



**Teisės į duomenų perkeliamumą gairės**

**Priimta 2016 m. gruodžio 13 d.  
Priimta su paskutiniais pakeitimais 2017 m. balandžio 5 d.**

Ši darbo grupė sudaryta pagal Direktyvos 95/46/EB 29 straipsnį. Ji yra nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais. Jos uždaviniai aprašyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje.

Sekretoriato paslaugas teikia Europos Komisijos Teisingumo ir vartotojų reikalų generalinio direktorato C direktoratas (Pagrindinės teisės ir teisinė valstybė), B-1049 Brussels, Belgium, Office No MO59 05/35.

Svetainė: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

## **TURINYS**

<b>Santrauka.....</b>	<b>3</b>
<b>I. Įvadas .....</b>	<b>3</b>
<b>II. Kokie yra pagrindiniai duomenų perkeliavimo elementai? .....</b>	<b>4</b>
<b>III. Kada galioja teisė į duomenų perkeliavimą? .....</b>	<b>9</b>
<b>IV. Kaip bendrosios naudojimosi duomenų subjekto teisėmis taisyklės taikomos duomenų perkeliavimui? .....</b>	<b>14</b>
<b>V. Kaip turi būti suteikiami perkeliami duomenys? .....</b>	<b>17</b>

## **Santrauka**

Bendrojo duomenų apsaugos reglamento 20 straipsniu sukuriamą naują teisę į duomenų perkeliamumą, kuri yra glaudžiai susijusi su teise susipažinti su duomenimis, tačiau nuo jos daugeliu atžvilgių skiriasi. Šia teise duomenų subjektams suteikiama galimybė gauti asmens duomenis, kuriuos jie pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir persiųsti tuos duomenis kitam duomenų valdytojui. Šios naujos teisės paskirtis – suteikti duomenų subjektui daugiau galių ir daugiau galimybių kontroliuoti su juo susijusius asmens duomenis.

Kadangi teise į duomenų perkeliamumą suteikiama galimybė tiesiogiai perduoti asmens duomenis iš vieno duomenų valdytojo kitam, teisė į duomenų perkeliamumą taip pat yra svarbi priemonė, padėsianti skatinti laisvą asmens duomenų srautą Europos Sąjungoje ir duomenų valdytojų konkurenciją. Ji padės pereiti nuo vieno paslaugų teikėjo prie kito ir taip skatins naujų paslaugų kūrimą, kaip numatyta bendrosios skaitmeninės rinkos strategijoje.

Šia nuomone pateikiamos gairės, kaip aiškinti ir įgyvendinti Bendrajame duomenų apsaugos reglamente nustatytą teisę į duomenų perkeliamumą. Ja siekiama aptarti teisę į duomenų perkeliamumą ir jos taikymo sritį. Šia nuomone paaiškinamos sąlygos, kuriomis taikoma ši nauja teisė, atsižvelgiant į teisinį duomenų tvarkymo pagrindą (duomenų subjekto sutikimą arba būtinybę įvykdyti sutartį) ir į tai, kad ši teisė taikoma tik duomenų subjekto pateiktiems asmens duomenims. Nuomonėje taip pat pateikiama konkrečių pavyzdžių ir kriterijų aplinkybėms, kuriomis taikoma ši teisė, paaiškinti. Šiuo klausimu WP29 mano, kad teisė į duomenų perkeliamumą apima duomenų subjekto sąmoningai pateiktus duomenis ir jam vykdant veiklą gautus asmens duomenis. Šios naujos teisės negalima sumenkinti ir jos taikyti tik asmeninei informacijai, kurią duomenų subjektas tiesiogiai pateikia, pavyzdžiui, per internetinę formą.

Remdamiesi gerąja patirtimi, duomenų valdytojai turėtų pradėti rengti priemones, padėsiančias atsakyti į prašymus perkelti duomenis, pvz., atsisieuntimo priemones ir programų sąsajas. Jie turėtų garantuoti, kad asmens duomenys būtų perduodami susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, nes jie turėtų būti skatinami užtikrinti formato, kuriuo duomenys teikiami tenkinant prašymą perkelti duomenis, sąveikumą.

Šia nuomone duomenų valdytojams taip pat padedama aiškiai suprasti atitinkamas savo prievoles ir rekomenduojami geriausios patirties metodai ir priemonės, padedantys įgyvendinti teisę į duomenų perkeliamumą. Galiausiai nuomonėje suinteresuotiesiems pramonės subjektams ir verslo asociacijoms rekomenduojama bendradarbiaujant tarpusavyje parengti bendrą sąveikių standartų ir formatų rinkinį, kad būtų galima įvykdyti teisės į duomenų perkeliamumą reikalavimus.

## **I. Įvadas**

Bendrojo duomenų apsaugos reglamento 20 straipsnyje nustatoma nauja teisė į duomenų perkeliamumą. Šia teise duomenų subjektams suteikiama galimybė be kliūčių gauti asmens duomenis, kuriuos jie pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir persiųsti tuos duomenis kitam duomenų valdytojui. Ši tam

tikromis sąlygomis taikoma teisė padeda didinti vartotojų pasirinkimą, vartotojų kontrolę ir suteikti jiems daugiau galių.

Asmenų, kurie naudojosi savo teise susipažinti su duomenimis pagal Duomenų apsaugos direktyvą 95/46/EB, galimybes riboja duomenų valdytojo pasirinktas formatas prašomai informacijai teikti. **Naująja teise į duomenų perkeliamumą siekiama suteikti duomenų subjektams galių savo asmens duomenų atžvilgiu, nes šia teise pagerinama jų galimybė lengvai perkelti, nusikopijuoti ar perduoti asmens duomenis iš vienos IT aplinkos į kitą (ar tai būtų jų pačių sistemos, trečiųjų šalių, kuriomis jie pasitiki, sistemos, ar naujų duomenų valdytojų sistemos).**

Duomenų perkeliamumu ne tik sustiprinamos asmeninės asmenų teisės ir galimybė kontroliuoti su jais susijusius asmens duomenis, tačiau ir suteikiama galimybė *perbalansuoti* duomenų subjektų ir duomenų valdytojų santykį<sup>1</sup>.

Nors teisė į asmens duomenų perkeliamumą gali sustiprinti ir paslaugų tarpusavio konkurenciją (nes padeda pereiti nuo vienos paslaugos prie kitos), Bendrojo duomenų apsaugos reglamentu reglamentuojami asmens duomenys, o ne konkurencija. Konkrečiai pagal 20 straipsnį perkeliama ne tik perėjimui nuo vienos paslaugos prie kitos būtini ar naudingi duomenys<sup>2</sup>.

Nors duomenų perkeliamumas yra nauja teisė, kitų rūšių perkeliamumas jau yra arba aptariamas kitų sričių teisės aktuose (pvz., sutarčių nutraukimo, tarptinklinio ryšio paslaugų ir tarpvalstybinio paslaugų prieinamumo srityse<sup>3</sup>). Iš įvairių rūšių perkeliamumo asmenys gali gauti tam tikros sinergijos ir netgi naudos, jeigu šis perkeliamumas bus įgyvendinamas suderintu metodu, nors analogijas reikėtų vertinti atsargiai.

Šioje nuomonėje pateikiamos gairės duomenų valdytojams, kad jie galėtų atnaujinti savo metodus, procesus ir politikos priemones, ir aiškiai išdėstoma duomenų perkeliamumo prasmė, kad duomenų subjektai įgytų galimybę veiksmingai naudotis nauja savo teise.

## **II. Kokie yra pagrindiniai duomenų perkeliamumo elementai?**

Bendrojo duomenų apsaugos reglamento 20 straipsnio 1 dalyje teisė į duomenų perkeliamumą apibrėžiama taip:

*Duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui, o duomenų valdytojas, kuriam asmens duomenys buvo pateikti, turi nesudaryti tam kliūčių [...].*

---

<sup>1</sup> Pagrindinis duomenų perkeliamumo tikslas – sustiprinti asmens galimybes kontroliuoti savo asmens duomenis ir užtikrinti, kad jie atliktų aktyvų vaidmenį duomenų ekosistemoje.

<sup>2</sup> Pavyzdžiui, šia teise bankams gali būti suteikta galimybė kontroliuojant vartotojui teikti papildomas paslaugas, naudojant asmens duomenis, iš pradžių surinktus teikiant energijos tiekimo paslaugas.

<sup>3</sup> Žr. Europos Komisijos bendrosios skaitmeninės rinkos darbotvarkę: <https://ec.europa.eu/digital-agenda/en/digital-single-market>, ypač pirmąjį politikos ramstį *Geresnė internetinė prieiga prie prekių ir paslaugų*.

## - Teisė gauti asmens duomenis

Pirmiausia, duomenų perkeliamumas yra **duomenų subjekto teisė gauti** duomenų valdytojo tvarkomų su duomenų subjektu susijusių **asmens duomenų poaibį** ir saugoti šiuos duomenis tolesniam asmeniniam naudojimui. Duomenys gali būti tokiu būdu saugomi privačiame įrenginyje arba privačioje debesioje, nebūtinai persiunčiant juos kitam duomenų valdytojui.

Šiuo aspektu duomenų perkeliamumas papildo teisę susipažinti su duomenimis. Vienas iš specifinių duomenų perkeliamumo aspektų – ši teisė yra lengvas būdas duomenų subjektams patiems valdyti ir pakartotinai naudoti savo duomenis. Šie duomenys turėtų būti perduodami *susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu*. Pavyzdžiui, duomenų subjektas gali pageidauti atsisiųsti savo dabartinį kūrinių sąrašą (arba klausytų kūrinių istoriją) iš srautinio muzikos siuntimo paslaugos, siekdamas išsiaiškinti, kiek kartų jis klausėsi konkrečių kūrinių, arba patikrinti, kokios muzikos jis nori įsigyti ar klausyti kitoje platformoje. Panašiai jis gali norėti atsisiųsti savo adresatų sąrašą iš saityno pašto programos, pavyzdžiui, siekdamas sudaryti vestuvių svečių sąrašą, arba atsisiųsti informaciją apie pirkinius naudojant įvairias lojalumo korteles, arba pasitikrinti savo anglies pėdsaką<sup>4</sup>.

## - Teisė persiųsti asmens duomenis iš vieno duomenų valdytojo kitam duomenų valdytojui

Antra, 20 straipsnio 1 dalyje duomenų subjektams numatyta teisė *be kliūčių persiųsti asmens duomenis iš vieno duomenų valdytojo kitam duomenų valdytojui*. Duomenų subjekto prašymu duomenis vienas duomenų valdytojas taip pat gali tiesiogiai persiųsti kitam, kai tai techniškai įmanoma (20 straipsnio 2 dalis). Šiuo klausimu 68 konstatuojamojoje dalyje duomenų valdytojai raginami kurti sąveikius formatus, kad būtų užtikrinamas duomenų perkeliamumas<sup>5</sup>, tačiau nesukuriant duomenų valdytojams prievolės nustatyti ar išlaikyti duomenų tvarkymo sistemas, kurios yra techniškai suderinamos<sup>6</sup>. Vis dėlto Bendruoju duomenų apsaugos reglamentu duomenų valdytojams draudžiama kurti duomenų persiuntimo kliūtis.

Iš esmės šiuo duomenų perkeliamumo elementu duomenų subjektams suteikiama galimybė ne tik gauti ir pakartotinai naudoti, bet ir persiųsti pateiktus duomenis kitam paslaugų teikėjui (arba tame pačiame, arba kitame verslo sektoriuje). Teisė į duomenų perkeliamumą tikimasi užkertant kelią duomenų susaistymui ne tik suteikti vartotojams daugiau galių, bet ir skatinti galimybes kurti inovacijas ir saugiai keistis asmens duomenimis tarp duomenų valdytojų, tai kontroliuojant duomenų subjektui<sup>7</sup>. Duomenų perkeliamumas gali skatinti kontroliuojamą ir ribotą vartotojų praktiką keistis asmens duomenimis tarp organizacijų ir taip pagerinti

<sup>4</sup> Šiais atvejais duomenų subjekto vykdomas duomenų tvarkymas gali patekti į namų ūkio veiklos sritį, kai visi duomenys tvarkomi kontroliuojant tik duomenų subjektui, arba duomenų subjekto vardu duomenis gali tvarkyti kita šalis. Pastaruoju atveju ta kita šalis turėtų būti laikoma duomenų valdytoju, netgi vien asmens duomenų saugojimo tikslu, ir turi laikytis Bendrajame duomenų apsaugos reglamente nustatytų principų ir įpareigojimų.

<sup>5</sup> Taip pat žr. V skirsnį.

<sup>6</sup> Atitinkamai ypatingą dėmesį reikėtų atkreipti į persiunčiamų duomenų formatą siekiant užtikrinti, kad duomenų subjektas arba kitas duomenų valdytojas duomenis galėtų be didelių pastangų panaudoti pakartotinai. Taip pat žr. V skirsnį.

<sup>7</sup> Žr. keletą eksperimentinių programų Europoje, pavyzdžiui [MiData](#) Jungtinėje Karalystėje, taip pat organizacijos FING vykdomą [MesInfos / SelfData](#) Prancūzijoje.

paslaugų kokybę ir vartotojų patirtį<sup>8</sup>. Duomenų perkeliamumas gali padėti persiųsti ir pakartotinai naudoti su vartotojais susijusius asmens duomenis tarp įvairių paslaugų, kuriomis jie domisi.

---

<sup>8</sup> Vadinamosios kiekybiškai išreikšto asmens (angl. *quantified self*) ir daiktų interneto (angl. *IoT*) pramonės sritys parodė, kaip naudinga (ir kaip rizikinga) susieti įvairių asmens gyvenimo aspektų, pvz., fizinės formos, veiklos ir kalorijų suvartojimo, asmens duomenis siekiant vienoje bendroje rinkmenoje gauti išsamesnį vaizdą apie asmens gyvenimą.

## - Kontrolė

Duomenų perkeliamumas garantuoja teisę gauti asmens duomenis ir juos tvarkyti pagal duomenų subjekto pageidavimus<sup>9</sup>.

Duomenų valdytojai, atsakantys į prašymą perkelti duomenis 20 straipsnyje nustatytais sąlygomis, nėra atsakingi už duomenų subjekto ar kitos asmens duomenis gaunančios įmonės atliekamą duomenų tvarkymą. Jie veikia duomenų subjekto vardu, net ir tada, kai asmens duomenys tiesiogiai persiunčiami kitam duomenų valdytojui. Šiuo aspektu duomenų valdytojas nėra atsakingas už duomenis gaunančio duomenų valdytojo pastangas laikytis duomenų apsaugos teisės, nes gavėją pasirenka ne duomenis siunčiantis duomenų valdytojas. Kartu duomenų valdytojas turėtų nustatyti apsaugos priemones, kuriomis būtų užtikrinta, kad jis tikrai veiktų duomenų subjekto vardu. Pavyzdžiui, duomenų valdytojai gali nustatyti procedūras, kuriomis užtikrinama, kad persiunčiami asmens duomenys tikrai yra tokio tipo, kokius duomenų subjektas nori persiųsti. Tai būtų galima padaryti gaunant duomenų subjekto patvirtinimą arba iki duomenų persiuntimo, arba anksčiau, kai duodamas pradinis sutikimas tvarkyti duomenis arba baigiama sudaryti sutartį.

Duomenų valdytojai, atsakantys į prašymus perkelti duomenis, nėra konkrečiai įpareigoti prieš persiųsdami duomenis patikrinti duomenų kokybę ir ją įsitikinti. Žinoma, šie duomenys jau iš anksto turėtų būti tikslūs ir atnaujinti laikantis Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalyje nurodytų principų. Be to, duomenų perkeliamumu duomenų valdytojas neįpareigojamas saugoti asmens duomenų ilgiau negu reikalinga arba ilgiau negu nurodytą duomenų saugojimo laikotarpį<sup>10</sup>. Svarbu, kad nėra papildomo reikalavimo saugoti duomenis ilgiau negu trunka taikytini duomenų saugojimo laikotarpiai, vien todėl, kad būtų galima patenkinti galimą būsimą prašymą perkelti duomenis.

Kai prašomus asmens duomenis tvarko duomenų tvarkytojas, pagal Bendrojo duomenų apsaugos reglamento 28 straipsnį sudarytoje sutartyje turi būti nurodyta prievolė padėti *duomenų valdytojui taikant tinkamas technines ir organizacines priemones [...] atsakyti į prašymus pasinaudoti duomenų subjekto teisėmis*. Taigi, duomenų valdytojas, bendradarbiaudamas su savo duomenų tvarkytojais, turėtų įdiegti specialias procedūras. Kai duomenis bendrai valdo keli duomenų valdytojai, sutartyje turėtų būti aiškiai paskirstyta kiekvieno duomenų valdytojo atsakomybė už prašymų perkelti duomenis nagrinėjimą.

Be to, duomenis gaunantis duomenų valdytojas<sup>11</sup> privalo užtikrinti, kad suteikti perkeliama duomenys būtų aktualūs ir jų nebūtų per daug, palyginti su tuo, kas reikalinga naujam duomenų tvarkymui. Pavyzdžiui, jeigu prašymas perkelti duomenis teikiamas saityno pašto tarnybai, o prašymą duomenų subjektas teikia siekdamas gauti e. pašto laiškus ir juos nusiųsti į apsaugotą archyvavimo platformą, naujasis duomenų valdytojas neprivalo tvarkyti duomenų subjekto korespondencijos partnerių kontaktinių duomenų. Jeigu ši informacija nėra aktuali naujo duomenų tvarkymo tikslu, jis neturėtų būti laikoma ir tvarkoma. Bet kuriuo atveju duomenis gaunantys duomenų valdytojai neprivalo priimti ir tvarkyti asmens duomenų, persiunčiamų pagal prašymą perkelti duomenis. Panašiai, kai duomenų subjektas prašo

<sup>9</sup> Teisė į duomenų perkeliamumą taikoma ne tik asmens duomenims, kurie naudingi ir aktualūs siekiant gauti duomenų valdytojo konkurentų teikiamas panašias paslaugas.

<sup>10</sup> Pagal minėtąjį pavyzdį, jeigu duomenų valdytojas nesaugo vartotojo leidžiamų kūrinių sąrašo, tada šių asmens duomenų negalima nurodyti prašyme perkelti duomenis.

<sup>11</sup> t. y., tas, kuris gauna asmens duomenis pagal prašymą perkelti duomenis, kurį duomenų subjektas pateikia kitam duomenų valdytojui.

perduoti savo banko operacijų duomenis tarnybai, padedančiai tvarkyti jo biudžetą, duomenis gaunantis duomenų valdytojas neprivalo priimti visų duomenų ar išsaugoti visų operacijų duomenų, kai jie suklasifikuojami naujosios tarnybos tikslais. Kitaip tariant, priimami ir išsaugomi duomenys turėtų būti tik tie, kurie yra reikalingi ir aktualūs duomenis gaunančio duomenų valdytojo paslaugai teikti.

*Duomenis gaunanti* organizacija tampa nauju šių asmens duomenų valdytoju ir turi laikytis Bendrojo duomenų apsaugos reglamento 5 straipsnyje nurodytų principų. Taigi, duomenis gaunantis *naujasis* duomenų valdytojas, vadovaudamasis 14 straipsnyje išdėstytais skaidrumo reikalavimais<sup>12</sup>, turi aiškiai ir tiesiogiai nurodyti naujo duomenų tvarkymo tikslą prieš teikdamas bet kokią prašymą persiusti perkeliamus duomenis. Kaip ir tvarkydamas kitus jo atsakomybei priklausančius duomenis, duomenų valdytojas turėtų taikyti 5 straipsnyje nustatytus principus, pvz., teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, vientisumo ir konfidencialumo, saugojimo trukmės apribojimo ir atskaitomybės principus<sup>13</sup>.

Asmens duomenis saugantys duomenų valdytojai turėtų būti pasirengę padėti savo duomenų subjektui pasinaudoti teise į duomenų perkeliamumą. Duomenų valdytojai taip pat gali nuspręsti priimti duomenis iš duomenų subjekto, bet neprivalo to daryti.

#### - Duomenų perkeliamumo santykis su kitomis duomenų subjektų teisėmis

**Savo teise į duomenų perkeliamumą asmuo naudojasi nedarydamas poveikio jokiai kitai teisei (tai galioja ir bet kurioms kitoms Bendrajame duomenų apsaugos reglamente numatytiems teisėms).** Duomenų subjektas gali ir toliau naudotis duomenų valdytojo paslauga ir pasinaudoti jos teikiamais pranašumais net ir po duomenų perkėlimo operacijos. Duomenų perkeliamumas pats savaime nesukelia pareigos ištrinti duomenis<sup>14</sup> iš duomenų valdytojo sistemų ir neturi poveikio pradiniam persiūtų duomenų saugojimo laikotarpiui. Duomenų subjektas gali naudotis savo teisėmis, kol duomenų valdytojas dar tvarko duomenis.

Taip pat, jeigu duomenų subjektas pageidauja pasinaudoti savo teise ištrinti savo asmens duomenis (teise būti pamirštam pagal 17 straipsnį), dėl pasinaudojimo teise į duomenų perkeliamumą duomenų valdytojas negali vilkinti tokio ištrynimo ar atsisakyti jį atlikti.

Jeigu duomenų subjektas nustatytų, kad naudojantis teise į duomenų perkeliamumą prašomi asmens duomenys neatitinka jo prašymo, turėtų būti visapusiškai vykdomas papildomas prašymas susipažinti su asmens duomenimis pagal Bendrojo duomenų apsaugos reglamento 15 straipsnį.

Be to, kai specialiuosiuose kitų sričių ES arba valstybės narės teisės aktuose taip pat numatytas tam tikros formos atitinkamų duomenų perkeliamumas, tenkinant prašymą perkelti duomenis pagal Bendrąjį duomenų apsaugos reglamentą taip pat turi būti atsižvelgiama į

<sup>12</sup> Be to, naujasis duomenų valdytojas neturėtų tvarkyti asmens duomenų, kurie nėra aktualūs, o turėtų būti tvarkomi tik naujais tikslais reikalingi duomenys, net jeigu asmens duomenys sudaro platesnį duomenų rinkinį, persiunčiamą duomenų perkeliavimo proceso pagrindu. Asmens duomenys, nereikalingi naujo duomenų tvarkymo tikslui pasiekti, turėtų būti kuo greičiau ištrinami.

<sup>13</sup> Kai duomenų valdytojas gauna asmens duomenis, jam persiūtus įgyvendinant teisę į duomenų perkeliamumą, duomenis galima laikyti pateiktais duomenų subjekto ir šie duomenys gali būti toliau persiunčiami įgyvendinant teisę į duomenų perkeliamumą, jeigu įvykdomos kitos šiai teisei taikomos sąlygos (t. y. duomenų tvarkymo teisinis pagrindas, ...).

<sup>14</sup> kaip nurodyta Bendrojo duomenų apsaugos reglamento 17 straipsnyje.



šiuose specialiuosiuose teisės aktuose nustatytas sąlygas. Pirma, jeigu iš duomenų subjekto pateikto prašymo aišku, kad jis ketina naudotis teisėmis ne pagal Bendrąjį duomenų apsaugos reglamentą, o tik pagal sektorinius teisės aktus, tada šiam prašymui nebus taikomos Bendrojo duomenų apsaugos reglamento nuostatos dėl duomenų perkeliamumo<sup>15</sup>. Tačiau jeigu prašymu siekiama perkelti duomenis pagal Bendrąjį duomenų apsaugos reglamentą, tokių specialiųjų teisės aktų buvimas nėra viršesnis už bendrą duomenų perkeliamumo principo taikymą bet kuriam duomenų valdytojui, kaip numatyta Bendrajame duomenų apsaugos reglamente. Vietoj to kiekvienu konkrečiu atveju turi būti įvertinama, kokį poveikį tokie specialieji teisės aktai gali turėti teisei į duomenų perkeliamumą, jeigu toks poveikis apskritai galimas.

### **III. Kada galioja teisė į duomenų perkeliamumą?**

- **Kokioms duomenų tvarkymo operacijoms taikoma teisė į duomenų perkeliamumą?**

Siekdami įvykdyti Bendrojo duomenų apsaugos reglamento reikalavimus, duomenų valdytojai privalo turėti aiškų asmens duomenų tvarkymo teisinį pagrindą.

Kaip numatyta Bendrojo duomenų apsaugos reglamento 20 straipsnio 1 dalies a punkte, duomenų tvarkymo operacijoms gali būti taikoma teisė į duomenų perkeliamumą, jeigu šios operacijos yra grindžiamos:

- duomenų subjekto sutikimu pagal 6 straipsnio 1 dalies a punktą arba 9 straipsnio 2 dalies a punktą, kai kalbama apie specialių kategorijų asmens duomenis);
- arba sutartimi, kurios šalis yra duomenų subjektas, pagal 6 straipsnio 1 dalies b punktą.

Pavyzdžiui, iš internetinio knygyno asmens įsigytų knygų pavadinimai arba naudojantis srautinio muzikos siuntimo paslauga klausomos dainos yra asmens duomenų, kuriems paprastai taikomas duomenų perkeliamumas, pavyzdžiai, nes šie duomenys tvarkomi pagal duomenų subjekto sudarytą sutartį.

Bendrajame duomenų apsaugos reglamente nenustatyta bendra teisė į duomenų perkeliamumą tais atvejais, kai asmens duomenų tvarkymas nėra grindžiamas sutikimu arba sutartimi<sup>16</sup>.

---

<sup>15</sup> Pavyzdžiui, jeigu duomenų subjekto prašymu konkrečiai siekiama suteikti galimybę informacijos apie sąskaitą paslaugų teikėjui susipažinti su duomenų subjekto banko sąskaitos istorija, antroje Mokėjimo paslaugų direktyvoje nurodytais tikslais tokia galimybė susipažinti su duomenimis turėtų būti suteikta pagal šios direktyvos nuostatas.

<sup>16</sup> Žr. Bendrojo duomenų apsaugos reglamento 68 konstatuojamąją dalį ir 20 straipsnio 2 dalį. 20 straipsnio 3 dalyje ir 68 konstatuojamojoje dalyje numatyta, kad duomenų perkeliamumas netaikomas, kai tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdomą duomenų valdytojui pavestas viešosios valdžios funkcijas, arba tada, kai duomenų valdytojas vykdo savo viešąsias pareigas arba teisinę prievolę. Todėl duomenų valdytojai neprivalo šiais atvejais sudaryti sąlygas perkelti duomenis. Tačiau, vadovaujantis principais, kuriais grindžiama teisė į duomenų perkeliamumą, geroji patirtis būtų sukurti procesus, kuriuos vykdomi būtų automatiškai atsakoma į prašymus perkelti duomenis. Tokio proceso pavyzdys būtų valdžios paslauga, suteikianti galimybę lengvai atsisiųsti praecityje pateiktas asmens pajamų mokesčio deklaracijas. Duomenų perkeliamumas kaip geroji patirtis, kai duomenys tvarkomi būtinais teisiniais pagrindais, siekiant teisėto intereso, ir galiojančios savanoriškos sistemos aptariamai WP29 nuomonės 6/2014 dėl teisėtų interesų 47–48 psl.

Pavyzdžiui, finansų įstaigos neprivalo atsakyti į prašymą perkelti asmens duomenis, tvarkomus vykdant jų prievoles užkirsti kelią pinigų plovimui bei kitiems finansiniams nusikaltimams ir juos aptikti; taip pat duomenų perkeliamumas netaikomas profesiniams kontaktiniams duomenims, tvarkomiems verslo subjektų tarpusavio santykių pagrindu, kai duomenų tvarkymas nėra grindžiamas nei duomenų subjekto sutikimu, nei jo sudaryta sutartimi.

Teisė į darbuotojų duomenų perkeliamumą paprastai taikoma tik tuo atveju, jei duomenys tvarkomi pagal sutartį, kurios viena iš šalių yra duomenų subjektas. Daugeliu atvejų šiomis aplinkybėmis sutikimas nebus laikomas laisvai duotu, nes darbdavio ir darbuotojo galios nėra vienodos<sup>17</sup>. Kai kurie žmogiškųjų išteklių duomenų tvarkymo atvejai grindžiami teisėtu interesu kaip teisiniu pagrindu arba yra reikalingi konkrečioms teisinėms prievolėms įdarbinimo srityje įvykdyti. Praktiškai teisė į duomenų perkeliamumą žmogiškųjų išteklių srityje neabejotinai bus susijusi su kai kuriomis duomenų tvarkymo operacijomis (pvz., darbo užmokesčio ir kompensacijų mokėjimo paslaugomis, vidaus samda), tačiau daugelį kitų atvejų reikės kiekvieną kartą vertinti atskirai, kad būtų galima patikrinti, ar įvykdytos visos teisės į duomenų perkeliamumą sąlygos.

Galiausiai teisė į duomenų perkeliamumą taikoma tik tuo atveju, jei *duomenys tvarkomi automatizuotomis priemonėmis*, todėl neapima didžiosios dalies popierinių bylų.

#### **- Kokiems asmens duomenims turi būti taikomas perkeliamumas?**

Pagal 20 straipsnio 1 dalį teisė į duomenų perkeliamumą taikoma, jeigu atitinkami duomenys yra:

- su duomenų subjektu susiję asmens duomenys,
- kuriuos duomenų subjektas *pateikė* duomenų valdytojui.

20 straipsnio 4 dalyje taip pat nurodyta, kad šios teisės įgyvendinimas neturi daryti neigiamo poveikio kitų asmenų teisėms ir laisvėms.

#### Pirmoji sąlyga: asmens duomenys yra susiję su duomenų subjektu

Prašyme perkelti duomenis gali būti nurodyti tik asmens duomenys. Todėl bet kurie anoniminiai<sup>18</sup> arba su duomenų subjektu nesusiję duomenys nebus prašymo objektas. Tačiau pseudoniminius duomenis, kuriuos galima aiškiai susieti su duomenų subjektu (pvz., jam pateikus atitinkamą identifikatorių, plg. su 11 straipsnio 2 dalimi), prašyme nurodyti galima.

Daugeliu aplinkybių duomenų valdytojai tvarko informaciją, apimančią keleto duomenų subjektų asmens duomenis. Tokiu atveju duomenų valdytojai neturėtų vadovautis pernelyg siauru frazės *su duomenų subjektu susiję asmens duomenys* aiškinimu. Pavyzdžiui, telefono pokalbių, asmeninių žinučių ar interneto telefonijos išsklotinėse (abonento paskyros istorijoje) gali būti nurodyti trečiųjų šalių, dalyvavusių priimamuose ir siunčiamuose skambučiuose, duomenys. Nors dėl šios priežasties išsklotinėse bus daugelio žmonių asmens duomenų, abonentams turėtų būti suteikta galimybė gauti šiuos duomenis pagal prašymus perkelti duomenis, nes išsklotinės yra susijusios (ir) su duomenų subjektu. Vis dėlto kai tokios išsklotinės persiunčiamos naujam duomenų valdytojui, šis naujas duomenų valdytojas neturėtų

<sup>17</sup> Kaip WP29 bendrais bruožais išdėstė savo 2001 m. rugsėjo 13 d. nuomonėje 8/2001 (WP48).

<sup>18</sup> [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_lt.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf)

jų tvarkyti jokių tikslų, kuris turėtų neigiamą poveikį trečiųjų šalių teisėms ir laisvėms (toliau žr.: trečioji sąlyga).

#### Antroji sąlyga: duomenų subjekto pateikti duomenys

Antrąją sąlygą taikymo sritis susiaurinama iki duomenų subjekto *pateiktų* duomenų.

Esama daugelio pavyzdžių, kai asmens duomenis sąmoningai ir aktyviai *teikia* duomenų subjektas, pvz., jis per internetines formas nurodo paskyros duomenis (pvz., pašto adresą, vartotojo vardą, amžių). Nepaisant to, duomenų subjekto *pateikti* duomenys gaunami ir stebint jo veiklą. Taigi, WP29 mano, kad siekiant visapusiškai įtvirtinti šią naują teisę, pateikti duomenys taip pat turėtų apimti asmens duomenis, kurie yra pastebimi iš vartotojų veiklos, pvz., neapdoroti išmaniojo skaitiklio ar kitų tipų sujungtųjų objektų duomenys<sup>19</sup>, veiklos žurnalai, svetainių lankymo ar paieškos veiksmų istorija.

Pastaroji duomenų kategorija neapima duomenų, kuriuos (naudodamas pastebėtus arba tiesiogiai kaip informaciją pateiktus duomenis) sukuria duomenų valdytojas, pvz., vartotojo profilio, sukurto analizuojant renkamus išmaniojo skaitiklio duomenis.

Siekiant nustatyti, ar teisė į duomenų perkeliamumą taikoma konkrečioms duomenims, juos galima skirstyti į įvairias kategorijas, priklausomai nuo jų kilmės. Toliau nurodytų kategorijų duomenys gali būti laikomi *pateiktais duomenų subjekto*:

- **duomenų subjekto aktyviai ir sąmoningai pateikti duomenys** (pavyzdžiui, pašto adresas, vartotojo vardas, amžius ir kt.);
- **duomenų subjekto pateikti duomenys, nustatyti stebėjimo būdu pagal naudojimąsi paslauga arba įrenginiu.** Tai, pavyzdžiui, gali būti asmens paieškos istorija, srauto duomenys ir duomenys apie vietovę. Tai gali būti ir kiti neapdoroti duomenys, pvz., nešiojamo įrenginio sekamas pulsas.

Tuo tarpu netiesiogiai nustatomi ir išvedami duomenis sukuria duomenų valdytojas, remdamasis *duomenų subjekto pateiktais* duomenimis. Pavyzdžiui, vartotojo sveikatos arba rizikos valdymo ir finansų reglamentavimo (pvz., siekiant nustatyti kreditingumą arba įvykdyti kovos su pinigų plovimu taisyklės) nuostatų pagrindu sukurto profilio vertinimo rezultatai patys savaime negali būti laikomi *pateiktais* duomenų subjekto. Nors tokie duomenys gali būti duomenų valdytojo saugomo profilio dalis ir yra netiesiogiai nustatomi ar išvedami duomenų subjekto pateiktų duomenų (pavyzdžiui, jo veiksmų) analizės būdu, šie duomenys paprastai nebus laikomi *pateiktais duomenų subjekto*, taigi, jų atžvilgiu ši nauja teisė nebus taikoma<sup>20</sup>.

<sup>19</sup> Galėdamas atsisiųsti duomenis, gautus stebint jo veiklą, duomenų subjektas taip pat galės susidaryti aiškesnę vaizdą apie duomenų valdytojo įgyvendinimo sprendimus, susijusius su pastebėtų duomenų sritimi, ir turės geresnes galimybes pasirinkti, kokius duomenis jis norės pateikti, kad gautų panašią paslaugą, taip pat suvoks, kaip laikomasi jo teisės į privatumą.

<sup>20</sup> Nepaisant to, duomenų subjektas vis tiek gali naudotis savo teise *iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi – teise susipažinti su asmens duomenimis ir <...> informacija <...> apie tai, kad esama 22 straipsnio 1 ir 4 dalyse nurodyto automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasminga informacija apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui, kaip nustatyta Bendrojo duomenų apsaugos reglamento 15 straipsnyje (kuriame aptariama teisė susipažinti su duomenimis).*

Apskritai, atsižvelgiant į teisės į duomenų perkeliamumą politikos tikslus, sąvoka *pateikti duomenų subjekto* turi būti aiškinama plačiai ir į ją turėtų nepateikti *netiesiogiai nustatyti duomenys* ir *išvesti duomenys*, apimantys asmens duomenis, kuriuos sukuria paslaugos teikėjas (pavyzdžiui, algoritminiai rezultatai). Duomenų valdytojas gali į šią sąvoką neįtraukti tų netiesiogiai nustatomų duomenų, bet turėtų įtraukti visus kitus asmens duomenis, kuriuos duomenų subjektas pateikė duomenų valdytojo suteiktomis techninėmis priemonėmis<sup>21</sup>.

Taigi, sąvoka *pateikti* apima asmens duomenis, susijusius su duomenų subjekto veikla ar asmens elgsenos stebėjimo rezultatu, tačiau neapima duomenų, gautų atliekant vėlesnę tos elgsenos analizę. O asmens duomenys, kuriuos duomenų valdytojas sukūrė tvarkydamas duomenis, pvz., suasmenindamas paslaugas ar teikdamas rekomendacijas, suskirstydamas vartotojus į kategorijas arba juos profiliuodamas, yra duomenys, kurie išvedami arba netiesiogiai nustatomi iš duomenų subjekto asmens duomenų, ir jų atžvilgiu teisė į duomenų perkeliamumą netaikoma.

Trečioji sąlyga: teisė į duomenų perkeliamumą neturi daryti neigiamo poveikio kitų asmenų teisėms ir laisvėms

### **Dėl asmens duomenų, susijusių su kitais duomenų subjektais**

Trečiają sąlyga siekiama užtikrinti, kad duomenys, tarp kurių yra kitų (sutikimo nedavusių) asmenų asmens duomenų, nebūtų paimami ir perduodami naujam duomenų valdytojui tais atvejais, kai šie duomenys, tikėtina, bus tvarkomi taip, kad tai turės neigiamą poveikį kitų duomenų subjektų teisėms ir laisvėms (Bendrojo duomenų apsaugos reglamento 20 straipsnio 4 dalis)<sup>22</sup>.

Toks neigiamas poveikis būtų daromas, pavyzdžiui, jeigu persiuntus duomenis iš vieno duomenų valdytojo kitam, trečiosios šalys netektų galimybės pasinaudoti savo teisėmis pagal Bendrąjį duomenų apsaugos reglamentą (pvz., teisėmis į informaciją, teise susipažinti su duomenimis ir kt.).

Duomenų subjektas, inicijuojantis savo duomenų persiuntimą kitam duomenų valdytojui, arba duoda savo sutikimą naujam duomenų valdytojui tvarkyti duomenis, arba su tuo duomenų valdytoju sudaro sutartį. Kai duomenų rinkinyje yra trečiųjų šalių asmens duomenų, turi būti nurodytas kitas duomenų tvarkymo teisinis pagrindas. Pavyzdžiui, duomenų valdytojas gali siekti teisėto intereso pagal 6 straipsnio 1 dalies f punktą, ypač kai duomenų valdytojo tikslas yra suteikti duomenų subjektui paslaugą, kuria pastarajam sudaromos sąlygos asmens duomenis tvarkyti vien asmeniniais ar namų ūkio veiklos tikslais. Duomenų subjekto inicijuotos duomenų tvarkymo operacijos, susijusios su asmenine veikla, kuri savo ruožtu yra susijusi su trečiosiomis šalimis ir gali turėti joms poveikį, ir toliau priklauso duomenų subjekto atsakomybei, jeigu dėl tokio duomenų tvarkymo duomenų valdytojas nepriima jokio savarankiško sprendimo.

<sup>21</sup> Tai apima visą informaciją apie duomenų subjektą, nustatytą iš veiklos, kurios tikslais renkami duomenys, pvz., operacijų istoriją ar prisijungimo žurnalą. Duomenys, surinkti sekant ir įrašant duomenų subjekto veiklą (pvz., naudojant programėlę, įrašančią pulsą, arba technologiją, skirtą sekti naršymo internete pobūdį), taip pat turėtų būti laikomi *pateiktais* duomenų subjekto, net jeigu duomenys nėra aktyviai ar sąmoningai persiunčiami.

<sup>22</sup> 68 konstatuojamojoje dalyje numatyta, kad *jei su tam tikru asmens duomenų rinkiniu yra susijęs daugiau nei vienas duomenų subjektas, teise gauti asmens duomenis neturėtų būti daromas poveikis kitų duomenų subjektų teisėms ir laisvėms pagal šį reglamentą*.

Pavyzdžiui, saityno pašto paslauga gali sudaryti sąlygas sukurti duomenų subjekto adresatų, draugų, giminaičių, šeimos narių ir kitų aplinkinių asmenų katalogą. Kadangi šie duomenys yra susiję su nustatytu asmeniu (ir jo sukurti), kuris pageidauja pasinaudoti savo teise į duomenų perkeliamumą, duomenų valdytojai turėtų persiųsti tam duomenų subjektui visą gaunamų ir siunčiamų e. laiškų katalogą.

Panašiai duomenų subjekto banko sąskaitoje gali būti asmens duomenų, susijusių net tik su sąskaitos turėtojo operacijomis, bet ir su kitų asmenų operacijomis (pvz., jeigu jie pervedė pinigus sąskaitos turėtojui). Nėra tikėtina, kad tų trečiųjų šalių teisėms ir laisvėms bus padarytas neigiamas poveikis banko sąskaitos informaciją persiuntus sąskaitos turėtojui, kai pateikiamas prašymas perkelti duomenis, jeigu abiejų pavyzdžių atveju duomenys bus naudojami tuo pačiu tikslu (t. y. adresato adresą naudos tik duomenų subjektas arba bus naudojama duomenų subjekto banko sąskaitos istorija).

Ir priešingai, trečiųjų šalių teisių ir laisvių nebus laikomasi, jeigu naujasis duomenų valdytojas asmens duomenis naudos kitais tikslais, pvz., jeigu duomenis gaunantis duomenų valdytojas kitų duomenų subjekto adresatų kataloge esančių asmenų asmens duomenis naudos rinkodaros tikslais.

Todėl, siekiant išvengti neigiamo poveikio atitinkamoms trečiosioms šalims, tvarkyti tokius asmens duomenis kitam duomenų valdytojui leidžiama tik tuo atveju, jeigu duomenis prižiūri tik perkėlimo prašantis vartotojas ir jie tvarkomi tik asmeninėms ar namų ūkio reikmėms. Duomenis gaunantis naujasis duomenų valdytojas (kuriam vartotojo prašymu gali būti persiunčiami duomenys), negali persiųstų trečiosios šalies duomenų naudoti savo paties tikslais, pvz., negali siūlyti tiems kitiems tretiesiems duomenų subjektams rinkodaros produktų ir paslaugų. Pavyzdžiui, ši informacija be trečiojo duomenų subjekto žinios ir sutikimo neturėtų būti naudojama trečiojo duomenų subjekto profiliui praturtinti ir jo socialinei aplinkai sumodeliuoti<sup>23</sup>. Jais taip pat negalima naudotis siekiant išgauti informaciją apie tokias trečiąsias šalis ir sukurti konkrečius profilius, net jeigu duomenų valdytojas jau turi jų asmens duomenis. Priešingu atveju toks duomenų tvarkymas, tikėtina, bus neteisėtas ir nesąžiningas, ypač jeigu atitinkamos trečiosios šalys neinformuojamos ir negali naudotis savo, kaip duomenų subjekto, teisėmis.

Be to, visų duomenų valdytojų (ir siunčiančių, ir gaunančių duomenis) pavyzdinė praktika yra įdiegti priemonės, kuriomis duomenų subjektams būtų sudarytos sąlygos pasirinkti aktualius duomenis, kuriuos jie pageidauja gauti ir persiųsti, ir, kai aktualu, atskirti kitų asmenų duomenis. Tai dar labiau padės mažinti trečiųjų šalių, kurių asmens duomenys gali būti perkeltami, riziką.

Be to, duomenų valdytojai turėtų įdiegti sutikimo gavimo mechanizmus kitiems atitinkamiems duomenų subjektams, kad duomenų persiuntimas būtų lengvesnis tais atvejais, kai tokios šalys pageidauja duoti sutikimą, pvz., jos taip pat nori perkelti savo duomenis kuriam nors kitam duomenų valdytojui. Tokia padėtis gali susidaryti, pavyzdžiui, socialiniuose tinkluose, tačiau dėl to, kokia pavyzdine praktika vadovautis, sprendžia duomenų valdytojai.

### **Dėl duomenų, kuriems taikomos intelektinės nuosavybės teisės ir komercinės paslaptys:**

---

<sup>23</sup> Socialinių tinklų kūrimo tarnyba, nesilaikydama skaidrumo principo ir neužtikrinusi tinkamo konkretaus duomenų tvarkymo teisinio pagrindo, neturėtų praturtinti savo narių profilio naudodamasi asmens duomenimis, kuriuos duomenų subjektas jai persiuntė naudodamasis savo teise į duomenų perkeliamumą.

Kitų asmenų teisės ir laisvės paminėtos 20 straipsnio 4 dalyje. Nors su duomenų perkeliamumu tai tiesiogiai ir nesusiję, tokias teises galima suvokti kaip apimančias *komercines paslaptis arba intelektinės nuosavybės teises, ypač autorių teises, kuriomis saugoma programinė įranga*. Vis dėlto nors prieš atsakant į prašymą perkelti duomenis į šias teises turėtų būti atsižvelgiama, *tai neturėtų lemti, kad duomenų subjektui būtų atsisakyta suteikti visą informaciją*. Be to, duomenų valdytojas neturėtų atmesti prašymo perkelti duomenis remdamasis kitos sutartinės teisės pažeidimu (pavyzdžiui, nesumokėta skola ar komerciniu konfliktu su duomenų subjektu).

Teisė į duomenų perkeliamumą nėra asmens teisė netinkamai naudoti informaciją tokiu būdu, kurį būtų galima laikyti nesąžininga praktika arba kuriuo būtų pažeidžiamos intelektinės nuosavybės teisės.

Tačiau galima verslo rizika pati savaime negali būti laikoma pagrindu neatsakyti į prašymą perkelti duomenis, o duomenų valdytojai gali persiųsti duomenų subjektų pateiktus asmens duomenis tokia forma, kuria nebūtų atskleista informacija, kuriai taikomos komercinės paslaptys arba intelektinės nuosavybės teisės.

#### **IV. Kaip bendrosios naudojimosi duomenų subjekto teisėmis taisyklės taikomos duomenų perkeliamumui?**

##### **- Kokia išankstinė informacija turėtų būti pateikta duomenų subjektui?**

Siekdami įgyvendinti naująją teisę į duomenų perkeliamumą, duomenų valdytojai turi informuoti duomenų subjektus apie šią naują teisę į duomenų perkeliamumą. Kai atitinkami asmens duomenys tiesiogiai renkami iš duomenų subjekto, tai turi būti daroma asmens *duomenų gavimo metu*. Jeigu asmens duomenys yra gauti ne iš duomenų subjekto, duomenų valdytojas turi pateikti informaciją, reikalaujamą 13 straipsnio 2 dalies b punkte ir 14 straipsnio 2 dalies c punkte.

Kai asmens duomenys yra gauti ne iš duomenų subjekto, 14 straipsnio 3 dalyje reikalaujama, kad informacija būtų pateikta per pagrįstą laikotarpį, bet ne vėliau kaip per vieną mėnesį nuo duomenų gavimo, ne vėliau kaip pirmą kartą susisiekiant su duomenų subjektu arba ne vėliau kaip atskleidžiant duomenis trečiosioms šalims<sup>24</sup>.

Teikdami reikalaujamą informaciją, duomenų valdytojai turi užtikrinti, kad jie teisę į duomenų perkeliamumą atskirtų nuo kitų teisių. Todėl WP29 visų pirma rekomenduoja duomenų valdytojams aiškiai išdėstyti, kuo skiriasi duomenų, kuriuos duomenų subjektas gali gauti naudodamasis teise susipažinti su duomenimis ir teise į duomenų perkeliamumą, tipai.

Be to, darbo grupė rekomenduoja duomenų valdytojams informaciją apie teisę į duomenų perkeliamumą visada pateikti, kol dar duomenų subjektai nepanaikino galimai turėtos paskyros. Taip vartotojams sudaromos sąlygos inventorizuoti savo asmens duomenis ir lengvai juos persiųsti į savo įrenginį arba kitam paslaugų teikėjui ir tik tada nutraukti sutartį.

Galiausiai WP29 rekomenduoja duomenis gaunantiems duomenų valdytojams taikyti gerąją patirtį pateikti duomenų subjektams visą informaciją apie jų paslaugoms vykdyti aktualių

---

<sup>24</sup> 12 straipsnyje reikalaujama, kad duomenų valdytojai *visus pranešimus [...] pateiktų glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba, ypač jei informacija yra konkrečiai skirta vaikui*.

asmens duomenų pobūdį. Šia praktika ne tik grindžiamas sąžiningas duomenų tvarkymas, bet ir vartotojams sudaromos sąlygos apriboti riziką trečiosioms šalims, taip pat sumažinti kitą nereikalingą asmens duomenų dubliavimą, net kai tai nesusiję su kitais duomenų subjektais.

**- Kaip duomenų valdytojas gali identifikuoti duomenų subjektą prieš atsakydamas į jo prašymą?**

Bendrajame duomenų apsaugos reglamente nenustatoma imperatyvių reikalavimų, kaip patvirtinti duomenų subjekto autentiškumą. Nepaisant to, 12 straipsnio 2 dalyje nurodyta, kad duomenų valdytojas neatsisako imtis veiksmų pagal duomenų subjekto prašymą pasinaudoti jo teisėmis (įskaitant teisę į duomenų perkeliamumą), nebent asmens duomenys tvarkomi tokiu tikslu, kuriam nereikia nustatyti duomenų subjekto tapatybės ir duomenų valdytojas įrodo, kad jis negali nustatyti duomenų subjekto tapatybės. Vis dėlto pagal 11 straipsnio 2 dalį tokiais aplinkybėmis duomenų subjektas gali pateikti daugiau informacijos, kad jo tapatybę būtų galima nustatyti. Be to, 12 straipsnio 6 dalyje numatyta, kad jeigu duomenų valdytojas turi pagrįstų abejonių dėl duomenų subjekto tapatybės, duomenų valdytojas gali paprašyti pateikti papildomos informacijos, reikalingos norint patvirtinti duomenų subjekto tapatybę. Kai duomenų subjektas pateikia papildomą informaciją, suteikiančią galimybę nustatyti jo tapatybę, duomenų valdytojas neatsisako vykdyti prašymo. Kai internetu renkama informacija ir duomenys yra susiję su pseudonimais ar unikaliais identifikatoriais, duomenų valdytojai gali įdiegti reikiamas procedūras, kuriomis asmeniui būtų sudarytos sąlygos pateikti prašymą perkelti duomenis ir gauti su juo susijusius duomenis. Bet kuriuo atveju duomenų valdytojai turi įdiegti autentiškumo patvirtinimo procedūrą, kad galėtų patikimai nustatyti duomenų subjekto, prašančio perkelti jo asmens duomenis arba apskritai įgyvendinančio Bendruoju duomenų apsaugos reglamentu jam suteiktas teises, tapatybę.

Dažnu atveju šios procedūros jau taikomos. Duomenų subjektų autentiškumą duomenų valdytojas dažnai jau būna patvirtinęs sudarydamas su tokiu duomenų subjektu sutartį arba gaudamas jo sutikimą, kad būtų tvarkomi duomenys. Taigi, asmens duomenys, panaudoti atitinkamam duomenų tvarkymu suinteresuotam asmeniui užregistruoti, taip pat gali būti naudojami kaip įrodymai duomenų subjekto autentiškumui patvirtinti duomenų perkeliavimo tikslais<sup>25</sup>.

Nors šiais atvejais siekiant iš anksto nustatyti duomenų subjektų tapatybę gali prireikti paprašyti jų teisinės tapatybės įrodymo, toks patikrinimas gali nebūti aktualus siekiant įvertinti duomenų ir atitinkamo asmens ryšį, nes toks ryšys nėra susijęs su oficialia arba teisine tapatybe. Iš esmės duomenų valdytojo galimybė paprašyti papildomos informacijos asmens tapatybei įvertinti negali būti neproporcingų reikalavimų pagrindas ir ja remiantis negali būti renkami asmens duomenys, kurie nėra aktualūs ar būtini asmens ir prašomų asmens duomenų ryšiui patikimiau nustatyti.

Daugeliu atvejų tokios autentiškumo patvirtinimo procedūros jau taikomos. Pavyzdžiui, vartotojo vardai ir slaptažodžiai dažnai naudojami siekiant leisti asmenims prisijungti prie savo duomenų e. pašto paskyroje, socialinių tinklų paskyroje ir įvairioms kitoms paslaugoms naudojamose paskyroje – kai kurias iš šių paskyrų asmenys nusprendė naudoti neatskleisdami viso savo vardo ir pavardės bei tapatybės.

---

<sup>25</sup> Pavyzdžiui, kai duomenų tvarkymas yra susijęs su vartotojo paskyra, atitinkamo prisijungimo vardo ir slaptažodžio pateikimo gali užtekti duomenų subjekto tapatybei nustatyti.

Jeigu dėl duomenų subjekto prašomų duomenų apimtį persiuntimas internetu kelia problemų, duomenų valdytojas gali ne tik numatyti ilgesnį daugiausia trejų mėnesių laikotarpį prašymui įvykdyti<sup>26</sup>, bet ir (pageidautina) gali būti priverstas apsvarstyti alternatyvias duomenų pateikimo priemones, pvz., srautinį duomenų siuntimą arba jų išsaugojimą CD, DVD ar kitose fizinėse laikmenose arba sudaryti sąlygas asmens duomenis persiųsti tiesiogiai kitam duomenų valdytojui (pagal Bendrojo duomenų apsaugos reglamento 20 straipsnio 2 dalį, kai tai techniškai įmanoma).

**- Per kokį nustatytą laiką reikia atsakyti į prašymą perkelti duomenis?**

12 straipsnio 3 dalyje reikalaujama, kad *duomenų valdytojas nepagrįstai nedelsdamas, tačiau bet kuriuo atveju ne vėliau kaip per vieną mėnesį nuo prašymo gavimo*, pateiktų duomenų subjektui informaciją apie veiksmus, kurių imtasi gavus prašymą. Šį vieno mėnesio laikotarpį sudėtingais atvejais galima pratęsti daugiausia iki trijų mėnesių, jeigu duomenų subjektas per mėnesį nuo pradinio prašymo gavimo buvo informuotas apie tokio vėlavimo priežastis.

Informacinės visuomenės paslaugas teikiantys duomenų valdytojai, tikėtina, turės geresnes galimybes įvykdyti prašymus per labai trumpą laiką. Siekiant patenkinti vartotojų lūkesčius, gera praktika yra apibrėžti laikotarpį, per kurį paprastai galima atsakyti į prašymą perkelti duomenis, ir tą laikotarpį nurodyti duomenų subjektams.

Duomenų valdytojai, atsisakantys patenkinti prašymą perkelti duomenis, pagal 12 straipsnio 4 dalį *ne vėliau kaip per vieną mėnesį nuo prašymo gavimo informuoja duomenų subjektą apie neveikimo priežastis ir apie galimybę pateikti skundą priežiūros institucijai bei pasinaudoti teisių gynimo priemone*.

**Duomenų valdytojai turi laikytis įpareigojimo atsakyti per nurodytą laiką, netgi jeigu tai bus atsisakymas. Kitaip tariant, duomenų valdytojas negali tylėti, kai jo prašoma patenkinti prašymą perkelti duomenis.**

**- Kuriais atvejais prašymą perkelti duomenis galima atmesti arba imti mokesť?**

12 straipsnyje duomenų valdytojui draudžiama už asmens duomenų suteikimą imti mokesť, nebent duomenų valdytojas gali įrodyti, kad prašymai yra akivaizdžiai nepagrįsti ar neproporcingi, *visų pirma dėl jų pasikartojančio turinio*. Informacinės visuomenės paslaugų teikėjams, besispecializuojantiems automatizuotai tvarkyti asmens duomenis, įdiegus automatizuotas sistemas, pvz., programų sąsajas<sup>27</sup>, gali būti lengviau keistis duomenimis su duomenų subjektu, taigi, sumažėtų galima pasikartojančių prašymų našta. Taigi, turėtų būti labai mažai atvejų, kai duomenų valdytojas galėtų pagrįsti atsisakymą pateikti prašomą informaciją, netgi remdamasis daugeliu prašymų perkelti duomenis.

Be to, siekiant įvertinti, ar prašymas yra neproporcingas, neturėtų būti atsižvelgiama į bendras procesų, sukurtų siekiant atsakyti į prašymus perkelti duomenis, išlaidas. Beje, Bendrojo duomenų apsaugos reglamento 12 straipsnyje kalbama apie vieno duomenų subjekto pateiktus prašymus, o ne apie bendrą duomenų valdytojo gautų prašymų skaičių. Taigi, bendros sistemos įgyvendinimo išlaidos neturėtų būti nei perkeliamos duomenų subjektams, nei naudojamos siekiant pagrįsti atsisakymą perkelti duomenis.

<sup>26</sup> 12 straipsnio 3 dalis: Duomenų valdytojas pateikia informaciją apie veiksmus, kurių imtasi gavus prašymą.

<sup>27</sup> Programų sąsaja reiškia duomenų valdytojų suteiktas programų ar interneto paslaugų sąsajas, kad kitos sistemos ar programos galėtų susijungti ir dirbti su jų sistemomis.



## V. Kaip turi būti suteikiami perkeliami duomenys?

- Kokių tikimasi priemonių, kurias duomenų valdytojas turėtų įgyvendinti duomenims pateikti

Bendrojo duomenų apsaugos reglamento 20 straipsnio 1 dalyje duomenų subjektams numatyta teisė be kliūčių persiųsti asmens duomenis iš vieno duomenų valdytojo, kuriam buvo pateikti asmens duomenys, kitam duomenų valdytojui.

Tokiomis kliūtimis galima laikyti bet kurias teisines, technines ar finansines duomenų valdytojo sudaromas kliūtis, kuriomis būtų atimama ar sulėtinama duomenų subjekto ar kito duomenų valdytojo prieiga prie duomenų, jų persiuntimas ar būtų sumažinama galimybė juos pakartotinai naudoti. Pavyzdžiui, tokios kliūtys galėtų būti už duomenų pateikimą imami mokesčiai, nepakankamas sąveikumas, galimybės nuskaityti duomenų formatą arba prisijungti prie programų sąsajos ar pateikto duomenų formato nebuvimas, pernelyg ilgas arba sudėtingas viso duomenų rinkinio atsisiaunimo procesas, sąmoningas duomenų rinkinio sujaukimas arba specifiniai ir nederami ar neproporcingi sektoriniai standartizavimo ar akreditavimo reikalavimai<sup>28</sup>.

20 straipsnio 2 dalyje taip pat nustatomos pareigos duomenų valdytojams persiųsti perkeliamus duomenis tiesiogiai kitiems duomenų valdytojams, *kai tai techniškai įmanoma*.

Ar techniškai įmanoma, prižiūrint duomenų subjektui, persiųsti duomenis iš vieno duomenų valdytojo kitam, turėtų būti vertinama kiekvienu konkrečiu atveju. 68 konstatuojamojoje dalyje aiškiau išdėstomos ribos, kas yra *techniškai įmanoma*, nurodant, kad tai *neturėtų sukurti duomenų valdytojams prievolės nustatyti ar išlaikyti duomenų tvarkymo sistemas, kurios yra techniškai suderinamos*.

Tikimasi, kad duomenų valdytojai asmens duomenis perduos sąveikiu formatu, tačiau tai neįpareigoja kitų duomenų valdytojų gebėti šiuos formatus nuskaityti. Taigi, tiesioginis duomenų persiuntimas iš vieno duomenų valdytojo kitam galėtų saugiai<sup>29</sup> vykti, kai įmanomas dviejų sistemų ryšys ir kai gaunanti sistema turi technines galimybes priimti gaunamus duomenis. Jeigu dėl techninių kliūčių tiesioginis persiuntimas neįmanomas, duomenų valdytojas tas kliūtis paaiškina duomenų subjektams, nes priešingu atveju jo sprendimo poveikis būtų panašus į atsisakymą imtis veiksmų pagal duomenų subjekto prašymą (12 straipsnio 4 dalis).

Techniniu lygmeniu duomenų valdytojai turėtų išsiaiškinti ir įvertinti du skirtingus, vienas kitą papildančius būdus perduoti perkeliamus duomenis duomenų subjektams ar kitiems duomenų valdytojams:

- tiesioginį viso perkeliamų duomenų rinkinio (arba keleto viso duomenų rinkinio dalių ištraukų) persiuntimą;
- automatizuotą priemonę, suteikiančią galimybę atsisiųsti aktualius duomenis.

<sup>28</sup> Gali kilti tam tikrų teisėtų kliūčių, pvz., susijusių su kitų asmenų teisėmis ir laisvėmis, paminėtomis 20 straipsnio 4 dalyje, arba susijusių su pačių duomenų valdytojų sistemų saugumu. Duomenų valdytojas privalo pagrįsti, kodėl tokios kliūtys laikytinos teisėtomis ir kodėl jos nelaikytinos kliūtimis pagal 20 straipsnio 1 dalį.

<sup>29</sup> Naudojantis ryšiu, kurio autentiškumas patvirtintas, ir reikiamo lygio duomenų šifravimu.

Antrajam būdai duomenų valdytojai gali teikti pirmenybę, kai duomenų rinkiniai yra sudėtingi ir dideli, nes šis būdas sudaro sąlygas atsisiųsti bet kurią duomenų rinkinio dalį, aktualią duomenų subjektui pagal jo prašymą, taip pat gali padėti kuo labiau sumažinti riziką ir gali suteikti galimybę naudoti duomenų sinchronizavimo mechanizmus<sup>30</sup> (pvz., duomenų valdytojams reguliariai palaikant tarpusavio ryšį). Tai gali būti geresnis būdas užtikrinti, kad naujasis duomenų valdytojas laikytųsi reikalavimų, ir tai būtų pradinio duomenų valdytojo geroji patirtis mažinant privatumui kylančią riziką.

Šie du skirtingi ir galbūt vienas kitą papildantys būdai pateikti aktualius perkeliamus duomenis galėtų būti įgyvendinami teikiant duomenis įvairiomis priemonėmis, pavyzdžiui, juos persiunčiant saugiomis žinutėmis, per SFTP serverį, saugią saityno programų sąsają arba interneto portalą. Duomenų subjektams turėtų būti suteikta galimybė asmeninius duomenis laikyti ir saugoti asmeninėje duomenų saugykloje, asmeninėje informacijos valdymo sistemoje<sup>31</sup> arba naudojantis kitokiomis trečiosios šalies, kuria jie pasitiki, paslaugomis ir suteikti leidimą duomenų valdytojams prireikus prieiti prie asmens duomenų ir juos tvarkyti.

#### - **Kokio tikimasi duomenų formato?**

Bendruoju duomenų apsaugos reglamentu duomenų valdytojams nustatomi reikalavimai asmens prašomus asmens duomenis pateikti tokiu formatu, kad juos būtų galima pakartotinai naudoti. Konkrečiai Bendrojo duomenų apsaugos reglamento 20 straipsnio 1 dalyje nurodoma, kad asmens duomenys turi būti perduodami *susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu*. 68 konstatuojamojoje dalyje pateikiamas papildomas paaiškinimas, kad šis formatas turėtų būti sąveikus, o pastaroji sąvoka Europos Sąjungoje apibrėžta<sup>32</sup> kaip:

*atskirų ir skirtingų organizacijų gebėjimas bendrai veikti siekiant abipusiai naudingų ir sutartų bendrų tikslų, įskaitant informacijos ir žinių mainus tarp organizacijų, atliekant veiklos procesus, kuriuos jos gali vykdyti, duomenų mainams naudojant savo atitinkamas IRT sistemas.*

Sąvokos *susistemintas, įprastai naudojamas ir kompiuterio skaitomas formatas* yra būtinųjų reikalavimų rinkinys, kuriuo turėtų būti skatinamas duomenų valdytojo pateikiamų duomenų formato sąveikumas. Tokiu būdu *susistemintas, įprastai naudojamas ir kompiuterio skaitomas formatas* yra priemonių specifikacijos, o sąveikumas yra pageidaujamas rezultatas.

Direktyvos 2013/37/ES<sup>33</sup> 21 konstatuojamojoje dalyje *elektroninis formatas* apibrėžiamas kaip:

<sup>30</sup> Sinchronizavimo mechanizmas gali padėti įvykdyti Bendrojo duomenų apsaugos reglamento 5 straipsnyje išdėstytus bendruosius įpareigojimus – jame nustatyta, kad *asmens duomenys turi būti [...] tikslūs ir prireikus atnaujinami*.

<sup>31</sup> Asmeninių informacijos valdymo sistemų klausimu žr., pavyzdžiui, Europos duomenų apsaugos priežiūros pareigūno nuomonę 9/2016, pateiktą adresu [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20\\_PIMS\\_opinion\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf).

<sup>32</sup> 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos sprendimas Nr. 922/2009/EB dėl Europos viešojo administravimo institucijų sąveikumo sprendimų (ISA) (OL L 260, 2009 10 3, p. 20).

<sup>33</sup> kuria iš dalies keičiama Direktyva 2003/98/EB dėl viešojo sektoriaus informacijos pakartotinio naudojimo.

*rinkmenos formatas, kurio struktūra leidžia kompiuterinėms programoms lengvai nustatyti, atpažinti ir gauti konkrečius duomenis, įskaitant atskirus konstatuojamus faktus ir jų vidaus struktūrą. Elektroninio formato rinkmenose užkoduoti duomenys laikomi elektroniniais duomenimis. Elektroniniai formatai gali būti atvirieji arba nuosavybiniai; jie gali būti oficialūs standartai arba ne. Elektroninio formato dokumentais nelaikomi dokumentai, užkoduoti naudojant tokį rinkmenos formatą, kuris riboja automatinę tvarkymą, nes iš jų duomenų negalima išskirti arba tai sunku padaryti. Kai tinkama, valstybės narės turėtų skatinti naudoti atvirose elektroninius formatus.*

Atsižvelgiant į platų galimų duomenų, kuriuos gali tvarkyti duomenų valdytojas, tipų spektrą, Bendrajame duomenų apsaugos reglamente nenustatyta konkrečių rekomendacijų dėl pateiktinų asmens duomenų formato. Tinkamiausias formatas įvairiuose sektoriuose bus skirtingas ir tinkamų formatų galbūt jau yra, jie visada turėtų būti pasirenkami taip, kad duomenys būtų perskaitomi ir duomenų subjektui būtų suteiktos plačios galimybės perkelti duomenis. Tokie formatai, kuriems taikomi brangiai kainuojantys licencijavimo apribojimai, nebūtų laikomi tinkamu metodu.

68 konstatuojamojoje dalyje paaiškinama, kad *duomenų subjekto teisė persiųsti arba gauti savo asmens duomenis neturėtų sukurti duomenų valdytojams prievolės nustatyti ar išlaikyti duomenų tvarkymo sistemas, kurios yra techniškai suderinamos. Taigi, perkeliamumu siekiama užtikrinti sąveikias sistemas, ne suderinamas sistemas*<sup>35</sup>.

Tikimasi, kad asmens duomenys bus teikiami tokiais formatais, kuriuos lengva generuoti iš bet kurio vidinio ar nuosavybinio formato. Pats duomenų perkeliamumas netiesiogiai reiškia papildomą duomenų valdytojų atliekamo duomenų tvarkymo lygmenį, t. y. duomenys išgaunami iš platformos ir atmetami asmens duomenys, kurių atžvilgiu netaikoma teisė į duomenų perkeliamumą, pvz., netiesiogiai nustatyti duomenys arba su sistemų saugumu susiję duomenys. Tokiu būdu duomenų valdytojai skatinami iš anksto savo sistemose nustatyti duomenis, kurie gali būti perkelti. Šis papildomas duomenų tvarkymas laikomas pagalbinio pagrindiniam duomenų tvarkymui, nes juo nesiekama duomenų valdytojo apibrėžto naujo tikslo.

Kai konkrečioje pramonės šakoje arba konkrečiomis aplinkybėmis nėra įprastai naudojamų formatų, **duomenų valdytojai asmeninius duomenis turėtų pateikti įprastai naudojamais atviraisiais formatais (pvz., XML, JSON, CSV,...) kartu su naudingais ir kuo labiau detalizuotais metaduomenimis**, išlaikydami aukštą duomenų išgavimo lygį. Tinkami metaduomenys turėtų būti naudojami siekiant tiksliai apibūdinti informacijos, kuria keičiamasi, reikšmę. Šių metaduomenų turėtų pakakti, kad duomenys būtų funkcionalūs ir būtų įmanoma juos pakartotinai naudoti, tačiau, žinoma, neturėtų būti atskleidžiama komercinių paslapčių. Taigi, nėra tikėtina, kad asmeniui pateikiamas e. pašto gaunamų laiškų dėžutės PDF variantas būtų pakankamai susistemintas ar jame būtų pakankamai duomenų, kurie sudarytų sąlygas lengvai pakartotinai panaudoti gaunamų laiškų dėžutės duomenis. Vietoj to e. pašto duomenys turėtų būti pateikiami tokiu formatu, kuriuo būtų išsaugomi visi

<sup>34</sup> ES glosarijuje (<http://eur-lex.europa.eu/eli-register/glossary.html>) pateiktas dar vienas lūkesčių, susijusių su šiose gairėse vartojamomis sąvokomis, pvz., *kompiuterio skaitomas, sąveikumas, atvirasis formatas, standartas, metaduomenys*, paaiškinimas.

<sup>35</sup> ISO/IEC 2382-01 sąveikumas apibrėžiamas taip: *gebėjimas palaikyti ryšį, vykdyti programas ar perduoti duomenis tarp įvairių funkcinų vienetų taip, kad vartotojui užtektų nedaug žinių apie unikalius tų vienetų ypatumus arba tų žinių apskritai nereikėtų*.

metaduomenys, kad duomenis būtų galima veiksmingai pakartotinai naudoti. Taigi, pasirinkdamas asmens duomenų pateikimo formatą, duomenų valdytojas turėtų atsižvelgti į tai, kaip šis formatas paveiktų ar sumažintų asmens teisę pakartotinai naudoti duomenis. Tais atvejais, kai duomenų valdytojai gali duomenų subjektui suteikti galimybę pasirinkti pageidaujamą asmens duomenų formatą, turėtų būti pateiktas aiškus pasirinkimo poveikio paaiškinimas. Tačiau papildomų metaduomenų tvarkymas vien tuo tikslu, kad jie galbūt bus būtini ar pageidaujami atsakant į prašymą perkelti duomenis, nėra teisėtas tokio duomenų tvarkymo pagrindas.

**WP29 tvirtai ragina suinteresuotuosius pramonės subjektus ir profesines asociacijas bendradarbiauti tarpusavyje siekiant parengti bendrą sąveikių standartų ir formatų rinkinį, kad būtų galima įvykdyti teisės į duomenų perkeliamumą reikalavimus.** Šis uždavinys taip pat buvo sprendžiamas kuriant Europos sąveikumo sistemą, pagal kurią buvo parengtas suderintas požiūris į sąveikumą organizacijoms, pageidaujančioms kartu teikti viešąsias paslaugas. Šia sistema jos taikymo srityje nustatomi tam tikri bendri elementai, pvz., žodynas, koncepcijos, principai, politikos kryptys, gairės, rekomendacijos, standartai, specifikacijos ir metodai<sup>36</sup>.

#### - **Kaip elgtis su dideliu ar sudėtingu asmens duomenų rinkiniu?**

Bendrajame duomenų apsaugos reglamente nepaaiškinta, kaip reaguoti, kai kyla tokių techninių problemų kaip didelis duomenų rinkinys, sudėtinga duomenų struktūra ar kt., kurios gali sukelti sunkumų duomenų valdytojams ar duomenų subjektams.

Vis dėlto visais atvejais itin svarbu, kad asmuo turėtų galimybę iki galo suprasti asmens duomenų, kuriuos gali pateikti duomenų valdytojas, apibrėžti, schemas ir struktūrą. Pavyzdžiui, pirmiausia duomenis būtų galima pateikti apibendrinta forma, naudojant komandų rinkinį, kuriuo naudodamasis duomenų subjektas galėtų perkelti asmens duomenų poaibius, o ne juos visus. Duomenų valdytojas *glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba* (žr. Bendrojo duomenų apsaugos reglamento 12 straipsnio 1 dalį) turėtų pateikti tokią duomenų apžvalgą, kad duomenų subjektas visada turėtų aiškią informaciją, kokius duomenis konkrečiu tikslu atsisiųsti ar persiųsti kitam duomenų valdytojui. Pavyzdžiui, duomenų subjektai turėtų turėti galimybę naudodami programinę įrangą šioje apžvalgoje lengvai nustatyti, atpažinti ir tvarkyti konkrečius duomenis.

Kaip jau minėta, praktinis būdas, kuriuo duomenų valdytojas gali atsakyti į prašymus perkelti duomenis, gali būti tinkamai apsaugotos ir dokumentais įformintos programų sąsajos suteikimas. Taip asmenims gali būti sudarytos sąlygos savo asmens duomenų prašymus duomenų valdytojams teikti per savo pačių arba trečiosios šalies programinę įrangą arba suteikti leidimą kitiems (įskaitant kitą duomenų valdytoją) tai daryti jų vardu, kaip nurodyta Bendrojo duomenų apsaugos reglamento 20 straipsnio 2 dalyje. Suteikiant prisijungimą prie duomenų per išorėje prieinamą programų sąsają, taip pat gali būti įmanoma pasiūlyti sudėtingesnę prieigos sistemą, kuria asmenims būtų sudaromos sąlygos teikti vėlesnius prašymus atsisiųsti visus duomenis kaip rinkinį arba kaip delta funkciją, apimančią tik po paskutinio atsisiuntimo padarytus pakeitimus, ir šie papildomi prašymai neapsunkintų duomenų valdytojo.

---

<sup>36</sup> Šaltinis: [http://ec.europa.eu/isa/documents/isa\\_annex\\_ii\\_eif\\_en.pdf](http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf).

## - Kaip galima apsaugoti perkeliamus duomenis?

Apskritai duomenų valdytojai turėtų garantuoti, *kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo*, kaip nurodyta Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies f punkte.

Tačiau asmens duomenų persiuntimas duomenų subjektui taip pat gali kelti tam tikrų saugumo klausimų:

Kaip duomenų valdytojams užtikrinti, kad asmens duomenys būtų saugiai perduoti tinkamam asmeniui?

Kadangi duomenų perkeliavimo tikslas – gauti asmens duomenis iš duomenų valdytojo informacinės sistemos, duomenų persiuntimas gali sukelti riziką tiems duomenims (visų pirma jeigu persiunčiant duomenis būtų pažeistas jų saugumas). Duomenų valdytojas privalo imtis visų saugumo priemonių, reikalingų siekiant ne tik užtikrinti, kad asmens duomenys būtų saugiai persiunčiami (naudojant ištisinį šifravimą arba duomenų šifravimą) į tinkamą paskirties vietą (naudojant patikimas autentiškumo patvirtinimo priemones), bet ir toliau apsaugoti jo sistemose liekančius asmens duomenis, taip pat įdiegti skaidrias galimų duomenų saugumo pažeidimų šalinimo procedūras<sup>37</sup>. Duomenų valdytojai turėtų įvertinti konkrečias su duomenų perkeliavimu susijusios rizikos rūšis ir imtis atitinkamų rizikos mažinimo priemonių.

Tokios rizikos mažinimo priemonės, be kita ko, galėtų būti: jeigu jau reikia patvirtinti duomenų subjekto autentiškumą – papildomos autentiškumo patvirtinimo informacijos, pvz., bendros paslapties ar kito autentiškumo patvirtinimo veiksnio, pvz., vienkartinio slaptažodžio, naudojimas; persiuntimo sustabdymas ar išaldymas, jeigu kyla įtarimas, kad paskyra buvo pažeista; jeigu duomenų valdytojas duomenis tiesiogiai persiunčia kitam duomenų valdytojui – turėtų būti naudojamas autentiškumo patvirtinimas pagal įgaliojimą, pvz., elektroniniu tapatumo nustatymo įrenginiu.

Tokios saugumo priemonės neturi virsti kliūtimis, jomis vartotojams neturi būti užkirstas kelias pasinaudoti savo teisėmis, pvz., neturi kilti papildomų išlaidų.

Kaip padėti vartotojams apsaugoti savo asmens duomenis nuosavose sistemose

Atsisiunčiant asmens duomenis iš internetinės paslaugos teikėjo, visada kyla rizika, kad vartotojai juos gali saugoti mažiau apsaugotose sistemose negu tos, kurias suteikia paslaugos teikėjas. Duomenų prašantis duomenų subjektas yra atsakingas už tinkamų priemonių nustatymą asmens duomenims savo paties sistemoje apsaugoti. Vis dėlto apie tai jį reikėtų informuoti, kad jis galėtų imtis veiksmų gautai informacijai apsaugoti. Vienas iš pavyzdinės praktikos variantų: duomenų valdytojai, siekiantys padėti duomenų subjektui pasiekti šį tikslą, gali taip pat rekomenduoti tinkamą (-us) formatą (-us), šifravimo priemones ir kitas saugumo priemones.

\* \* \*

---

<sup>37</sup> Laikantis Direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

Priimta Briuselyje 2016 m. gruodžio 13 d.

*Darbo grupės vardu*  
*Pirmininkė*  
*Isabelle FALQUE-PIERROTIN*

Priimta su paskutiniaisiais pakeitimais 2017 m.  
balandžio 5 d.

*Darbo grupės vardu*  
*Pirmininkė*  
*Isabelle FALQUE-PIERROTIN*