REKOMENDACIJA

NUASMENINIMO METODAI

ĮŽANGA

Naudojant įvairius įrenginius, jutiklius ir tinklus sukuriama gausybė duomenų ir atsiranda naujos duomenų rūšys, o duomenų laikymo kaina darosi nereikšminga, visuomenėje stiprėja kartotinio šių duomenų naudojimo interesas ir poreikis. Atvirieji duomenys visuomenei, pavieniams asmenims ir organizacijoms neabejotinai gali būti naudingi, tačiau tik tuo atveju, jeigu bus gerbiamos kiekvieno asmens teisės į asmens duomenų ir privataus gyvenimo apsaugą.

Nuasmeninimas (angl. *anonymization* arba *data masking*) gali būti tinkama naudos išsaugojimo ir rizikos mažinimo strategija. Visiškai nuasmeninus duomenų rinkinį ir panaikinus galimybę nustatyti asmens tapatybę, tokiems duomenims nebetaikomi Europos Sąjungos (ES) duomenų apsaugos teisės aktai. Antra vertus, iš konkrečių atvejų tyrimų ir mokslinių straipsnių aiškiai matyti, kad, remiantis gausiu asmens duomenų rinkiniu, parengti visiškai anoniminį duomenų rinkinį ir kartu išsaugoti tiek jame esančios informacijos, kiek reikia užduočiai atlikti, nėra paprasta. Pavyzdžiui, anoniminiu laikomą duomenų rinkinį sujungus su kitu duomenų rinkiniu, gali atsirasti galimybė nustatyti vieno arba daugiau asmenų tapatybę.

Duomenų valdytojams nuasmeninimas gali būti vertingas kaip strategija, ypač atviruųjų duomenų panaudojimo reikmėms, kartu mažinant susijusiems asmenims gresiančius pavojus. Vis dėlto konkrečių atvejų tyrimai ir moksliniai straipsniai parodė, kaip sunku parengti visiškai anoniminį duomenų rinkinį, kartu išsaugant užduočiai atlikti svarbią informaciją.

Vadovaujantis Direktyva 95/46/EB ir kitais susijusiais ES teisės aktais, anonimiškumo pasiekiama tvarkant asmens duomenis taip, kad nebebūtų galima atsekti asmens tapatybės. Todėl duomenų valdytojai, atsižvelgdami į visas priemones, kuriomis koks nors valdytojas arba trečioji šalis „galėtų“ pasinaudoti asmens tapatybei nustatyti, turėtų įvertinti kelis aspektus.

Nuasmeninimas – tai tolesnis asmens duomenų tvarkymas; toks procesas turi atitikti suderinamumo reikalavimą, t. y. turi būti vykdomas atsižvelgiant į teisinį pagrindą ir tolesnio tvarkymo aplinkybes. Be to, nuasmenintiems duomenims netaikomi duomenų apsaugos teisės aktai, tačiau duomenų subjektams vis vien gali būti suteikta teisė į apsaugą pagal kitas nuostatas (pvz., dėl pranešimų konfidencialumo apsaugos).

Pagrindiniai nuasmeninimo metodai yra randomizavimas ir apibendrinimas. Aptariami šie metodai: iškraipytų duomenų įterpimas, perstatymas, diferencinis privatumas, agregavimas, *k* anonimiškumas, *l* įvairovė ir *t* tankis. Aiškinami šių metodų principai, jų privalumai ir trūkumai, taip pat dažniausios su kiekvieno metodo taikymu susijusios klaidos ir nesėkmės.

Rekomendacija parengta remiantis kiekvieno metodo patikimumu, kuris grindžiamas šiais trimis kriterijais:

i) ar išlieka galimybė išskirti pavienį asmenį;
ii) ar išlieka galimybė susieti įrašus, susijusius su pavieniu asmeniu;
iii) ar iš informacijos galima gauti išvestinių duomenų apie pavienį asmenį.

Žinant pagrindinius kiekvieno metodo privalumus ir trūkumus, lengviau nuspręsti, kaip atitinkamomis aplinkybėmis parengti tinkamą nuasmeninimo procedūrą.

Siekiant išsiaiškinti kai kuriuos pavojus ir klaidingas nuomones, aptariamas ir duomenų kodavimas pseudonimais, kuris, beje, nėra nuasmeninimo metodas. Tai – tik galimybės duomenų rinkinį susieti su duomenų subjekto pirmine tapatybe sumažinimas, t. y. naudinga saugumo priemonė.

Pagaliau duomenų valdytojai turėtų atsižvelgti į tai, kad ir nuasmenintas duomenų rinkinys duomenų subjektams vis dar gali kelti liekamąją riziką. Viena vertus, nuasmeninimo ir pakartotinio tapatybės nustatymo srityse išties aktyviai vykdomi moksliniai tyrimai ir reguliariai skelbiama apie naujoves, kita vertus, net ir nuasmeninti duomenys, pvz., statistiniai, gali būti naudojami pavienių asmenų profiliams papildyti, taip sukeliant naujas duomenų apsaugos problemas.

Taigi nuasmeninimas neturėtų būti laikomas vienkartine užduotimi, o duomenų valdytojai turėtų reguliariai kaskart iš naujo įvertinti susijusią riziką.

APIBRĖŽTIS IR TEISINĖ ANALIZĖ

Išanalizavus pagrindiniuose ES duomenų apsaugos teisės aktuose pateikiamas su nuasmeninimu susijusias formuluotes, galima pabrėžti šiuos keturis aspektus:

- nuasmeninimas gali būti asmens duomenų tvarkymo siekiant negrąžinamai panaikinti galimybę nustatyti duomenų subjekto tapatybę rezultatas;
- egzistuoja keletas nuasmeninimo metodų, ES ir Lietuvos Respublikos teisės aktuose privalomas jo standartas nenustatytas;
- svarbiais reikėtų laikyti su aplinkybėmis susijusius veiksnius: turi būti atsižvelgiama į „visas“ priemones, kuriomis „galėtų“ pasinaudoti duomenų valdytojas ir kuri nors trečioji šalis asmens tapatybei nustatyti, ypatingą dėmesį skiriant priemonėms, kurios, atsižvelgiant į dabartinį technologijų lygį, pastaruoju metu jau „gali būti“ panaudojamos (dėl padidėjusių skaičiavimo pajėgumų ir prieinamų priemonių);
- nuasmeninimui būdingas rizikos veiksnys: į jį reikėtų atsižvelgti vertinant nuasmeninimo metodikos tinkamumą, be kitų dalykų, atsižvelgiant į galimus tokiu metodu nuasmenintų duomenų panaudojimo būdus; be to, turėtų būti įvertintas tos rizikos dydis ir pasireiškimo tikimybė.

Nuasmeninimas yra asmens duomenims taikomas metodas, kuriuo siekiama panaikinti tapatybės atsekimo galimybę. Todėl pradinė sąlyga yra ta, kad asmens duomenys turėjo būti renkami ir tvarkomi remiantis taikomais teisės aktais dėl duomenų laikymo ir būti tokio pavidalo, kad būtų galima nustatyti asmens tapatybę.

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (ADTAĮ) 3 straipsnyje pabrėžiama, kad asmens duomenys „... saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi“. To paties įstatymo 12 straipsnyje teigiama, kad „..tais atvejais, kai atliekamiems tyrimams nėra būtini asmens tapatybę nustatantys duomenys, duomenų valdytojas teikia duomenų gavėjui tokius asmens duomenis, iš kurių negalima nustatyti asmens tapatybės“. ADTAĮ 13 straipsnyje teigiama, kad „..ypatingi asmens duomenys statistikos tikslais renkami tik tokia forma, kuri neleistų tiesiogiai ar netiesiogiai nustatyti duomenų subjekto tapatybę, išskyrus įstatymų nustatytus atvejus“. ADTAĮ 13^1 straipsnyje teigiama, kad „..socialinio ir viešosios nuomonės tyrimo tikslais privalo būti renkami tik atliekamam socialiniam ir viešosios nuomonės tyrimui būtini asmens duomenys, panaudoti konkrečiam socialiniam ir viešosios nuomonės tyrimui asmens duomenys turi būti nedelsiant pakeisti taip, kad nebūtų galima nustatyti duomenų subjekto tapatybės“.

Asmens duomenys turėtų būti nuasmeninami standartiniu būdu laikantis įvairių teisės reikalavimų. Jeigu duomenų valdytojas pageidauja išlaikyti tokius asmens duomenis ir pasiekus pirminio arba tolesnio tvarkymo tikslus, nuasmeninimo metodai turėtų būti taikomi taip, kad nesugrąžinamai būtų panaikinta tapatybės nustatymo galimybė.

Nuasmeninimas, kaip tolesnio asmens duomenų tvarkymo atvejis, gali būti laikomas suderinamu su pirminiais tvarkymo tikslais tik tuo atveju, jeigu nuasmeninimo procedūra suteikia galimybę patikimai parengti nuasmenintą informaciją pagal šio dokumento nuostatas. Nuasmeninti duomenys yra tokie anoniminiai duomenys, kurie anksčiau buvo susieti su asmeniu, kurio tapatybė galėjo būti nustatyta, bet dabar nebesuteikiantys tokios galimybės.

Duomenų valdytojai daugiausia dėmesio turėtų skirti konkrečioms priemonėms, kurių prireiktų norint atlikti nuasmeninimo metodui priešingą procedūrą, ypač atsižvelgiant į sąnaudas ir praktinę patirtį, reikalingas toms priemonėms įgyvendinti, taip pat įvertinant jų tikėtinumą bei sudėtingumą. Pavyzdžiui, jie turėtų įvertinti nuasmeninimo pastangas ir sąnaudas (būtino laiko ir išteklių požiūriu) atsižvelgdami į vis didesnę nebrangių techninių priemonių, padedančių nustatyti į duomenų rinkinius įtrauktų asmenų tapatybę, pasiūlą, didėjantį kitų duomenų rinkinių (pvz., parengtų pagal atvirųjų duomenų politiką) viešą prieinamumą ir gausius nevisiško nuasmeninimo pavyzdžius,

susijusius su atitinkamu neigiamu, o kartais ir nepataisomu poveikiu duomenų subjektams. Reikėtų atkreipti dėmesį į tai, kad asmens tapatybės nustatymo rizika ilgainiui gali didėti, be to, ji priklauso nuo informacinių ir ryšių technologijų pažangos.

„Priemonės, kurios galėtų būti naudojamos sprendžiant, ar galima nustatyti asmens tapatybę“, yra priemonės, kuriomis gali pasinaudoti „duomenų valdytojas arba kitas asmuo“. Taigi labai svarbu suprasti, kad tuo atveju, jeigu duomenų valdytojas neištrina pirminių duomenų (kuriais remiantis galima nustatyti asmens tapatybę) įvykio lygmeniu ir jeigu duomenų valdytojas perduoda dalį šio duomenų rinkinio (pvz., pašalinęs arba paslėpęs duomenis, kuriais remiantis galima nustatyti asmens tapatybę), iš tokių duomenų sudarytas duomenų rinkinys vis dar laikytinas asmens duomenimis.

Tik tuo atveju, kai duomenų valdytojas duomenis agreguoja tokiu lygmeniu, kuriuo nebegalima nustatyti individualių įvykių, iš tokių duomenų sudarytas duomenų rinkinys gali būti laikomas anoniminiu. Pavyzdžiui, jeigu organizacija įvykių lygmeniu renka duomenis apie asmenų judėjimą kelionių metu, įvykių lygmens duomenys apie asmenų keliavimo būdą bet kurios šalies požiūriu vis dar bus laikomi asmens duomenimis, jeigu duomenų valdytojas (arba bet kuri kita šalis) tebeturės galimybę gauti pirminius netvarkytus duomenis, net jeigu iš trečiosioms šalims pateikto rinkinio buvo pašalinti tiesioginiai identifikatoriai. Bet jeigu duomenų valdytojas ištrintų netvarkytus duomenis ir trečiosioms šalims pateiktų tik aukštu lygmeniu agreguotus statistikos duomenis, pvz., „X kryptimi pirmadieniais važiuoja 160 proc. daugiau keleivių nei antradieniais“, tai būtų laikoma anoniminiais duomenimis.

Taikant veiksmingą nuasmeninimo sprendimą, panaikinama bet kurios šalies galimybė duomenų rinkinyje išskirti konkretų asmenį susiejant du to duomenų rinkinio (arba dviejų atskirų duomenų rinkinių) įrašus ir gauti kokią nors išvestinę informaciją remiantis šiuo duomenų rinkiniu. Galima teigti, kad norint užtikrinti, jog nebebūtų galima nustatyti duomenų subjekto tapatybės, nepakanka vien tiesiogiai pašalinti identifikavimo elementus. Norint panaikinti galimybę nustatyti asmens tapatybę, dažnai reikės imtis papildomų priemonių, kurios vėlgi priklausys nuo tvarkymo aplinkybių ir tikslų, kuriais numatoma naudoti nuasmenintus duomenis.

Abi nuasmeninimo metodų grupės – duomenų randomizavimas ir apibendrinimas – turi trūkumų, tačiau tam tikromis aplinkybėmis ir sąlygomis kiekviena iš šių grupių gali būti tinkama pageidaujamam tikslui pasiekti, tuo pat metu nepažeidžiant duomenų subjekto privatumo. Asmens tapatybės nustatymas reiškia ne tik galimybę sužinoti asmens vardą, pavardę ir (arba) adresą, bet ir galimybę nustatyti asmens tapatybę išskyrimo, susiejimo arba išvadų darymo būdu. Be to, duomenų apsaugos teisės aktų taikymo požiūriu nėra svarbu, kokie yra duomenų valdytojo arba gavėjo ketinimai. Jeigu, remiantis duomenimis, galima nustatyti asmens tapatybę, vadinasi, taikytini duomenų apsaugos reikalavimai.

Kai duomenų rinkinį, kuriam buvo pritaikytas koks nors nuasmeninimo metodas (nuasmeninimą atliko ir duomenis paskelbė pirminių duomenų valdytojas) tvarko trečioji šalis, tai ji gali teisėtai daryti neatsižvelgdama į duomenų apsaugos reikalavimus, jeigu ji neturi galimybės (tiesiogiai arba netiesiogiai) nustatyti į pirminį duomenų rinkinį įtrauktų duomenų subjektų tapatybės. Tačiau trečiosios šalys, priimdamos sprendimą, kaip naudoti ir – svarbiausia – derinti tokius nuasmenintus duomenis siekiant savo tikslų, privalo atsižvelgti į pirmiau minėtas aplinkybes ir sąlygas (įskaitant konkrečias pirminių duomenų valdytojo taikomų nuasmeninimo metodų ypatybes), nes dėl susijusių padarinių joms gali būti taikoma skirtinga atsakomybė. Jeigu dėl minėtų veiksnių kyla nepriimtina duomenų subjektų tapatybės nustatymo rizika, tokiu atveju tvarkymui ir vėl bus taikomi duomenų apsaugos teisės aktai.

Svarstydami nuasmeninimo metodų taikymo galimybes, duomenų valdytojai turi atsižvelgti į šiuos rizikos veiksnius:

- dažnai klaidingai manoma, kad pseudonimais užkoduoti duomenys ir nuasmeninti duomenys yra lygiaverčiai. „Techninės analizės ir metodų patikimumo“ skyriuje bus paaiškinta, kad pseudonimais užkoduotų duomenų negalima prilyginti nuasmenintai informacijai, nes, naudojantis tokiais duomenimis, išlieka galimybė išskirti pavienį duomenų subjektą ir jį susieti su įvairiais duomenų rinkiniais. Suteikiant pseudonimą, veikiausiai bus įmanoma nustatyti asmens tapatybę,

todėl tokiems duomenims taikoma teisinė duomenų apsaugos sistema. Tai ypač aktualu mokslinių, statistinių arba istorinių tyrimų atveju;

- kita klaida – manyti, kad jeigu duomenys buvo tinkamai nuasmeninti (buvo įvykdytos visos pirmiau nurodytos sąlygos ir kriterijai), asmenims nebetaikomos jokios apsaugos priemonės. Taip manyti klaidinga dėl to, kad šiems duomenims gali būti taikomi kiti teisės aktai.
- trečia klaida susijusi su poveikio, kurį tam tikromis aplinkybėmis pavieniams asmenims gali padaryti tinkamai nuasmeninti duomenys, nepaisymu, ypač profiliavimo atveju. Todėl, net jei tokio tipo duomenims būtų nebetaikomi duomenų apsaugos teisės aktai, dėl trečiosioms šalims pateiktų nuasmenintų duomenų rinkinių naudojimo gali nukentėti privatumas. Jeigu nuasmeninta informacija (dažnai susieta su kitais duomenimis) naudojamasi priimant sprendimus, darančius poveikį (nors ir netiesioginį) pavieniams asmenims, ji turi būti tvarkoma labai apdairiai.

TECHNINĖ ANALIZĖ IR METODŲ PATIKIMUMAS

Yra įvairių praktinių nuasmeninimo būdų ir metodų, jų patikimumas skirtingas. Aptarsime pagrindinius aspektus, į kuriuos turėtų atsižvelgti šiuos metodus taikantys duomenų valdytojai. Pirmiausia jie turi įvertinti garantijas, kurias galima suteikti konkrečiu metodu, atsižvelgiant į esamą technologijų lygį ir įvertinant tris labai svarbius nuasmeninimo požiūriu rizikos veiksnius:

- *išskyrimo galimybę* (angl. *singling out*), t. y. galimybę išskirti kai kuriuos arba visus įrašus, pagal kuriuos būtų galima nustatyti į duomenų rinkinį įtraukto asmens tapatybę;
- *susiejimo galimybę* (angl. *linkability*), t. y. galimybę susieti bent du įrašus, susijusius su tuo pačiu duomenų subjektu arba ta pačia duomenų subjektų grupe (toje pačioje duomenų bazėje arba dviejose skirtingose duomenų bazėse). Jeigu išpuolio vykdytojas gali nustatyti (pvz., atlikdamas koreliavimo analizę), kad du įrašai priskirti tai pačiai asmenų grupei, tačiau negali iš tos grupės išskirti pavienių asmenų, tai šiuo metodu apsaugoma nuo išskyrimo, bet neužtikrinama apsauga nuo susiejimo;
- *išvados padarymo galimybę* (angl. *inference*), t. y. galimybę dedukcijos būdu gana tikėtinai nustatyti požymio vertę remiantis kitų požymių rinkinio vertėmis.

Taigi sprendimu, padedančiu apsisaugoti nuo šių trijų rizikos veiksnių, būtų patikimai panaikinta galimybė iš naujo nustatyti asmens tapatybę labiausiai tikėtinomis duomenų valdytojų arba kurios nors trečiosios šalies pasitelktinomis priemonėmis. Asmens tapatybės nustatymo galimybės panaikinimo ir nuasmeninimo metodai yra šiuo metu atliekamų mokslinių tyrimų objektas ir kad tokie tyrimai visuomet parodydavo, jog nėra metodo, kuris neturėtų trūkumų. Plačiąja prasme yra du skirtingi nuasmeninimo būdai: pirmasis grindžiamas ***randomizavimo***, antrasis – ***apibendrinimo*** principu. Šioje rekomendacijoje aptariami ir kiti principai, pvz., *pseudonimų suteikimo, diferencinio privatumo, l įvairovės, t tankio*.

Toliau paaiškinsime vartojamas sąvokas. Duomenų rinkinys būna sudarytas iš skirtingų įrašų, susijusių su pavieniais asmenimis (duomenų subjektais). Kiekvienas įrašas susietas su vienu duomenų subjektu ir yra sudarytas iš kiekvienam požymiui (pvz., metai) priskirtų verčių, dar vadinamų įvesties elementais (pvz., 2013). Duomenų rinkinys – tai įrašų rinkinys, kurį taip pat galima pateikti lentelės (arba lentelių rinkinio) ar diagramos su pastabomis ir (arba) svorinėmis vertėmis, kaip tai dabar vis dažniau daroma, pavidalu. Požymių, susijusių su duomenų subjektu arba duomenų subjektų grupe, deriniai gali būti vadinami kvaziidentifikatoriais. Kartais duomenų rinkinyje gali būti daug įrašų, susijusių su tuo pačiu asmeniu. Išpuolio vykdytojas – tai trečioji šalis (t. y. ne duomenų valdytojas ir ne duomenų tvarkytojas), netyčia arba tyčia mėginanti gauti pirminius duomenis.

1. Randomizavimas (angl. *randomization*)

Randomizavimas – tai metodų, kuriais keičiamas duomenų tikrumas siekiant panaikinti aiškią duomenų ir asmens sąsają, grupė. Kai duomenys yra gana nekonkretūs, jų nebegalima susieti su konkrečiu asmeniu. Taikant randomizavimą, atskirų įrašų savitumas nemažėja, nes kiekvienas

įrašas vis viena bus išvedamas pagal atskirą duomenų subjektą, tačiau šiuo būdu užtikrinama apsauga nuo išvestinės informacijos gavimo išpuolių ir (arba) rizikos ir jį, siekiant suteikti didesnę privatumo garantiją, galima derinti su apibendrinimu. Norint užtikrinti, kad, remiantis įrašu, nebūtų galima nustatyti pavienio asmens tapatybės, gali prireikti papildomų metodų.

1.1. Iškraipytų duomenų įterpimas (angl. *noise addition*)

Iškraipytų duomenų įterpimo metodas pirmiausia naudingas tada, kai požymiai gali turėti reikšmingą neigiamą poveikį asmenims. Šio metodo esmė – į duomenų rinkinį įtrauktų požymių pakeitimas sumažinant jų tikslumą, tačiau išsaugant bendrą pasiskirstymą. Tvarkydamas duomenų rinkinį, stebėtojas manys, kad vertės yra tikslios, bet tai bus teisinga tik iš dalies. Pavyzdžiui, jeigu asmens ūgis iš pradžių buvo išmatuotas centimetrų tikslumu, nuasmenintame duomenų rinkinyje ūgis gali būti nurodomas tik ±10 cm tikslumu. Jeigu šis metodas bus taikomas veiksmingai, trečioji šalis negalės nustatyti asmens tapatybės ir neturėtų galėti ištaisyti duomenis arba kaip nors kitaip nustatyti, kaip duomenys buvo pakeisti. Iškraipytų duomenų įterpimą paprastai reikia derinti su kitais nuasmeninimo metodais, pvz., su akivaizdžių požymių ir kvaziidentifikatorių pašalinimu. Iškraipymo laipsnis turėtų priklausyti nuo to, kokio lygio informacija yra reikalinga, ir nuo apsaugotų požymių atskleidimo daromo poveikio asmenų privatumui.

1.2. Perstatymas (angl. *permutation*)

Taikant šį metodą, lentelėje esančių požymių vertės sukeičiamos vietomis taip, kad kai kurios iš jų būtų dirbtinai susietos su kitais duomenų subjektais. Tai naudinga, kai svarbu išsaugoti tikslų kiekvieno į duomenų rinkinį įtraukto požymio pasiskirstymą.

Perstatymas gali būti laikomas savita iškraipytų duomenų įterpimo rūšimi. Pagal klasikinį iškraipytų duomenų įterpimo metodą požymiai pakeičiami pasirenkant atsitiktines vertes. Dėsningai iškraipytų duomenų įterpimas gali būti sunkiai įvykdomas uždavinys, o nedaug pakeičiant požymių vertes gali būti neužtikrintas pakankamas privatumas. Perstatymo metodas – tai alternatyva, kurią taikant duomenų rinkinio vertės pakeičiamos tiesiog sumaišant vietomis skirtingų įrašų vertes. Tokiu sukeitimu užtikrinama, kad verčių intervalas ir paskirstymas išliktų tokie patys, o verčių ir asmenų koreliacijos pasikeistų. Jeigu dviem arba daugiau požymių būdingas loginis tarpusavio ryšys arba statistinė koreliacija ir atliekamas nepriklausomas jų perstatymas, toks ryšys sunaikinamas. Todėl gali būti svarbu susijusių požymių rinkinio perstatymą atlikti taip, kad nebūtų pažeistas loginis tarpusavio ryšys, nes kitaip išpuolio vykdytojas galėtų nustatyti sukeistus požymius ir atlikti atvirkštinį perstatymą.

Tarkime, medicinos duomenų rinkinyje yra požymių poaibis „hospitalizavimo priežastys, simptomai, atsakingas skyrius“; dažniausiai tarp šių verčių bus stiprus loginis ryšys, todėl, atlikus tik vienos iš šių verčių perstatymą, ją bus galima nustatyti ir gal netgi atlikti atvirkštinį perstatymą.

Panašiai kaip ir iškraipytų duomenų įterpimo atveju, vien perstatymo pritaikymas gali neužtikrinti nuasmeninimo, todėl jis visada turėtų būti derinamas su akivaizdžių požymių ir (arba) kvaziidentifikatorių pašalinimu.

1.3. Diferencinis privatumas (angl. *differential privacy*)

Diferencinis privatumas priskiriamas randomizavimo metodų grupei, tačiau jis pagrįstas kitokiu principu: iškraipytų duomenų įterpimas taikytinas prieš paskelbiant duomenų rinkinį, o diferencinio privatumo metodas gali būti taikomas, kai duomenų valdytojas parengia nuasmenintus duomenų rodinius, išsaugodamas pirminių duomenų kopiją. Tokie nuasmeninti rodiniai paprastai parengiami naudojant užklausų poaibį, skirtą tam tikrai trečiajai šaliai. Į šį poaibį vėliau sąmoningai įtraukiami atsitiktiniai iškraipyti duomenys. Taikydamas diferencinio privatumo metodą, duomenų valdytojas sužino, kiek iškraipytų duomenų jis turėtų įterpti ir kokiu pavidalu, kad užtikrintų reikiamas privatumo garantijas. Šiuo atveju labai svarbu nuolat stebėti (ne rečiau kaip kiekvienos

naujos užklausos atveju), ar neatsirado galimybė nustatyti asmens tapatybę pasinaudojant užklausos rezultatų aibe. Be to, derėtų paaiškinti, kad diferencinio privatumo metodu pirminiai duomenys nepakeičiami, o kol jie išlieka, duomenų valdytojas, atsižvelgdamas į visas galimas pasitelktinas priemones, asmens tapatybę gali nustatyti pasinaudodamas diferencinio privatumo užklausų rezultatais. Šie rezultatai taip pat turėtų būti laikomi asmens duomenimis.

Vienas iš diferenciniu privatumu pagrįsto metodo privalumų yra tas, kad duomenų rinkiniai įgaliotosioms trečiosioms šalims teikiami pagal konkrečias užklausas, o ne paskelbiant visą duomenų rinkinį. Kad būtų lengviau atlikti auditą, duomenų valdytojas gali išsaugoti visų užklausų ir prašymų sąrašą, taip užtikrindamas, kad trečiosios šalys negautų duomenų, su kuriais jos neturi teisės susipažinti. Be to, norint geriau apsaugoti privatumą, užklausai gali būti taikomi nuasmeninimo, pvz., iškraipytų duomenų įterpimo arba pakeitimo, metodai. Tyrinėtojams dar nepavyko sukurti gero interaktyvaus užklausų ir jų rezultatų teikimo mechanizmo, kurį naudojant būtų galima ir gana tiksliai (t. y. kuo mažiau iškraipant duomenis) atsakyti į visas užklausas, ir apsaugoti privatumą.

Siekiant apriboti išvados padarymo ir susiejimo išpuolių galimybę, būtina sekti subjektų teikiamas užklausas ir stebėti apie duomenų subjektus gautą informaciją; todėl diferencinio privatumo metodu valdomos duomenų bazės neturėtų būti prieinamos viešoms paieškos sistemoms, kuriose nėra užklausas teikiančių subjektų sekimo galimybės.

2. Apibendrinimas (angl. *generalization*)

Apibendrinimas yra antroji nuasmeninimo metodų grupė. Pagal šį principą duomenų subjektų požymiai apibendrinami arba, kitaip tariant, susilpninami, kiek pakeičiant atitinkamą mastelį arba dydžio eilę (pvz., informaciją pateikiant ne miesto, o regiono mastu, mėnesio, o ne savaitės apimtimi). Nors apibendrinimas, siekiant panaikinti išskyrimo galimybę, ir gali būti veiksmingas, ne visais atvejais šiuo principu užtikrinamas tinkamas nuasmeninimas; pirmiausia, taikant šį principą, būtina pasitelkti specialius sudėtingus kiekybinius metodus, kuriais būtų panaikinta susiejimo ir išvados padarymo galimybė.

2.1. Agregavimas ir k anonimiškumas (angl. *aggregation* ir *k-anonymity*)

Agregavimo ir *k* anonimiškumo metodais siekiama panaikinti galimybę išskirti duomenų subjektus, juos grupuojant kartu su ne mažiau kaip *k* kitų asmenų. Šiuo tikslu požymių vertės apibendrinamos tokiu mastu, kad kiekvienam asmeniui būtų priskirta tokia pat vertė. Pavyzdžiui, vietovės mastelį pastambinus nuo miesto iki šalies, bus įtraukta daugiau duomenų subjektų. Pavienių asmenų gimimo datos gali būti apibendrintos datų intervalais arba sugrupuotos pagal mėnesius arba metus. Kitus skaitinius požymius (pvz., darbo užmokestį, svorį, ūgį, vaisto dozę) galima apibendrinti verčių intervalais (pvz., darbo užmokestis nuo 20 000 iki 30 000 EUR). Šie metodai gali būti taikomi tada, kai dėl požymių tikslių verčių koreliacijos gali susidaryti kvaziindikatoriai.

2.2. l įvairovė ir t tankis (angl. *l-diversity* ir *t-closeness*)

l įvairovės metodu išplečiamas *k* anonimiškumo metodas, siekiant užtikrinti, kad nebebūtų galima rengti determinavimo būdu pagrįstų išpuolių, pasirūpinant, kad kiekvienoje lygiavertiškumo klasėje kiekvienam požymiui būtų priskirta ne mažiau kaip *l* skirtingų verčių.

Vienas iš pagrindinių siektinų tikslų – riboti lygiavertiškumo klasių, kurioms būtų būdingas menkas požymių kintamumas, susidarymą, kad bendrųjų žinių apie tam tikrą duomenų subjektą turinčiam išpuolio vykdytojui visada liktų didelių abejonių dėl savo išvadų.

l įvairovės metodas naudingas norint apsaugoti duomenis nuo išpuolių siekiant gauti išvestinių duomenų, kai požymių vertės yra gerai pasiskirsčiusios. Tačiau reikia pabrėžti, kad šiuo metodu negalima panaikinti informacijos nutekinimo galimybės, jeigu požymiai skaidinyje pasiskirstę netolygiai arba priklauso mažam verčių arba reikšminių verčių intervalui. Todėl *l* įvairovės metodas neapsaugo nuo tikimybinio išvadų darymo išpuolių.

t tankio metodas yra patobulintas *l* įvairovės metodas, nes juo siekiama sudaryti lygiavertiškumo klases, kurioms būtų būdingas panašus į pirminį požymių pasiskirstymas lentelėje. Šis metodas naudingas tada, kai svarbu, kad duomenys būtų kuo panašesni į pirminius, todėl lygiavertiškumo klasei taikomas papildomas apribojimas, pagal kurį kiekvienoje lygiavertiškumo klasėje turėtų būti ne tik mažiau kaip *l* skirtingų verčių, bet ir kiekviena vertė turi būti pateikta tiek kartų, kiek reikalinga tam, kad būtų atkurtas pirminis kiekvieno požymio pasiskirstymas.

3. Pseudonimų suteikimas (angl. *pseudonymisation*)

Pseudonimų suteikimas – tai metodas, pagal kurį vienas požymis (paprastai – unikalus) įraše pakeičiamas kitu. Todėl išlieka galimybė netiesiogiai nustatyti fizinio asmens tapatybę; taigi vien pseudonimų suteikimas neužtikrina duomenų rinkinio anonimiškumo. Vis dėlto šis metodas vis tiek aptariamas, nes su jo taikymu susiję dažni nesusipratimai ir klaidos.

Taikant pseudonimų suteikimo metodą, sumažinama galimybė duomenų rinkinį susieti su pirmine duomenų subjekto tapatybe; taigi šis metodas yra naudinga saugumo priemonė, bet tai nėra nuasmeninimo metodas.

Pseudonimų suteikimo rezultatas gali nepriklausyti nuo pirminės vertės (pvz., jeigu tai atsitiktinis duomenų valdytojo sugeneruotas skaičius arba duomenų subjekto pasirinkta pavardė) arba gali būti sukuriamas naudojantis požymio arba jų grupės pirminėmis vertėmis, pvz., taikant maišos funkciją arba šifravimo sistemą.

Toliau aprašyti dažniausiai taikomi pseudonimų suteikimo metodai.

- Šifravimas naudojant slaptą raktą (angl. *encryption with secret key*): šiuo atveju raktą turintis asmuo gali nesunkiai atkurti kiekvieno duomenų subjekto tapatybę dešifravęs duomenų rinkinį, nes asmens duomenys, nors ir užšifruoti, tebėra duomenų rinkinyje. Jeigu buvo pritaikyta pažangi šifravimo sistema, dešifravimas galimas tik žinant raktą.
- Maišos funkcija (angl. *hash function*): tai – funkcija, kuri iš bet kokio dydžio įvesties duomenų (tai gali būti vienas požymis arba požymių rinkinys) parengia nustatyto dydžio išvesties duomenis ir kurios negalima atlikti priešinga kryptimi; tai reiškia, kad nebelieka pakartotinio tapatybės nustatymo rizikos, būdingos šifravimui. Tačiau, jeigu yra žinomas maišos funkcijos įvesties verčių intervalas, šioms vertėms galima pakartotinai pritaikyti maišos funkciją ir taip gauti teisingą tam tikro įrašo vertę. Pavyzdžiui, jeigu duomenų rinkiniui buvo pritaikytas pseudonimų suteikimo metodas, pagrįstas nacionalinių asmens tapatybės kodų maišos funkcija, tuomet šiuos kodus galima nustatyti tiesiog pritaikant maišos funkciją visoms galimoms įvesties vertėms ir rezultatą palyginant su duomenų rinkinyje esančiomis vertėmis. Maišos funkcijos paprastai yra skirtos palyginti greitam skaičiavimui ir nėra atsparios jėgos metodo išpuoliams. Kad būtų galima masiškai atkurti didelį verčių, kurioms buvo pritaikyta maišos funkcija, rinkinį, taip pat gali būti parengiamos iš anksto apskaičiuotų verčių lentelės.
- Taikant „druskos“ naudojimu pagrįstą maišos funkciją (angl. *salted-hash function*) (prie požymio, kuriam taikoma maišos funkcija, pridedama atsitiktinė vertė, vadinama „druska“), galima sumažinti įvesties vertės nustatymo tikimybę, tačiau pagrįstomis priemonėmis vis vien gali būti įmanoma apskaičiuoti pirminę požymio vertę, paslėptą sudėtingesnės maišos funkcijos (su „druskos“ elementu) rezultatu.
- Saugomo rakto naudojimu pagrįsta maišos funkcija (angl. *keyed-hash function with stored key*): tai tam tikra maišos funkcija, kai naudojamas papildomas įvesties elementas – slaptas raktas (ši funkcija nuo „druskos“ naudojimu pagrįstos funkcijos skiriasi tuo, kad „druska“ paprastai nėra slaptas elementas). Duomenų valdytojas, naudodamas slaptą raktą, šią funkciją gali pakartotinai pritaikyti požymiui, tačiau išpuolio vykdytojui tampa gerokai sunkiau pakartoti šią funkciją nežinant rakto, nes mėgintinų variantų skaičius yra per didelis, kad būtų įmanoma tai padaryti.
- Determinavimu pagrįstas šifravimas arba panaikinamo rakto naudojimu pagrįsta maišos funkcija (angl. *deterministic encryption or keyed-hash function with deletion of the key*): pagal šį metodą kiekvienam duomenų rinkinyje esančiam požymiui kaip pseudonimas gali būti parenkamas atsitiktinis skaičius, o tada panaikinama atitikties lentelė. Pasitelkus tokį sprendimą, galima sumažinti

galimybę duomenų rinkinyje esančius asmens duomenis susieti su kitame duomenų rinkinyje, kuriame naudojamas kitoks pseudonimas, esančiais duomenimis apie tą patį asmenį. Skaičiavimo požiūriu išpuolio vykdytojui, pasitelkusiam net ir pažangų algoritmą, būtų sunku iššifruoti arba pakartoti funkciją, nes, neturint rakto, reikėtų išmėginti kiekvieną galimą raktą.

- Pakaitinių simbolių naudojimas (angl. *tokenization*): šis metodas paprastai taikomas (nors gali būti taikomas ir kitur) finansų sektoriuje, siekiant kortelių atpažinimo numerius (angl. *ID*) pakeisti vertėmis, kurios išpuolio vykdytojui būtų ne tokios naudingos. Šis metodas sukurtas remiantis pirmiau aptartais metodais ir paprastai grindžiamas vienakrypčių šifravimo priemonių taikymu arba eilės numerio ar atsitiktine tvarka sugeneruoto numerio, kuris nėra matematiškai gaunamas iš pirminių duomenų, priskyrimu pasitelkiant indeksavimo funkciją.

4. Dažnos klaidos

- Manymas, kad pseudonimais užkoduotas duomenų rinkinys yra nuasmenintas: duomenų valdytojai dažnai mano, kad vieno arba daugiau požymių pašalinimas arba pakeitimas yra pakankama duomenų nuasmeninimo priemonė. Daugybė pavyzdžių rodo, kad taip nėra; vien tik pakeitus identifikatorių nepanaikinama galimybė nustatyti duomenų subjekto tapatybę, jeigu duomenų rinkinyje lieka kvaziidentifikatorių arba jeigu asmens tapatybę vis dar galima nustatyti pasinaudojant kitų požymių vertėmis. Nustatyti asmens tapatybę pseudonimais užkoduotame duomenų rinkinyje gali būti taip pat lengva, kaip ir pasinaudojant pirminiais duomenimis. Kad duomenų rinkinį būtų galima laikyti nuasmenintu, reikėtų imtis papildomų priemonių, įskaitant požymių pašalinimą arba apibendrinimą arba pirminių duomenų ištrynimą ar bent jau jų agregavimą aukštesniu lygmeniu.
- Su pseudonimų suteikimu, kuriuo siekiama sumažinti susiejimo galimybę, susijusios dažnos klaidos:

- to paties rakto naudojimas skirtingose duomenų bazėse: skirtingų duomenų bazių susiejimo galimybės pašalinimas labai priklauso nuo to, ar naudojamas raktu pagrįstas algoritmas ir ar pavienis asmuo įvairiomis aplinkybėmis atitinka skirtingus pseudonimais užkoduotus požymius. Taigi, norint sumažinti susiejimo galimybę, svarbu vengti skirtingose duomenų bazėse naudoti tokį patį raktą;
- skirtingų (kaitaliojamų) raktų suteikimas skirtingiems naudotojams: gali būti patrauklu skirtingoms naudotojų grupėms suteikti skirtingus raktus ir keisti raktą, kai jis panaudojamas tam tikrą kartų skaičių (pvz., naudoti tą patį raktą dešimčiai įvesties elementų, susijusių su tuo pačiu naudotoju, įrašyti). Tačiau, jeigu ši operacija bus parengta netinkamai, gali susidaryti tam tikri šablonai, dėl kurių iš dalies sumažės tikėtina nauda. Pavyzdžiui, kaitaliojant raktą pagal tam tikriems asmenims taikomas specialias taisykles, gali būti palengvinta su tais asmenimis susijusių įvesties elementų susiejimo galimybė. Be to, periodinis pseudonimais užkoduotų duomenų dingimas, kai tik atsiranda nauji duomenys, gali būti ženklas, kad abu įrašai susiję su tuo pačiu fiziniu asmeniu;
- rakto laikymas: jeigu slaptas raktas bus saugomas kartu su pseudonimais užkoduotais duomenimis ir duomenys bus nutekinti, išpuolio vykdytojui gali būti lengva susieti pseudonimais užkoduotus duomenis su jų pirminiu požymiu. Tas pats pasakytina apie atvejį, kai raktas laikomas atskirai nuo duomenų, bet nesaugiai.

IŠVADOS IR REKOMENDACIJOS

Išvados

Tapatybės duomenų panaikinimo ir nuasmeninimo metodai yra intensyvių mokslinių tyrimų objektas. Šiame dokumente nuosekliai parodyta, kad kiekvienas metodas turi privalumų ir trūkumų. Dažniausiai neįmanoma pateikti būtinųjų rekomendacijų dėl pasitelktinų parametrų, nes kiekvienas duomenų rinkinys turėtų būti nagrinėjamas atsižvelgiant į konkretų atvejį.

Daugeliu atvejų ir nuasmenintas duomenų rinkinys duomenų subjektams gali kelti liekamąją riziką. Išties, net jeigu nebelieka galimybės iš įrašo išgauti tikslių asmens duomenų, vis tiek įmanoma

surankioti informaciją apie tą asmenį pasinaudojant kitais esamais informacijos šaltiniais (viešais arba neviešais).

Reikėtų pabrėžti, kad netinkamai atliktas nuasmeninimas duomenų subjektams daro ne tik tiesioginį poveikį (nemalonumai, laiko gaišimas ir kontrolės praradimo jausmas, kylantis dėl įtraukimo į grupę nepranešus arba negavus išankstinio sutikimo), gali būti ir kitokių netinkamo nuasmeninimo netiesioginio poveikio padarinių, susijusių su tuo, kad koks nors išpuolio vykdytojas, remdamasis sutvarkytais nuasmenintais duomenimis, duomenų subjektą per klaidą pasirinko savo objektu, ypač jeigu tas išpuolio vykdytojas turi neteisėtų ketinimų.

Todėl pabrėžiama, kad nuasmeninimo metodais galima suteikti privatumo garantijų, tačiau tik tuo atveju, jeigu šių metodų taikymas tinkamai organizuojamas, t. y., norint pasiekti reikiamą nuasmeninimo lygį ir kartu parengti naudingus duomenis, turi būti aiškiai nustatytos nuasmeninimo procedūros prielaidos (aplinkybės) ir tikslas (-ai).

Rekomendacijoje darytina išvada, kad nuasmeninimo metodais galima užtikrinti privatumą ir parengti veiksmingas nuasmeninimo procedūras, tačiau tik tuo atveju, jeigu šių metodų taikymas tinkamai organizuojamas, t. y., norint pasiekti reikiamą nuasmeninimo lygį ir kartu pateikti tam tikrus naudingus duomenis, turi būti tiksliai nustatytos nuasmeninimo procedūros 4 prielaidos (aplinkybės) ir tikslas (-ai). Geriausia, jei sprendimai būtų grindžiami remiantis konkrečiais atvejais, galbūt derinant įvairius metodus ir kartu atsižvelgiant į parengtas praktines rekomendacijas.

Rekomendacijos

- Kai kuriems nuasmeninimo metodams būdingi tam tikri apribojimai. Duomenų valdytojai, norėdami pagal tam tikrą metodą parengti nuasmeninimo procedūrą, iš pradžių turi rimtai įvertinti šiuos apribojimus. Jie privalo atsižvelgti į siekiamus nuasmeninimo tikslus, pvz., apsaugoti asmenų privatumą skelbiant duomenų rinkinį arba sudarant galimybę iš duomenų rinkinio gauti tam tikrą informaciją.
- Visi šiame dokumente aprašyti metodai nevisiškai atitinka veiksmingo nuasmeninimo kriterijus (t. y. asmens išskyrimo galimybės nebuvimo; su asmeniu susijusių įrašų susiejimo galimybės nebuvimo; su asmeniu susijusių išvestinių duomenų gavimo galimybės nebuvimo). Antra vertus, taikant tam tikrą metodą, kai kuriuos iš šių rizikos veiksnių galima visiškai arba iš dalies pašalinti, todėl būtina kruopščiai parengti tinkamą konkretaus metodo taikymo konkrečioje situacijoje procedūrą ir derinti šiuos metodus tarpusavyje, kad būtų gautas patikimas rezultatas.

Toliau pateiktoje lentelėje trijų pagrindinių reikalavimų požiūriu apžvelgiami aptariamų metodų privalumai ir trūkumai.

	Ar išlieka išskyrimo rizika?	Ar išlieka susiejimo rizika?	Ar išlieka išvados padarymo rizika?
Pseudonimų suteikimas	Taip	Taip	Taip
Iškraipytų duomenų įterpimas	Taip	Ne (laikantis tam tikrų sąlygų)	Ne (laikantis tam tikrų sąlygų)
Pakeitimas	Taip	Taip	Ne (laikantis tam tikrų sąlygų)
Agregavimas arba *k* anonimiškumas	Ne	Taip	Taip
l įvairovė	Ne	Taip	Ne (laikantis tam tikrų sąlygų)
Diferencinis privatumas	Ne (laikantis tam tikrų sąlygų)	Ne (laikantis tam tikrų sąlygų)	Ne (laikantis tam tikrų sąlygų)
Maiša ar pakaitinių simbolių naudojimas	Taip	Taip	Ne (laikantis tam tikrų sąlygų)

Lentelė. Aptariamų metodų privalumai ir trūkumai

- Būtų geriausia, jei sprendimai būtų priimami atsižvelgiant į kiekvieną konkretų atvejį. Radus sprendimą (t. y. nustačius išsamią nuasmeninimo procedūrą), atitinkantį šiuos tris kriterijus, būtų patikimai panaikinta galimybė nustatyti asmens tapatybę labiausiai tikėtinomis priemonėmis, kurias galėtų pasitelkti duomenų valdytojas arba kokia nors trečioji šalis.
- Kai pasiūlymas neatitinka kurio nors iš šių kriterijų, turėtų būti atliekamas išsamus asmens tapatybės nustatymo rizikos vertinimas. Norint sumažinti asmens tapatybės nustatymo riziką, reikėtų atsižvelgti į toliau aprašytą gerąją patirtį.

Geroji nuasmeninimo patirtis

Bendrieji patarimai

Nesivadovaukite principu „paskelbk ir pamiršk“. Atsižvelgdami į liekamąją asmens tapatybės nustatymo riziką, duomenų valdytojai turėtų:

- reguliariai nustatyti naują riziką ir atlikti pakartotinius liekamosios rizikos vertinimus;
- vertinti, ar nustatytos rizikos valdymo priemonės yra pakankamos, ir imtis atitinkamų taisomųjų veiksmų;
- stebėti ir valdyti riziką.

Vertindami liekamąją riziką, atsižvelkite į galimybę nustatyti asmens tapatybę, remiantis nenuasmeninta duomenų rinkinio dalimi (jeigu tokia yra), ypač jeigu ši dalis būtų sujungta su nuasmeninta dalimi, ir į galimą požymių (pvz., geografinės vietovės ir turto duomenų) koreliaciją.

Su aplinkybėmis susiję veiksniai

- Turėtų būti aiškiai išdėstyti duomenų rinkinio nuasmeninimo tikslai, nes jie yra labai svarbūs vertinant asmens tapatybės nustatymo riziką.
- Šiuo tikslu taip pat turėtų būti atsižvelgta į visus svarbius su aplinkybėmis susijusius veiksnius, pvz., pirminių duomenų pobūdį, taikomas kontrolės priemones (įskaitant saugumo priemones, kuriomis ribojama galimybė naudotis duomenų rinkiniais), imties dydį (kiekybines charakteristikas), viešų informacijos šaltinių (kuriais galėtų remtis gavėjai) buvimą, numatomą duomenų teikimą trečiosioms šalims (ribotas, neribotas, pvz., internetu, ir t. t.).

- Turėtų būti aptarti galimi išpuolio vykdytojai, atsižvelgiant į duomenų patrauklumą tiksliniams išpuoliams (šiuo požiūriu taip pat labai svarbu įvertinti informacijos slaptumą ir duomenų pobūdį).

Techniniai aspektai

- Duomenų valdytojai turėtų nurodyti taikomą nuasmeninimo metodą arba jų rinkinį, ypač jeigu nuasmenintą duomenų rinkinį jie ketina paskelbti.
- Akivaizdūs (pvz., reti) požymiai ir (arba) kvaziidentifikatoriai turėtų būti pašalinti iš duomenų rinkinio.
- Jeigu taikomas iškraipytų duomenų įterpimo metodas (atliekant randomizavimą), įrašams taikytinas iškraipymo lygis turėtų būti nustatomas atsižvelgiant į požymio vertę (t. y. neturėtų būti įterpiami pernelyg iškraipyti duomenys), požymių, kuriuos reikia apsaugoti, poveikį duomenų subjektams ir (arba) duomenų rinkinio retumą.
- Jeigu remiamasi diferencinio privatumo metodu (atliekant randomizavimą), turėtų būti atsižvelgiama į būtinybę stebėti užklausas ir nustatyti privatumą pažeidžiančias užklausas, įvertinus jų kaupiamąjį poveikį.
- Jeigu taikomi apibendrinimo principu pagrįsti metodai, labai svarbu, kad duomenų valdytojas neapsiribotų vienu apibendrinimo kriterijumi, net jeigu jis būtų taikomas tam pačiam požymiui, kitaip tariant, turėtų būti parenkami įvairūs masteliai arba įvairūs laiko intervalai. Parenkant taikytiną kriterijų, turi būti remiamasi požymių verčių paskirstymu nagrinėjamoje aibėje. Reikėtų užtikrinti kintamumą lygiavertiškumo klasėse, pvz., atsižvelgiant į pirmiau minėtus su aplinkybėmis susijusius veiksnius (imties dydį ir t. t.), turėtų būti parinkta tam tikra ribinė vertė, ir, jeigu ji nėra pasiekta, atitinkama imtis turėtų būti atmesta (arba turėtų būti nustatytas kitoks apibendrinimo kriterijus).

Nemokama nuasmeninimo programinė įranga:

- „Anonimatron“. Adresas internete: http://anonimatron.sourceforge.net/Anonimatron/Anonimatron.html;
- „Data Anonymizer“. Adresas internete: http://www.softpedia.com/get/Internet/Servers/Database-Utils/Data-Anonymizer.shtml.

Parengė Valstybinės duomenų apsaugos inspekcijos
Informacijos ir technologijų skyriaus vyr. specialistas Valdas Šulinskas
Inspekcijos adresas internete *www.ada.lt*

Rekomendacija parengta remiantis Europos Komisijos 29 straipsnio duomenų apsaugos darbo grupės parengta Nuomone 05/2014 dėl nuasmeninimo metodų.

Adresas internete: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*