uždavinys – sukurti ilgalaikę teisės aktų sistemą. Europos duomenų apsaugos taisyklės, pasibaigus reformai, turėtų toliau užtikrinti aukšto lygio apsaugą ir teisinį tikrumą kelių kartų piliečiams, viešojo administravimo institucijoms ir įmonėms vidaus rinkoje. Kokia sudėtinga bebūtų padėtis ar technologija, taikytinos taisyklės ir standartai, kuriuos turi įgyvendinti nacionalinės institucijos ir kurių įmonės ir technologijų kūrėjai privalo laikytis, turi būti aiškios. Asmenys taip pat turėtų gerai žinoti savo teises.

Komisijos visapusiškas požiūris, kuriuo siekiama spręsti problemas ir siekti pagrindinių šiame komunikate išdėstytų tikslų, bus tolesnių diskusijų su kitomis Europos institucijomis ir suinteresuotosiomis šalimis, taip pat konkrečių pasiūlymų ir teisėkūros bei neteisėkūros priemonių pagrindas. Todėl Komisija laukia pastabų dėl šiame komunikate išdėstytų klausimų.

Pasibaigus poveikio vertinimui, Komisija, atsižvelgdama į šias pastabas ir ES pagrindinių teisių chartiją, **2011 m. siūlys teisės aktus**, kuriais peržiūrės duomenų apsaugos teisės sistemą ir taip sustiprins ES siekį saugoti asmens duomenis visose ES politikos, be kita ko, teisėsaugos ir nusikaltimų prevencijos, srityse, atsižvelgiant į šių sričių specifiką. Kartu bus įgyvendinamos ir neteisėkūros priemonės, pvz., siekiant skatinti savireguliavimą ir tirti galimybes įgyvendinti ES privatumo apsaugos ženklų sistemą.

Po to Komisija **vertins, ar reikia** su naująja bendrąja duomenų apsaugos sistema **suderinti kitas teisės priemones**. Pirmiausia, tai susiję su Reglamentu (EB) Nr. 45/2001, kurio nuostatas reikės suderinti su naująja bendrąja teisės sistema. Vėliau taip pat reikės nuodugniai ištirti poveikį kitoms konkretiems sektoriams skirtoms priemonėms.

[51] Žr. 2010 m. kovo 9 d. ETT Sprendimą *Komisija prieš Vokietiją*, C-518/07.

Be to, Komisija, **vykdydama aktyvią pažeidimų nagrinėjimo politiką** tais atvejais, kai ES duomenų apsaugos taisyklės neteisingai įgyvendinamos ir taikomos, toliau užtikrins, kad teisingas Sąjungos teisės įgyvendinimas šioje srityje būtų tinkamai stebimas. Ši duomenų apsaugos priemonių peržiūra nedaro poveikio valstybių narių prievolei įgyvendinti galiojančias asmens duomenų apsaugos teisės priemones ir užtikrinti tinkamą jų taikymą[52].

Geriausias ES duomenų apsaugos standartų rėmimo ir skatinimo visame pasaulyje būdas – užtikrinti aukšto lygio vienodą duomenų apsaugą ES.

[52] Įskaitant Tarybos pamatinį sprendimą 2008/977/TVR; valstybės narės iki 2010 m. lapkričio 27 d. turi imtis reikiamų priemonių, kuriomis įgyvendinamos šio pamatinio sprendimo nuostatos.