ASMENS DUOMENŲ APSAUGOS GAIRĖS SMULKIAJAM IR VIDUTINIAM VERSLUI

„SolPriPa“ projekto gairės

Gairių parengimas finansuotas pagal Europos Sąjungos Teisių, lygybės ir pilietiškumo programą (2014–2020).

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

MYKOLO ROMERIO UNIVERSITETAS

Vilnius, 2019 m.

Solving Privacy Paradox

Sprendžiant privatumo paradoksą: asmens duomenų apsaugos, kaip pagrindinės teisės ir vieno iš svarbiausių vartotojų pasitikėjimo skaitmenine ekonomika veiksnių, aukštų standartų skatinimas („SolPriPa“ projektas)

2018 m. rugsėjo 17 d. Lietuvoje startavo 2 metų trukmės Valstybinės duomenų apsaugos inspekcijos ir Mykolo Romerio universiteto iš dalies Europos Sąjungos lėšomis finansuojamas Lietuvos aukštų asmens duomenų apsaugos standartų skatinimo projektas SolPriPa.

Tikslai. Tobulinti projekto partnerių neformaliojo išsilavinimo institucinius ir organizacinius gebėjimus; skatinti organizacijas pagerinti verslo veiklos valdymą asmens duomenų apsaugos srityje; didinti visuomenės informuotumą apie duomenų apsaugos problemas ir skatinti netoleranciją piktnaudžiavimui asmens duomenimis; skatinti socialinį solidarumą ir jaunimo pilietiškumą, ugdyti jų pilietiškumo kompetenciją, būtiną aktyviam ir atsakingam dalyvavimui nuolat kintančioje visuomenėje.

Veiklos. Įgyvendinant SolPriPa projektą numatyta vesti mokymus, parengti įvairių mokymo priemonių, skirtų geriau įsisavinti mokymų medžiagą, rengti informuotumo didinimo seminarus ir kitas priemones skirtingų tikslinių grupių nariams, pavyzdžiui, konkursas jaunimui ir programėlės sukūrimas.

Tikslinės grupės: smulkaus ir vidutinio verslo atstovai, startuoliai, sveikatos priežiūros ir žiniasklaidos sektoriai, pažeidžiamesnės visuomenės grupės, tokios kaip jaunimas ar vyresnio amžiaus žmonės.

SANTRUMPOS

BDAR – nuo 2018 m. gegužės 25 d. pradėtas taikyti 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)

DAP – duomenų apsaugos pareigūnas

Duomenų subjektas – fizinis asmuo, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti

EDAV – Europos duomenų apsaugos valdyba

29 straipsnio darbo grupė – pagal 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo 29 straipsnį sudaryta 29 straipsnio duomenų apsaugos darbo grupė

ES – Europos Sąjunga

EEE – Europos Ekonominė Erdvė

VDAI – Valstybinė duomenų apsaugos inspekcija

PDAV – poveikio duomenų apsaugai vertinimas

TURINYS

ĮŽANGA

Nuo 2018 m. gegužės 25 d. pradėtas taikyti 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Šiame reglamente išdėstomos fizinio asmens teisės ir nustatomos duomenis tvarkančių ir už jų tvarkymą atsakingų subjektų – duomenų valdytojų ir duomenų tvarkytojų, pareigos. Jame taip pat nustatomi šių taisyklių laikymosi užtikrinimo metodai ir sankcijų už taisyklių pažeidimą taikymas.

BDAR yra **tiesioginio taikymo** Europos Sąjungos teisės aktas. Be BDAR tam tikrus asmens duomenų tvarkymo ypatumus nustato ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Taigi duomenų valdytojai ir duomenų tvarkytojai privalo užtikrinti, kad asmens duomenų tvarkymas atitiktų šiais teisės aktais nustatytas taisykles.

BDAR taikymas priklauso **ne nuo įmonės dydžio**, bet nuo atliekamo asmens duomenų tvarkymo pobūdžio. Kita vertus, ne visos BDAR nustatytos prievolės taikomos smulkiajam ir vidutiniam verslui, pvz., įmonėms, kuriose dirba mažiau kaip 250 darbuotojų, nereikia tvarkyti duomenų tvarkymo veiklos įrašų (išskyrus numatytas išimtis), ne visos įmonės turi paskirti duomenų apsaugos pareigūną ir t. t.

Šiomis gairėmis[1] siekiama supažindinti smulkiojo ir vidutinio verslo subjektus su BDAR reikalavimais, paaiškinant juos, remiantis aktualia jų taikymo praktika ir taikymo pavyzdžiais.

Norint geriau suprasti BDAR reikalavimus ir kaip juos tinkamai įgyvendinti praktikoje, taip pat rekomenduojame susipažinti su 29 straipsnio darbo grupės gairėmis, ją nuo 2018 m. gegužės 25 d. pakeitusios Europos duomenų apsaugos valdybos parengtomis gairėmis bei Valstybinės duomenų apsaugos metodiniais dokumentais, kuriuos galite rasti šiais adresais:

- http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360;
- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm;
- https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en;

https://vdai.lrv.lt/lt/informacija-visuomenei/rekomendacijos-gaires-ir-kt.

ASMENS DUOMENŲ SĄVOKA

BDAR pateikiama asmens duomenų sąvoka. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma, pagal identifikatorių, kaip antai, vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

KAS LAIKOMA ASMENS DUOMENIMIS?

Pagal BDAR pateikiamą „asmens duomenų“ sąvoką, asmens duomenys yra:

1. Bet kokia informacija, susijusi su asmeniu;
2. Informacija, susijusi su gyvu asmeniu;
3. Informacija apie asmenį, kurio tapatybė yra nustatyta arba gali būti nustatyta.

- Dėl plataus apibrėžimo net ir lengvai gaunama, iš pirmo žvilgsnio neesminė, **bet susijusi su fiziniu asmeniu informacija**, laikytina asmens duomenimis. Sąvoka „informacija“ apima garso, vaizdo,

[1] Rengiant metodinę medžiaga remtasi BDAR, Europos Komisijos pateikiama informacija, Europos duomenų apsaugos valdybos gairėmis, 29 straipsnio darbo grupės gairėmis ir kitų šalių praktika.

genetinius duomenis, pirštų atspaudus ir t. t. Ši informacija gali būti pateikiama raidėmis, skaičiais, grafiniu, fotografiniu vaizdu, garsu (telefonu) ir kitomis formomis.

- Asmens tapatybė gali būti nustatyta tiesiogiai arba netiesiogiai iš duomenų, susijusių su kita informacija, kurią turi arba gali gauti įmonė.

Asmens tapatybė gali būti **nustatyta** pagal **tiesiogiai** asmenį identifikuojančius duomenis (pvz., vardą ir pavardę, asmens kodą ir pan.) arba **netiesiogiai**, t. y. kai turimų duomenų nepakanka konkrečiam asmeniui nustatyti, tačiau asmens tapatybę galima nustatyti panaudojant kitus duomenis, nepaisant to, ar įmonė juos turi (pvz., automobilio valstybinis numeris, vaizdo duomenys, telefono ryšio numeris ir kt.).

Taigi, asmens duomenys apima **informaciją apie fizinius asmenis**, kurie:

- Gali būti (yra) identifikuoti tiesiogiai iš atitinkamos informacijos; arba
- Gali būti netiesiogiai identifikuojami iš turimos informacijos kartu su kita informacija, t. y. skirtinga informacija, kuri surinkta kartu, gali atskleisti konkretaus asmens tapatybę.

Pastebėtina, kad galimybė nustatyti asmens tapatybę nebūtinai reiškia gebėjimą sužinoti asmens vardą ir pavardę.

Pavyzdžiai

Asmens duomenys: vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, telefono ryšio numeris, elektroninio pašto adresas (pvz., vardas.pavarde@imone.com), pilietybė, socialinio draudimo numeris, gimimo data, banko kortelės numeris, išsilavinimo duomenys (baigta mokykla, diplomų ir sertifikatų duomenys), darbovietė, pajamos ir darbo užmokestis, duomenys apie turimą turtą (žemę, automobilį, butą, vertybinius popierius), duomenys apie sveikatą (sveikatos būklę, kraujo grupė ir kt.), vaizdo duomenys, biometriniai duomenys, šeimos narių duomenys (jei jie siejami su duomenų subjektu), pomėgiai, pirkimo ir pirkinių istorija, asmens lankomi interneto puslapiai, atsitiktinai sugeneruotas telefono ryšio numeris, buvimo vietos duomenys (pvz., buvimo vietos duomenys mobiliajame telefone), interneto protokolo (IP) adresas ir kt.

SVARBU! Nėra asmens duomenų baigtinio sąrašo.

AR JURIDINIŲ ASMENŲ DARBUOTOJŲ DUOMENYS LAIKYTINI ASMENS DUOMENIMIS?

Įmonės darbuotojų darbo el. pašto adresai, tokie kaip vardas.pavarde@imone.eu aiškiai yra susiję su konkrečiu asmeniu, todėl yra laikomi asmens duomenimis.

BDAR taikomas duomenims, susijusiems su asmenimis, kurie veikia kaip individualūs prekybininkai, profesinę veiklą vykdantys fiziniai asmenys, partneriai ir įmonių direktoriai, kai informacija yra susijusi su jais, kaip su asmenimis, o ne kaip su juridinio asmens atstovais.

AR PSEUDONIMINIAI DUOMENYS VIS DAR YRA ASMENS DUOMENYS?

Asmens duomenys, iš kurių pašalinta asmenį identifikuojanti informacija, kurie yra užšifruoti ar kuriems yra suteikti pseudonimai, bet kuriuos galima panaudoti iš naujo nustatant asmens tapatybę, išlieka asmens duomenimis ir jiems taikomas BDAR.

Pavyzdys

Sveikatos priežiūros įstaiga, atlikdama mokslinį medicininį tyrimą, privalo užtikrinti tiriamųjų asmenų anonimiškumą. Todėl asmenims vietoj jų vardo ir pavardės yra suteikiami identifikaciniai kodai (pseudonimai), kurie ir naudojami tyrime kartu su kitais asmens duomenimis (pvz., duomenimis apie sveikatą, tyrimų rezultatais). Tretieji asmenys, pagal tyrime naudojamus duomenis, neturi galimybės nustatyti tiriamųjų asmenų tapatybės. Tačiau siekiant užtikrinti tyrimo konfidencialumą ir objektyvumą, sveikatos priežiūros įstaiga sudaro tiriamųjų sąrašą, kuriame tiriamojo vardas ir pavardė yra susiejami su jam suteiktu identifikaciniu kodu. Taigi, įstaiga gali nesunkiai nustatyti tiriamojo tapatybę, ir tai jau laikytina asmens duomenimis, o šių duomenų tvarkymui taikomas BDAR.

KAS NĖRA LAIKOMA ASMENS DUOMENIMIS?

- BDAR netaikomas anoniminės informacijos tvarkymui, įskaitant duomenų tvarkymą statistiniais ar tyrimų tikslais. Asmens duomenys, kurių anonimiškumas užtikrintas taip, kad asmens tapatybė negali arba nebegali būti nustatyta, nebelaikomi asmens duomenimis. Kad duomenys būtų iš tiesų anoniminiai, anonimiškumas turi būti užtikrintas negrįžtamai.
- Informacija apie juridinį asmenį, atskirai nuo jos savininkų ar direktorių, nėra asmens duomenys ir nepatenka į BDAR taikymo sritį. Informacija apie valdžios institucijas taip pat nėra laikytina asmens duomenimis.

Pavyzdys

Juridinio asmens kodas, elektroninio pašto adresas, pvz., info@imone.com, nuasmeninti ar anoniminiai duomenys nėra asmens duomenys.

SPECIALIŲ KATEGORIJŲ ASMENS DUOMENYS

Specialių kategorijų duomenimis yra laikomi toliau nurodyti asmens duomenys. Juos galite tvarkyti tik esant tam tikroms išimtims:

- Asmens duomenys, atskleidžiantys rasinę arba etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus;
- Priklausymas profesinėms sąjungoms;
- Genetiniai duomenys, biometriniai duomenys, tvarkomi siekiant nustatyti asmens tapatybę;
- Su sveikata susiję duomenys;
- Duomenys, susiję su asmens lytiniu gyvenimu ar lytine orientacija.

Pagal BDAR tai yra jautresni duomenys, todėl jų tvarkymui reikalaujama daugiau apsaugos. Šiuos duomenis galite rinkti ir naudoti **tik esant tam tikroms sąlygoms, nurodytoms BDAR 9 straipsnio 2 dalyje**, pvz., gavus aiškų sutikimą, jeigu tai leidžiama pagal nacionalinius įstatymus ir kt.

KAM TAIKOMAS BDAR?

BDAR MATERIALINĖ TAIKYMO SRITIS

BDAR taikomas asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam **automatizuotomis priemonėmis**, pvz., kompiuteriu, informacinėje sistemoje, naudojant vaizdo kameras ir kt., ir asmens

duomenų, kurie sudaro **susisteminto rinkinio**[2], dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis pvz., popierinės darbuotojų asmens bylos, klientų duomenys rūšiuojami abėcėlės tvarka ir kt.

Taigi, kai įmonė ar fizinis asmuo, kuris verčiasi profesine ar ūkine komercine veikla, renka, saugo ar kitokiu būdu tvarko savo darbuotojų, klientų ar kitų duomenų subjektų asmens duomenis, BDAR yra taikomas.

Pavyzdžiai

- Individualioje įmonėje dirba tik vienas darbuotojas, tačiau įmonė, teikdama savo paslaugas, išsisaugo klientų (fizinių asmenų) vardą, pavardę ar telefono ryšio numerį. Taip pat įmonė vykdo vaizdo stebėjimą jai priklausančiose patalpose (pvz., įrengta viena vaizdo kamera turto saugumui užtikrinti). Tokiu atveju įmonė laikoma asmens duomenų valdytoju ir įmonei taikomos BDAR nuostatos.
- Esate fizinis asmuo ir užsiimate drabužių prekyba internetu. Vykdydami veiklą renkate klientų (fizinių asmenų) asmens duomenis (vardą, pavardę, kontaktinius duomenis ir t. t.), tokiu atveju Jūs laikomas asmens duomenų valdytoju ir Jums taikomas BDAR.

Atsiminkite, kad BDAR taikomas ir tokiems Jūsų darbuotojų asmens duomenims, kaip, pvz., darbo el. pašto adresams, tokiems kaip vardas.pavarde@imone.eu, arba darbuotojų darbo telefono numeriams.

BDAR TAIKYMO IŠIMTYS

BDAR **netaikomas** asmens duomenų tvarkymui, kai:

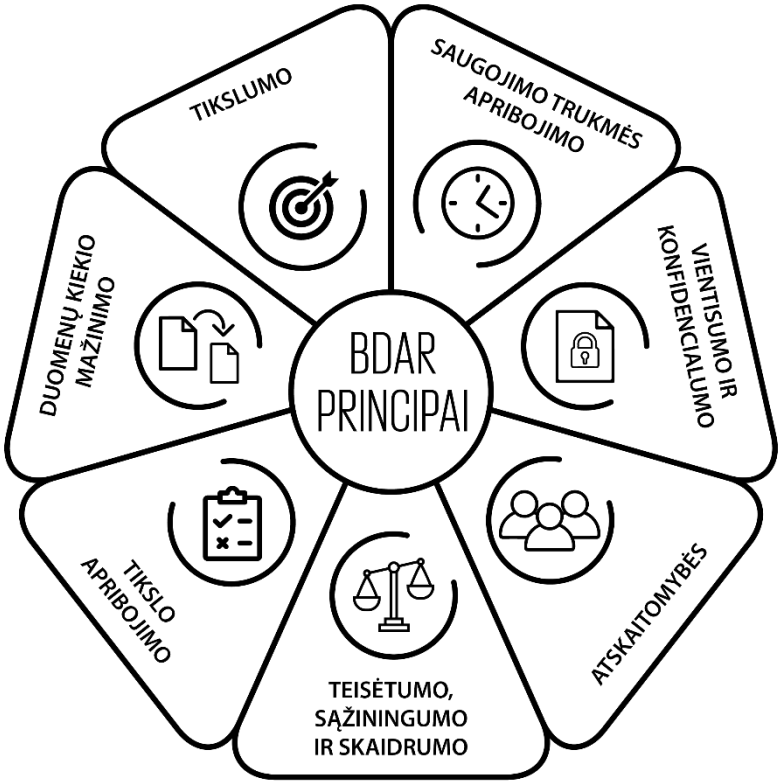
- Asmens duomenis tvarko *fizinis asmuo, užsiimdamas išimtinai asmenine ar namų ūkio veikla*, t. y. asmuo tvarko duomenis tik asmeniniais tikslais arba savo namuose vykdomos veiklos tikslais, su sąlyga, kad nėra jokio ryšio su profesine ar komercine veikla, kitu atveju BDAR taikomas;
- Tvarkomi *mirusių asmenų duomenys*;
- Tvarkomi *juridinių asmenų duomenys*. Atkreiptinas dėmesys, kad informacija, susijusi su vienanare įmone, gali būti laikoma asmens duomenimis, jeigu pagal ją galima nustatyti fizinio asmens tapatybę;
- Asmens duomenys tvarkomi vykdant veiklą, kuriai ES teisė netaikoma.

Pavyzdžiai

- Asmuo pasinaudoja savo asmenine adresų knygele, kad elektroniniu paštu pakviestų draugus į gimtadienį. Tokiu atveju BDAR netaikomas.
- Įmonė, naudodamasi programa „Excel“, sukuria juridinių asmenų sąrašą, kuriuos ji laiko potencialiais klientais. Tokiu atveju BDAR taip pat netaikomas.

[2] Susistemintas rinkinys – bet kuris susistemintas pagal specialius kriterijus prieinamų asmens duomenų rinkinys, kuris gali būti centralizuotas, decentralizuotas arba suskirstytas funkciniu ar geografiniu pagrindu.

SU ASMENS DUOMENŲ TVARKYMU SUSIJĘ PRINCIPAI



ATSKAITOMYBĖS PRINCIPAS

BDAR įtvirtina duomenų valdytojo **atskaitomybės principą**, kuris reiškia, kad duomenų valdytojas (duomenų tvarkytojas) yra atsakingas už tai, kad būtų laikomasi šio reglamento principų ir taisyklių bei turi **sugebėti įrodyti**, kad jų laikomasi. Taigi atskaitomybės principas įpareigoja Jus būti aktyviais įrodant atitiktį BDAR, įgyvendinti kitus BDAR principus ir nustatytas asmens duomenų tvarkymo taisykles ir sugebėti tai įrodyti.

Yra įvairiausių priemonių, kurių galite ir atitinkamais atvejais turite imtis siekdami įgyvendinti atskaitomybės principą (sąrašas nebaigtinis):

- Tinkamų organizacinių ir techninių priemonių taikymas;
- Duomenų apsaugos politikos ar privatumo politikos priėmimas ir įgyvendinimas;
- Asmens duomenų saugumo pažeidimų fiksavimas ir, kai reikia, pranešimas apie juos priežiūros institucijai ir (ar) duomenų subjektams;
- Jei taikoma, duomenų veiklos įrašų tvarkymas;
- Jei taikoma, duomenų apsaugos pareigūno paskyrimas;
- Poveikio duomenų apsaugai atlikimas, kai dėl asmens duomenų tvarkymo operacijų gali kilti didelis pavojus fizinio asmens teisėms ir laisvėms;
- Standartizuotosios duomenų apsaugos ir pritaikytosios duomenų apsaugos užtikrinimas.

Svarbu prisiminti, kad iš atskaitomybės principo kylančių pareigų įgyvendinimas yra **tęstinis procesas**. Jūs turėtumėte periodiškai ar atsižvelgdami į pasikeitusias asmens duomenų tvarkymo aplinkybes peržiūrėti ir, kai reikia, atnaujinti atskaitomybės principo įgyvendinimo priemones.

TEISĖTUMO, SĄŽININGUMO IR SKAIDRUMO PRINCIPAS

Teisėtumo, sąžiningumo ir skaidrumo principas įpareigoja asmens duomenis duomenų subjekto atžvilgiu tvarkyti teisėtu, sąžiningu ir skaidriu būdu.

Teisėtumas reiškia, kad asmens duomenys turi būti tvarkomi remiantis bent viena BDAR įtvirtinta teisėto asmens duomenų tvarkymo sąlyga: duomenų subjekto sutikimu; sutarties su duomenų subjektu vykdymu; teisine prievole; duomenų subjekto ar kito fizinio asmens gyvybinių interesų apsauga; užduoties, viešojo intereso labui, vykdymu; teisėtais duomenų valdytojo ar trečiosios šalies interesais.

Teisėtumas taip pat įpareigoja įmones, kai tvarkomi specialių kategorijų asmens duomenys ar asmens duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas, juos tvarkyti tik BDAR nustatytomis sąlygomis.

Plačiau teisėto asmens duomenų tvarkymo sąlygos aptariamos šių gairių skyriuje „Teisėto asmens duomenų tvarkymo “.

Be nurodytų, teisėto asmens duomenų tvarkymo sąlygų, teisėtumas turėtų būti suprantamas plačiau, t. y. kad, tvarkant asmens duomenis, jie turi būti naudojami taip, kad nebūtų pažeisti ir kitų teisės sričių teisės aktais keliami reikalavimai, pvz., kylantys iš baudžiamosios ar civilinės teisės.

Sąžiningumas reiškia, kad asmens duomenų tvarkymas turi būti atliekamas sąžiningai. Duomenų subjektas turi būti informuotas, kad yra tvarkomi jo asmens duomenys ir apie su tuo susijusias rizikas.

Sąžiningumas taip pat reiškia, kad duomenų subjektas neturi būti klaidinamas apie tai, kaip yra renkami ir toliau tvarkomi jo asmens duomenys.

Skaidrumas[3] reiškia, kad duomenų subjektams turėtų būti aišku, kaip su jais susiję asmens duomenys yra renkami, naudojami ar jie yra kitaip tvarkomi, taip pat, kokiu tikslu ir mastu asmens duomenys yra ar bus tvarkomi. Duomenų subjektai turėtų būti informuoti apie su asmens duomenų tvarkymu susijusius pavojus, apsaugos priemones ir apie tai, kaip naudotis savo teisėmis. Jūs turite būti skaidrūs, atviri ir sąžiningi fizinių asmenų atžvilgiu apie tai, kokia veikla užsiimate, kokiais tikslais ir kaip tvarkote asmens duomenis. Jūs duomenų subjektui informaciją turėtumėte pateikti aiškia ir paprasta kalba, **ypač kai tai susiję su informacijos teikimu vaikams**. Informacija duomenų subjektui turėtų būti teikiama glausta, skaidria, suprantama ir lengvai prieinama forma.

Skaidrumas yra glaudžiai susijęs su BDAR įtvirtintomis duomenų subjektų teisėmis ir jų įgyvendinimo taisyklėmis, pvz., skaidrumo reikalavimai įgyvendinami pateikiant informaciją duomenų subjektui, kai asmens duomenys yra renkami iš duomenų subjekto ar gaunami ne iš jo.

TIKSLO APRIBOJIMO PRINCIPAS

Tikslo apribojimo principas įpareigoja asmens duomenis rinkti *nustatytais, aiškiai apibrėžtais* bei *teisėtais* tikslais ir toliau jų netvarkyti su tais tikslais nesuderinamu būdu. Todėl asmens duomenų tvarkymas, kai tvarkymo tikslai yra neapibrėžti ar neriboti, taip pat, kai asmens duomenys yra renkami tikintis, kad jie galbūt bus reikalingi ateityje, yra neteisėtas. Taigi turėtumėte būti atviri ir aiškiai pasakyti, kokiais tikslais tvarkote asmens duomenis.

Svarbu pabrėžti, kad asmens duomenų tvarkymo tikslas turėtų būti apibrėžiamas **ne vėliau** kaip asmens duomenų rinkimo pradžia.

Tikslo apribojimo principas yra glaudžiai susijęs su teisėtumo, sąžiningumo ir skaidrumo principu, nes pasirinktas asmens duomenų tvarkymo tikslas turi būti teisėtas. Kaip jau aptarta šių gairių skyriuje „Teisėtumo, sąžiningumo ir skaidrumo principas“, teisėtumas neturi būti suprantamas vien kaip BDAR įtvirtintos teisėto asmens duomenų tvarkymo sąlygos pasirinkimas.

[3] Daugiau informacijos apie skaidrumo principą galima rasti 29 straipsnio duomenų apsaugos darbo grupės 2017 m. lapkričio 29 d. Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairėse Nr. WP 260, 1 red.

Kaip nustatyti asmens duomenų tvarkymo tikslą?

Asmens duomenys turi būti renkami *nustatytais* tikslais. Jūs turite žinoti, kokiu tikslu ar tikslais bus naudojami asmens duomenys, ir neturite rinkti asmens duomenų, kurie nėra būtini, pakankami ar tinkami tam tikslui ar tikslams, kuriais ketinate juos naudoti, pasiekti. Taigi apibrėžiant tikslą yra apibrėžiamos asmens duomenų tvarkymo ribos.

Tikslas turi būti *aiškiai apibrėžtas*. Todėl tikslas turi būti apibūdintas pakankamai, konkrečiai ir nedviprasmiškai, kad būtų galima nustatyti, kokios asmens duomenų tvarkymo operacijos yra atliekamos, o tikslą vienodai suprastų visos suinteresuotos šalys: duomenų subjektai, priežiūros institucijos, duomenų tvarkytojai ar kiti duomenų valdytojai.

Įvardijant tikslą, reikėtų atkreipti dėmesį, kad pakankamas ir konkretus tikslo įvardijimas neturėtų būti suprantamas, kaip reikalavimas tikslą labai išsamiai, vartojant teisinius terminus. Tikslas turėtų būti pateikiamas aiškia ir paprasta kalba.

Neaiškūs ar bendro pobūdžio tikslai, pvz., „vartotojų patyrimo patobulinimas“, „rinkodara“, „IT saugumas“ arba „būsimi tyrimai“ – nepateikiant išsamesnės informacijos, paprastai neatitiks kriterijaus „nustatytais“. Tikslo nurodymo išsamumo laipsnis priklauso nuo konkretaus konteksto, kuriame tvarkomi asmens duomenys ir nuo tvarkomų asmens duomenų.

Pavyzdys

Maža parduotuvė, kuri parduoda sukneles ir unikalius aksesuarus, naudoja vienintelį tiesioginės rinkodaros įrankį – metinį katalogą, patenkantį į jos 200 klientų namus popierine forma. Užsisakydami katalogą (ir kaip aiškiai nurodoma pačiame kataloge), klientai informuojami, kad jie gali atsisakyti prenumeratos bet kuriuo metu: asmeniškai, raštu, el. paštu arba paskambinę į parduotuvę. Jie taip pat informuojami, kad jų duomenimis nebus dalijamasi su kitais ir jie bus *naudojami tik katalogo siuntimui*. Šiame paprastame kontekste tai yra pakankamas tikslų apibrėžimas. Kita vertus, jei ši parduotuvė naudotų sudėtingas analizes, kad gautų informaciją, reikalingą suasmenintų ir tikslingų pasiūlymų rengimui, tikslai turi būti nurodyti daug išsamiau.

Kur nustatyti asmens duomenų tvarkymo tikslą?

Asmens duomenų tvarkymo tikslas gali būti pateikiamas įvairiais būdais. Jeigu laikotės skaidrumo reikalavimų, tikėtina, kad Jūs jau esate pasirinkę tinkamą būdą tikslui įvardyti, pvz., informacija apie asmens duomenų tvarkymo tikslą yra pateikiama duomenų tvarkymo veiklos įrašuose; informacija apie asmens duomenų tvarkymo tikslą pateikiama privatumo politikoje ir pan.

Tolesnis asmens duomenų tvarkymas[4]

BDAR leidžia toliau tvarkyti asmens duomenis kitais tikslais nei tais, kuriais jie buvo surinkti, tačiau tokiam asmens duomenų tvarkymui yra taikomi apribojimai. Todėl, jei siekiate tvarkyti asmens duomenis kitais tikslais, negu tais, dėl kurių asmens duomenys buvo surinkti, Jūs tai galite daryti, jeigu:

- Įsitikinate, kad asmens duomenų tvarkymas kitu tikslu yra **suderinamas** su tikslu, dėl kurio iš pradžių asmens duomenys buvo surinkti. Tokiu atveju nereikalaujama atskiro teisinio pagrindo, užtenka to pagrindo, kuriuo remiantis leidžiama rinkti asmens duomenis; arba
- Gaunate duomenų subjekto sutikimą; arba
- Remiatės ES ar nacionaline teise.

BDAR iš anksto nustato, kad tolesnis asmens duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais turėtų būti laikomas

[4] Daugiau informacijos apie tikslo apribojimą galima rasti 29 straipsnio duomenų apsaugos darbo grupės 2013 m. balandžio 2 d. nuomonėje Nr. 03/2013 *Dėl tikslo ribojimo*, skiltyje „Europos duomenų apsaugos valdybos metodinė informacija“. Nors nuomonė po BDAR taikymo pradžios nėra atnaujinta, tačiau joje pateiktos asmens duomenų tvarkymo tikslo nustatymo gairės yra aktualios ir dabar.

suderinamu su tikslu, dėl kurio iš pradžių asmens duomenys buvo surinkti. Kitais atvejais būtina įvertinti, ar tikslai yra suderinami.

Siekiant nustatyti, ar tolesnio duomenų tvarkymo tikslas suderinamas su tikslu, dėl kurio iš pradžių asmens duomenys buvo surinkti, būtina atsižvelgti, be kita ko, į šias aplinkybes:

- Visas sąsajas tarp tikslų, kuriais asmens duomenys buvo surinkti, ir numatomo tolesnio duomenų tvarkymo tikslų;
- Aplinkybes, kuriomis asmens duomenys buvo surinkti, visų pirma, susijusias su duomenų subjektų ir duomenų valdytojo tarpusavio santykiu;
- Asmens duomenų pobūdį, visų pirma, ar tvarkomi specialių kategorijų asmens duomenys, ar tvarkomi asmens duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas;
- Numatomo tolesnio duomenų tvarkymo galimas pasekmes duomenų subjektams;
- Tinkamų apsaugos priemonių, kurios gali apimti šifravimą ar pseudonimų suteikimą, buvimą.

Paprastai naujasis tikslas neturėtų būti laikomas suderinamu su tikslu, kuriuo buvo surinkti asmens duomenys, jeigu jis gali būti duomenų subjektui netikėtas, sukelti jam nepageidaujamas teisines pasekmes ar naujasis tikslas labai skiriasi nuo pirminio.

Pavyzdžiai

- Odontologijos klinika, siekdama teikti odontologijos paslaugas, renka savo klientų asmens duomenis. Odontologijos klinika nusprendžia išsiaiškinti, kokio amžiaus asmenims yra dažniausiai teikiamos paslaugos. Kadangi asmens duomenų tvarkymas statistiniais tikslais yra laikomas suderinamu su pirminiu asmens duomenų rinkimo tikslu, klinikai naujo teisinio pagrindo asmens duomenų tvarkymui nereikia. Tačiau ji turi pareigą imtis tinkamų saugumo priemonių, kad būtų apsaugotos duomenų subjekto teisės ir laisvės, pvz., pseudonimų suteikimas ir kt.
- Į odontologijos kliniką kreipiasi poilsio pasiūlymų teikimu užsiimanti įmonė, prašydama pateikti klinikos klientų kontaktinius duomenis, kad jiems galėtų siųsti pasiūlymus. Šiuo atveju toks asmens duomenų teikimas būtų laikomas nesuderinamu su tikslu, kuriuo asmens duomenys buvo surinkti.

Svarbu atkreipti dėmesį, kad, bet kuriuo atveju, toliau tvarkydami asmens duomenis turite užtikrinti, kad būtų laikomasi BDAR nustatytų principų, visų pirma, kad duomenų subjektas būtų informuotas apie tolesnio asmens duomenų tvarkymo tikslus ir apie savo teises. Todėl gali reikėti atnaujinti sutikimus, jei asmens duomenys buvo tvarkomi remiantis duomenų subjekto sutikimu, atnaujinti privatumo politiką ar pranešimus, ir, kai reikia, imtis papildomų organizacinių ir techninių saugumo priemonių.

DUOMENŲ KIEKIO MAŽINIMO PRINCIPAS

Pagal **duomenų kiekio mažinimo principą** asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi. Šis principas reiškia, kad asmens duomenys turėtų būti tvarkomi tik tuomet, jei asmens duomenų tvarkymo tikslo pagrįstai negalima pasiekti kitomis priemonėmis. Jeigu Jūsų tikslų pagrįstai neįmanoma pasiekti netvarkant asmens duomenų, tuomet turėtumėte pasirinkti mažiausią reikalingą kiekį asmens duomenų, siekiamam tikslui pasiekti.

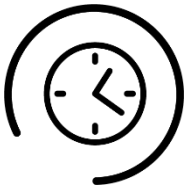
Norėdami įsitikinti, kad asmens duomenys yra adekvatūs, tinkami ir tik tokie, kurių reikia, Jūs turėtumėte įsivertinti, kokio tikslo siekdami tvarkote asmens duomenis. Žinodami konkretų tikslą, toliau turėtumėte įsivertinti, kokius konkrečius asmens duomenis turėdami jį galite pasiekti.

TIKSLUMO PRINCIPAS

Tikslumo principas nustato, kad asmens duomenys turi būti tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi. Taigi BDAR įpareigoja Jus būti aktyvius ir imtis pagrįstų priemonių, kad asmens duomenys būtų tikslūs, pvz., nustatyti asmens duomenų ištrynimo arba periodinės peržiūros terminus. Nustatę, kad asmens duomenys yra nebereikalingi ar netikslūs, turite pareigą imtis visų pagrįstų priemonių, siekdami užtikrinti, kad netikslūs asmens duomenys būtų ištaisyti arba ištrinti.

Tam tikrais atvejais, tikslumo principo laikymasis reiškia, kad, kai asmens duomenis renkate ne tiesiogiai iš duomenų subjekto, Jūs turėtumėte įsitikinti, kad juos renkate iš patikimų šaltinių, užtikrinančių, kad jų tvarkomi asmens duomenys yra tikslūs.

Tikslumo principas yra glaudžiai susijęs su duomenų subjekto teise reikalauti ištaisyti duomenis, apie kurią detaliau kalbama šių gairių skyriuje „Teisė reikalauti ištrinti duomenis („teisė būti pamirštam“)“.



SAUGOJIMO TRUKMĖS APRIBOJIMO PRINCIPAS

Saugojimo trukmės apribojimo principas nustato, kad asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi. Taigi turėtumėte užtikrinti, kad asmens duomenų saugojimo laikotarpis būtų minimalus.

Vertindami, kiek saugosite asmens duomenis, turėtumėte atsižvelgti, pirmiausia, į asmens duomenų tvarkymo tikslą, nes nuo jo priklauso, kokius asmens duomenis tvarkote. Asmens duomenų tvarkymo tikslas Jums taip pat leis įvertinti, ar atitinkama Jūsų veikla ir ją vykdant atliekamas asmens duomenų tvarkymas yra reglamentuojamas kitų teisės sričių teisės aktais, kuriuose jau gali būti nustatytas dokumentų ir tuo pačiu asmens duomenų saugojimo terminas. Kitais atvejais, pareiga nustatyti asmens duomenų saugojimo terminą kyla Jums.

Daugiau apie saugojimo trukmės apribojimo principo įgyvendinimą informacijos rasite šių gairių skyriuje „Kiek laiko turiu saugoti asmens duomenis?“.

VIENTISUMO IR KONFIDENCIALUMO PRINCIPAS

Vientisumo ir konfidencialumo principas nustato, kad asmens duomenys turi būti tvarkomi tokiu būdu, 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. Šis principas Jus įpareigoja turėti tinkamas saugumo priemones, kad apsaugotumėte tvarkomus asmens duomenis.

Daugiau informacijos apie tai, kaip įgyvendinti vientisumo ir konfidencialumo principą, rasite šių gairių skyriuje „Asmens duomenų saugumas“.

TEISĖTO ASMENS DUOMENŲ TVARKYMO SĄLYGOS

BDAR 6 straipsnis numato teisėto duomenų tvarkymo sąlygas.

Įmonė (duomenų valdytojas) gali tvarkyti asmens duomenis tik esant **bent vienai iš šių sąlygų**:

- Gavus duomenų subjekto **sutikimą**;
- Esant **sutartinei prievolei** (pagal įmonės ir kliento sutartį);
- Siekiant įvykdyti **teisinę prievolę** (nustatytą ES ar nacionalinės teisės aktuose);
- Tvarkyti duomenis yra būtina siekiant atlikti užduotį, vykdomą **viešojo intereso** labui, arba

vykdant duomenų valdytojui pavestas **viešosios valdžios funkcijas** (kaip nustatyta ES ar nacionalinės teisės aktuose);

- Siekiant **apsaugoti** asmens gyvybinius interesus;
- Tvarkyti duomenis būtina siekiant **teisėtų** įmonės arba trečiosios šalies **interesų** (išskyrus numatytas išimtis).

Turite žinoti bei galėti pagrįsti, kodėl asmens duomenys yra tvarkomi remiantis viena ar kita teisine sąlyga.

DUOMENŲ SUBJEKTO SUTIKIMAS

Duomenų subjekto sutikimas – bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiškais veiksmais, kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys.

Sutikimas laikomas tinkamu, kai:

- Duotas laisva valia;
- Konkretus ir nedviprasmiškas;
- Tinkamai informuoto asmens valios išreiškimas pareiškimu arba vienareikšmiškais veiksmais, kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys.

Laisvos valios išraiška pasireiškia realios sprendžiamosios galios suteikimu asmeniui, t. y. asmuo gali pasirinkti duoti ar neduoti sutikimą dėl jo asmens duomenų tvarkymo ir dėl to nepatirs jokių neigiamų pasekmių.

Pavyzdys

Asmuo, norėdamas įsigyti prekę internetu, privalo pateikti savo asmens duomenis (pvz., vardą, pavardę, adresą, el. pašto adresą) bei sutikti su pirkimo–pardavimo taisyklėmis, kuriose nurodyta, kad pirkdamas prekę jis sutinka, jog jo duomenys būtų tvarkomi tiesioginės rinkodaros tikslais. Nepažymėdamas, kad susipažino ir sutinka su šiomis taisyklėmis, asmuo negali įsigyti norimos prekės. Šiuo atveju, sutikimas nebus laikomas savanorišku ir tinkamu, kadangi duomenų subjektas negali laisvai nuspręsti, nepasiduodamas aplinkybėms (nes nuo tokio sutikimo priklauso sutarties sudarymas).

BDAR nenustato reikalavimų, kokia forma ar būdais turi būti duodamas asmens sutikimas, tačiau nustato šias sutikimo sąlygas:

- Kaip duomenų valdytojas **turite galėti įrodyti**, kad asmuo sutiko su duomenų tvarkymu;
- Turi būti užtikrinama, kad asmuo **suvoktų kam ir dėl ko** jis duoda sutikimą, todėl jis turi būti tinkamai informuojamas apie:
  - asmens duomenis renkančios įmonės tapatybę (t. y. pavadinimą, juridinio asmens kodą ir pan.),
  - numatomo asmens duomenų tvarkymo tikslus,
  - duomenų, kurie bus tvarkomi rūšis,
  - galimybę atšaukti sutikimą,
  - tai, kad duomenys bus naudojami tik automatizuotam sprendimų priėmimui, įskaitant profiliavimą (jei taikoma),
  - duomenų perdavimą trečiosioms šalims ir kt.
- Sutikimo prašymas turi būti pateiktas **suprantama ir lengvai prieinama forma, aiškiai ir paprasta kalba**, jame neturėtų būti nesąžiningų sąlygų;
- Tyla, iš anksto pažymėti langeliai, **neveikimas neturėtų būti laikomi sutikimu**;
- Sutikimas gaunamas rašytiniu pareiškimu (įskaitant, elektronines priemones), susijusiu su kitais klausimais, turi būti **aiškiai atskirtas** nuo kitų klausimų;
- Sutikimas **neturi būti dviprasmiškas**;
- **Atšaukti sutikimą** turi būti taip pat lengva kaip jį duoti. Apie teisę atšaukti savo sutikimą,

asmuo turi būti informuojamas prieš jam duodant sutikimą.

Pavyzdžiai

- Įmonė siūlo įsigyti muzikos programėlę. Tam, kad galėtų pasiūlyti specialiai parinktas dainas ir galbūt koncertus, turi būti prašoma programėlės naudotojų sutikimo tvarkyti duomenis apie jų muzikinį skonį.
- Elektroninė parduotuvė siūlo pirkėjui paskyroje savo noru įrašyti savo gimimo mėnesį ir dieną (kai ši informacija nėra privaloma pildyti), jei pirkėjas sutinka (pageidauja), kad gimtadienio proga iš pardavėjo gautų pasveikinimą ar dovanėlę.

Netinkamo sutikimo pavyzdžiai

- Darbdavys gauna darbuotojo sutikimą nuolat vykdyti vaizdo stebėjimą darbuotojo darbo vietoje. Šiuo atveju sutikimas greičiausiai nebus *išreikštas laisva valia*, nes tarp darbdavio ir darbuotojo yra pavaldumo santykiai. Akivaizdu, kad duomenų subjektas negali atsisakyti duoti sutikimo, jeigu jis yra socialiai priklausomas (pvz., pasirašęs darbo sutartį ar pan.) arba kai sutikimas siejamas su poreikiais ar privilegijomis, nuo kurių duomenų subjektas yra priklausomas.
- Elektroninės prekybos taisyklėse nustatyta, kad susipažindamas su prekių įsigijimo taisyklėmis pirkėjas sutinka, kad jo asmens duomenys būtų naudojami tiesioginės rinkodaros tikslu. Šiuo atveju sutikimas nėra tinkamas, kadangi sutikimas nėra *išreikštas laisva valia* (t. y. asmeniui nesudaroma galimybė pasirinkti ar jis pageidauja gauti tiesioginės rinkodaros pasiūlymus ar ne) *ir nėra atskirtas* nuo klausimų, susijusių su prekių įsigijimu.

Vaikų sutikimas

- Už nepilnametį iki 14 metų sutikimą turi duoti vaiko tėvai ar globėjai. Sutikimas galioja tik tokiu mastu, kokiu duotas. Atsižvelgiant į turimas technologijas, reikia dėti pagrįstas pastangas, kad būtų patikrinta, ar gautas sutikimas tikrai atitinka visas sutikimo sąlygas. Tai reiškia, kad įmonė turi įgyvendinti amžiaus patikrinimo priemones (pvz., užduoti kontrolinius klausimus ar imtis kitų veiksmų savo svetainėje).
- Jei vaikui tiesiogiai siūlomos informacinės visuomenės paslaugos, vaiko asmens duomenų tvarkymas yra teisėtas, jei sutikimą duoda ne jaunesnis kaip 14 metų vaikas. **Informacinės visuomenės paslaugos** – paprastai už atlyginimą elektroninėmis priemonėmis ir per atstumą individualiu paslaugos gavėjo prašymu teikiamos paslaugos.
- Vaikui tapus suaugusiu, jis turi teisę sutikimą atšaukti ir reikalauti duomenis sunaikinti.
- Tėvų sutikimo nereikalaujama tiesiogiai vaikui teikiant prevencijos ar konsultavimo paslaugas, nes jomis siekiama apsaugoti vaiko interesus.
- Konkrečiai vaikui skirta informacija turi būti lengvai prieinama ir pateikiama aiškia bei paprasta kalba, kurią vaikas lengvai suprastų.

Pavyzdys

Tėvų arba globėjų sutikimą reikia gauti, jeigu Jūsų įmonė siūlo žaidimus vaikams iki 14 metų internetinių socialinių tinklų svetainėse ir renka tam tikrus vaikų asmens duomenis (pvz., vardą, pavardę ir kt.).

SUTARTINĖ PRIEVOLĖ

Sutartiniu pagrindu asmens duomenys gali būti tvarkomi:

- Vykdant įmonės sutartinius įsipareigojimus, nustatytus sutartyje su klientu;
- Siekiant imtis veiksmų kliento prašymu prieš sudarant sutartį.

Pagal sutartį tvarkomi asmens duomenys ir vykdomi asmens duomenų tvarkymo veiksmai turi būti būtini, t. y. nevykdant sutartyje pateiktų asmens duomenų tvarkymo, sutartis negalėtų būti įvykdyta.

Sutartis turi atitikti Lietuvos Respublikos civiliniame kodekse ir kituose teisės aktuose nustatytus reikalavimus.

Turite žinoti, kad asmens duomenys tvarkomi sutartiniu pagrindu ir turėti galimybę sutarties egzistavimą pagrįsti netgi tuo atveju, kai sutartis sudaroma konkliudentiniais veiksmais.

Pavyzdys

Įmonė vykdo prekybą internetu. Ji gali tvarkyti tuos pirkėjų asmens duomenis, kurių reikia sutarčiai sudaryti, pvz., pirkėjo vardą, pavardę, prekės pristatymo adresą, kredito kortelės numerį (jeigu mokama kortele) ir pan.

TEISINĖ PRIEVOLĖ

Teisinė prievolė asmens duomenų tvarkymui taikytina tuo atveju, jei asmens duomenų tvarkymas įmonei nustatytas ES ar Lietuvos Respublikos teisės aktuose.

Šis teisinis pagrindas netaikomas pirmiau paminėtoms sutartinėms prievolėms.

Taip pat galioja principas – asmens duomenis tvarkyti tik tuo atveju, kai tai yra būtina ir turėti galimybę pagrįsti konkrečių teisės aktų, kuriais vadovaujamasi, egzistavimą.

Kai asmens duomenis tvarkote vykdant Jūsų įmonei tenkančią teisinę prievolę:

- Duomenų tvarkymo pagrindas turėtų būti įtvirtintas ES arba nacionalinėje teisėje;
- Nereikalaujama kiekvienu atskiru duomenų tvarkymo atveju specialaus teisės akto;
- Kelioms duomenų tvarkymo operacijoms gali užtekti vieno teisės akto;
- ES arba nacionalinėje teisėje turėtų būti nustatytas asmens duomenų tvarkymo tikslas, taip pat asmens duomenų tvarkymo teisėtumo pagrindas, tvarkytinų asmens duomenų rūšis, duomenų subjektai (asmenų grupė, kurių asmens duomenys bus tvarkomi), duomenų gavėjai ir t. t.;
- ES arba nacionalinėje teisėje taip pat turėtų būti nustatyta teisinę prievolę vykdančio asmens rūšis, pvz., privati įmonė, viešasis asmuo ar kt.

Pavyzdžiai

- Įmonė turi samdomų darbuotojų. Tam, kad darbuotojai būtų apdrausti valstybiniu socialiniu draudimu, teisės aktais darbdavys įpareigotas SODRAI pateikti darbuotojo asmens duomenis (pvz., savo darbuotojų pajamas).
- Pagal Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymą finansų ir kitos įstaigos bei įmonės privalo atitinkamais atvejais nustatyti kliento ir naudos gavėjo tapatybę bei nustatytais atvejais teikti kliento asmens duomenis Finansinių nusikaltimų tyrimo tarnybai.

VIEŠASIS INTERESAS

Viešojo intereso sąvoka nėra apibrėžta teisės aktuose, tačiau šiose rekomendacijose viešasis interesas suprantamas, kaip visuomenei svarbi vertybė, gėris, kurio užtikrinimu turi rūpintis valdžios įstaigos (taip pat ir viešojo administravimo subjektai), ir į kurį neatsižvelgus būtų pažeistos ne vieno, o daugelio žmonių teisės ir teisėti interesai, pvz., žemės reformos tikslai, mokesčių surinkimas, aplinkos apsauga ir teritorijų planavimas Lietuvos vyriausiojo administracinio teismo praktikoje yra pripažįstami viešuoju interesu.

Viešojo intereso pagrindu asmens duomenų tvarkymas yra teisėtas, kai:

- Teisės aktuose nustatytos užduotys vykdomos viešojo intereso labui;
- Vykdomos viešosios valdžios pavestos funkcijos, nustatytos teisės aktuose.

Viešojo intereso siekis yra aktualiausias valdžios institucijoms, tačiau jis gali būti taikomas bet kuriai įmonei ar įstaigai, kuri vykdo viešosios valdžios funkcijas arba atlieka viešojo intereso užduotis.

Šiuo atveju asmens duomenų tvarkymas turi būti būtinas. Jei viešojo intereso labui taikomas užduotis ar funkcijas galima būtų atlikti nenaudojant asmens duomenų, asmens duomenų tvarkymas būtų neteisėtas. Be to, pagrindinė užduotis ar funkcija turi būti aiškiai pagrįsta įstatymais.

Privalote žinoti konkretų teisės aktą, kuriuo vadovaudamasi vykdo atitinkamą užduotį ar funkciją, kad galėtų įrodyti asmens duomenų tvarkymo teisėtumą.

ASMENS GYVYBINIAI INTERESAI

Asmens duomenų tvarkymas gali būti teisėtas, jei norima apsaugoti asmens gyvybę ar sveikatą. Jei asmens gyvybinius interesus galima apsaugoti kitais būdais (netvarkant asmens duomenų), tai asmens duomenų tvarkymas būtų neteisėtas.

Šiuo atveju asmens duomenys turėtų būti tvarkomi, tik kai duomenų tvarkymas negali būti akivaizdžiai grindžiamas kitu teisiniu pagrindu, pavyzdžiui, įmonė ar įstaiga negali vadovautis gyvybiniais interesais dėl sveikatos ar kitų specialiųjų duomenų tvarkymo, jei asmuo gali, bet atsisako duoti sutikimą. Kai kurių rūšių duomenų tvarkymas gali būti reikalingas tiek dėl svarbių viešojo intereso priežasčių, tiek dėl asmens gyvybinių interesų, pvz., kai duomenis būtina tvarkyti humanitariniais tikslais, siekiant stebėti epidemiją ir jos paplitimą arba susidarius ekstremaliajai humanitarinei situacijai, visų pirma, gaivalinių ir žmogaus sukeltų nelaimių atvejais.

Pavyzdys

Į ligoninės skubios medicininės pagalbos skyrių atvežtas į avariją patekęs pacientas, kuris yra nesąmoningas, todėl sutikimo duoti negali. Ligoninei nereikia jo sutikimo ieškoti jo asmens dokumentų, kad galėtų patikrinti, ar šis asmuo yra ligoninės duomenų bazėje ir rasti jo ankstesnę ligos istoriją ar susisiekti su jo artimaisiais.

TEISĖTI INTERESAI

Įmonei dažnai reikia tvarkyti asmens duomenis, kad galėtų atlikti su savo veikla susijusias užduotis. Toks asmens duomenų tvarkymas ne visada gali būti grindžiamas teisine ar sutartine prievole. Tokiais atvejais asmens duomenų tvarkymą galite grįsti įmonės teisėtais interesais.

Tam, kad asmens duomenys galėtų būti tvarkomi vadovaujantis šia teisine sąlyga, turite:

- Nustatyti teisėtą interesą (nors teisėti interesai yra lanksti teisėto duomenų tvarkymo sąlyga, tačiau negalima manyti, kad ji visada bus tinkamiausia);
- Įvertinti intereso teisėtumą ir veiklos tikslingumą, t. y. atsakyti į klausimą, koks duomenų tvarkymo tikslas ir kokių interesų yra siekiama;
- Įsitikinti, kad asmens duomenų tvarkymas (būtent tokia apimtimi) yra būtinas nustatytam tikslui pasiekti;
- Įvertinti poveikį asmens privatumui; įsitikinti, kad teisėti interesai nedaro didelio poveikio asmenų teisėms ir laisvėms;
- Subalansuoti savo interesus bei asmens teises ir laisves; pasverti, ar asmens interesai ir pagrindinės jo teisės nėra viršesni už įmonės interesus, o ypač tais atvejais, kai tvarkomi vaikų asmens duomenys;
- Įvertinti, ar asmuo galėtų pagrįstai tikėtis, kad jo duomenys bus tvarkomi nustatytu tikslu bei būdu.

Be to, norint tvarkyti asmens duomenis, siekiant teisėtų interesų, turite atsižvelgti *į šiuos aspektus*:

- Teisėti interesai gali būti ir trečiųjų asmenų interesai; jie gali apimti komercinius interesus, individualius interesus ar platesnes socialines teises;
- Jei įmonė gali tą patį rezultatą pasiekti kitu būdu ar remdamasi kita teisine sąlyga, ji negali

vadovautis teisėtu interesu;

- Jeigu duomenų subjekto interesai arba pagrindinės teisės ir laisvės (atsižvelgiant į pagrįstus asmens lūkesčius jų santykių su duomenų valdytoju pagrindu) yra viršesni už įmonės interesus, šiuo teisiniu pagrindu vadovautis tvarkant asmens duomenis negalima;
- Įmonė privalo tinkamai informuoti asmenį apie jo duomenų tvarkymą;
- Įmonės, priklausančios įmonių grupėms, gali turėti teisėtą interesą vidaus administravimo tikslais persiųsti klientų ar darbuotojų asmens duomenis įmonių grupės viduje. Šiuo atveju turi būti laikomasi bendrųjų principų, reglamentuojančių asmens duomenų perdavimą įmonių grupės viduje trečiojoje valstybėje esančiai įmonei;
- Elektroninių ryšių tinklų bei paslaugų teikėjų ir kitų oficialių (įgaliotų) informacinių technologijų saugumo tarnybų atliekamas asmens duomenų tvarkymas, kiek tai yra būtina ir proporcinga siekiant užtikrinti tinklo ir informacijos saugumą, gali būti laikomas teisėtu atitinkamos įmonės interesu, nes tai galėtų užkirsti kelią neteisėtai prieigai prie elektroninių ryšių tinklų, sustabdyti atkirtimo nuo paslaugos atakas ir neleisti pakenkti kompiuterių bei elektroninių ryšių sistemoms.

Pavyzdys

Siekdama užtikrinti tinklo saugumą, įmonė stebi savo darbuotojų IT įrenginių naudojimą. Įmonė gali teisėtai tvarkyti asmens duomenis šiuo tikslu tik tuo atveju, jeigu pasirenkamos mažiausiai darbuotojų teises į privatumą apribojančios priemonės, pvz., apribojamas tam tikrų svetainių prieinamumas, užuot kaupus informaciją apie darbuotojo lankymąsi kitose interneto svetainėse.

DUOMENŲ VALDYTOJO IR DUOMENŲ TVARKYTOJO SANTYKIAI

KAS YRA DUOMENŲ TVARKYTOJAS?

Duomenų tvarkytoju laikomas fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri **duomenų valdytojo vardu** tvarko asmens duomenis.

Duomenų valdytojas nustato duomenų tvarkymo tikslus ir priemones. Jeigu Jūsų įmonė sprendžia, kodėl ir kaip bus tvarkomi asmens duomenys, ji yra duomenų valdytoja, bet jeigu ji tvarko asmens duomenis pagal kitos įmonės įgaliojimus ar nurodymus, kitos įmonės vardu ar pan. – ji bus duomenų tvarkytojas.

Duomenų tvarkytojai:

- Tvarko asmens duomenis tik duomenų valdytojo vardu (duomenų valdytojo naudai ir pagal duomenų valdytojo nurodymus);
- Yra nesusiję darbo santykiais su duomenų valdytoju, t. y. nėra duomenų valdytojo darbuotojai.

Duomenų tvarkytojas paprastai yra įmonei nepriklausanti trečioji šalis, su kuria sudaroma sutartis dėl tam tikrų veiksmų atlikimo. Duomenų tvarkytojas gali būti įgaliotas atlikti bet kokius veiksmus duomenų valdytojo nuožiūra: vykdyti vaizdo stebėjimą (pvz., saugos tarnybos), užtikrinti asmens duomenų saugojimą ar naikinimą, vykdyti kompiuterių priežiūrą, daryti atsargines duomenų kopijas (pvz., informacinių sistemų priežiūros paslaugas teikiantys asmenys), tvarkyti buhalterinę apskaitą ir kt.

Pavyzdys

Mažmeninės prekybos įmonė nusprendžia debesies serveryje saugoti savo klientų duomenų bazės atsarginę kopiją. Tuo tikslu ji sudaro sutartį su debesijos paslaugų teikėju, kuris garsėja savo duomenų apsaugos standartais ir turi sertifikuotą duomenų šifravimo sistemą. Debesijos paslaugų teikėjas yra duomenų tvarkytojas, nes jis įmonės vardu tvarkys klientų asmens duomenis, t. y. saugos juos savo serveriuose.

Įmonių grupės atveju viena įmonė gali būti kitos įmonės duomenų tvarkytoja (pvz., dukterinė įmonė gali atlikti duomenų tvarkytojo funkciją).

Įmonė gali būti duomenų valdytojas arba duomenų tvarkytojas, arba tuo pačiu metu ir duomenų valdytojas, ir duomenų tvarkytojas.

Pavyzdys

Gamykla, kurioje dirba daug žmonių, yra pasirašiusi sutartį su apskaitos įmone, kad ši skaičiuotų jiems darbo užmokestį. Gamykla praneša apskaitos įmonei, kai reikia išmokėti darbo užmokestį, kai koks nors darbuotojas išeina iš darbo arba padidinamas darbo užmokestis. Ji pateikia visus algalapiams ir mokėjimams reikalingus duomenis. Apskaitos įmonė suteikia IT sistemą ir saugo darbuotojų duomenis. Šiuo nurodytu atveju gamykla yra duomenų valdytojas, o apskaitos įmonė – duomenų tvarkytojas. Tačiau apskaitos įmonė kartu yra ir duomenų valdytoja, nes tvarko savo darbuotojų asmens duomenis ir saugo telefoninių pokalbių įrašus kokybės paslaugų užtikrinimo tikslu.

Duomenų tvarkytojas turi veikti tik vadovaudamasis duomenų valdytojo nurodymais, tik jam dokumentais patvirtintomis instrukcijomis.

Jei duomenų tvarkytojas pats nustato asmens duomenų tvarkymo tikslą ir būdus (o ne veikia tik pagal valdytojo nurodymus), jis laikomas duomenų valdytoju ir jam taikoma duomenų valdytojo atsakomybė.

KOKIE REIKALAVIMAI KELIAMI DUOMENŲ TVARKYTOJUI?

Tvarkyti asmens duomenis gali būti patikima tik tokiems duomenų tvarkytojams, kurie yra (potencialiai) pajėgūs užtikrinti asmens duomenų tvarkymą laikantis BDAR reikalavimų.

Paskirtas duomenų tvarkytojas turi užtikrinti, kad techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų BDAR standartus ir būtų užtikrinta fizinių asmenų teisių apsauga.

KODĖL REIKALINGA SUTARTIS TARP DUOMENŲ VALDYTOJO IR DUOMENŲ TVARKYTOJO?

Kai pasitelkiate duomenų tvarkytoją atlikti tam tikrus asmens duomenų tvarkymo veiksmus, tarp Jūsų įmonės ir tvarkytojo turi būti pasirašoma sutartis ar susitarimas.

Sutartimi ar kitu teisės aktu reglamentuojamas duomenų tvarkytojo atliekamas duomenų tvarkymas užtikrina, kad duomenų valdytojas ir duomenų tvarkytojas supranta savo įsipareigojimus ir atsakomybę.

KAS TURI BŪTI ĮTRAUKTA Į SUTARTĮ SU DUOMENŲ TVARKYTOJU?

Sutartyje su duomenų tvarkytoju turite konkrečiai apibrėžti asmens duomenų tvarkymo apimtis ir aiškiai nurodyti duomenų tvarkytojų pareigas ir atsakomybes:

- Duomenų tvarkymo dalykas ir trukmė;
- Duomenų tvarkymo pobūdis ir tikslas;
- Perduodami tvarkyti asmens duomenys (jų rūšys) ir duomenų subjektai (jų kategorijos), kurių asmens duomenys perduodami tvarkyti;
- Duomenų valdytojo prievolės ir teisės.

Taip pat sutartyje su duomenų tvarkytoju arba atitinkamame teisės akte turite nustatyti, kad:

- Duomenys tvarkomi tik pagal duomenų valdytojo dokumentais įformintus nurodymus;

- Duomenų tvarkytojas užtikrina, kad asmenys, įgalioti tvarkyti asmens duomenis, būtų įsipareigoję užtikrinti konfidencialumą arba jiems būtų taikoma atitinkama įstatymais nustatyta konfidencialumo prievolė;
- Duomenų tvarkytojas užtikrina ir įgyvendina saugumo priemones;
- Duomenų tvarkytojas gali pasitelkti kitą duomenų tvarkytoją (subtvarkytoją) tik gavęs išankstinį duomenų valdytojo sutikimą ir pasirašydamas rašytinę sutartį;
- Duomenų tvarkytojas padeda duomenų valdytojui užtikrinti, kad būtų laikomasi BDAR (pvz., padeda duomenų valdytojui įvykdyti įsipareigojimus, susijusius su duomenų tvarkymo saugumu, pranešimu apie asmens duomenų pažeidimus ir duomenų apsaugos poveikio vertinimais, padėti duomenų valdytojui suteikti galimybę susipažinti su dokumentais ir leisti duomenų subjektams pasinaudoti savo teisėmis pagal BDAR.
- Pagal duomenų valdytojo pasirinkimą, baigus teikti su duomenų tvarkymu susijusias paslaugas, ištrina arba grąžina duomenų valdytojui visus asmens duomenis ir ištrina esamas jų kopijas, išskyrus atvejus, kai remiantis ES ar valstybės narės teise reikalaujama asmens duomenis saugoti;
- Pateikia duomenų valdytojui visą informaciją, būtiną siekiant įrodyti, kad vykdomos šiame straipsnyje nustatytos prievolės, ir sudaro sąlygas bei padeda duomenų valdytojui arba kitam duomenų valdytojo įgaliotam auditoriui atlikti auditą, įskaitant patikrinimus.

KADA GALIMA DUOMENŲ TVARKYTOJUI PASITELKTI KITĄ DUOMENŲ TVARKYTOJĄ (SUBTVARKYTOJĄ)?

Duomenų tvarkytojui draudžiama pasitelkti kitą duomenų tvarkytoją be išankstinio konkretaus arba bendro rašytinio duomenų valdytojo leidimo.

Duomenų tvarkytojas gali perleisti dalį savo užduoties kitam duomenų tvarkytojui (subtvarkytojui), sudarydamas su juo sutartį, arba paskirti bendrą duomenų tvarkytoją, **jeigu iš anksto gavo rašytinį duomenų valdytojo sutikimą.**

Bendro rašytinio leidimo atveju duomenų tvarkytojas informuoja duomenų valdytoją apie visus planuojamus pakeitimus, susijusius su kitų duomenų tvarkytojų (subtvarkytojų) pasitelkimu ar pakeitimu, ir taip duomenų tvarkytojas duomenų valdytojui suteikia galimybę nesutikti su tokiais pakeitimais.

Jei duomenų tvarkytojas pasitelkia subtvarkytoją, jis, kaip pirminis duomenų tvarkytojas, atsako duomenų valdytojui už subtvarkytojo įsipareigojimų vykdymą.

Pavyzdys

Įmonė, administruojanti sveikatos priežiūros įstaigos informacinę sistemą, ketina pasitelkti duomenų tvarkytoją, kuris teiks serverių priežiūros paslaugas. Tokiu atveju sveikatos priežiūros įstaigos duomenų tvarkytojas gali pasitelkti subtvarkytoją serverių priežiūros paslaugoms tik turėdamas sveikatos priežiūros įstaigos (duomenų valdytojo) leidimą.

DUOMENŲ TVARKYTOJO ATSAKOMYBĖ

BDAR numato daugiau pareigų duomenų tvarkytojams, todėl duomenų tvarkytojas, be sutartinių įsipareigojimų duomenų valdytojui, pagal BDAR taip pat turi šias tiesiogines pareigas:

- Nepasitelkti subtvarkytojo be išankstinio rašytinio duomenų valdytojo sutikimo;
- Bendradarbiauti su VDAI;
- Užtikrinti duomenų tvarkymo saugumą;
- Tvarkyti duomenų veiklos įrašus apie duomenų tvarkytojo veiklą (jei reikia);
- Pranešti duomenų valdytojui apie visus asmens duomenų saugumo pažeidimus;
- Paskirti duomenų apsaugos pareigūną (jei reikia);
- Jei reikia, paskirti (raštu) atstovą ES.

BDAR reikalavimus pažeidusiems duomenų tvarkytojams taip pat gali tekti atlyginti ir duomenų subjekto dėl pažeidimo patirtą turtinę bei neturtinę žalą. Duomenų tvarkytojui atsakomybė kils tik pažeidus BDAR konkrečiai jam įtvirtintas pareigas (užtikrinti konfidencialumą, pranešti apie asmens duomenų saugumo pažeidimus, baigus teikti paslaugas ištrinti visus tvarkytus duomenis ir pan.) arba veikus priešingai teisėtiems duomenų valdytojo nurodymams.

Dėl šios priežasties kaip duomenų valdytojai, sudarydami sutartis su duomenų tvarkytojais, turėtumėte būti itin atidūs: sutartyse konkrečiai ir aiškiai įtvirtinkite reikalavimus duomenų tvarkymui, detalizuokite BDAR įtvirtintas duomenų tvarkytojų pareigas.

Atkreiptinas dėmesys, kad BDAR numato ir **solidarią atsakomybę**, t. y., kai su tuo pačiu duomenų tvarkymo atveju yra susiję keli duomenų valdytojai ir (ar) tvarkytojai, jie pagal susitarimą dalijasi atsakomybę tarpusavyje.

BDAR DOKUMENTAI IR JŲ NUOSTATOS

BDAR nereglamentuoja konkrečių dokumentų ir jų nuostatų, išskyrus duomenų tvarkymo veiklos įrašus. BDAR nurodyta tik tai, kad duomenų valdytojas turi įgyvendinti tinkamą duomenų apsaugos politiką. Jūs, kaip duomenų valdytojas, siekiamas įrodyti, kad tinkamai taikote BDAR ir laikotės BDAR reikalavimų, t. y. užtikrinate atitiktį BDAR, turėtumėte patvirtinti ir skelbti (taikyti) tam tikrus dokumentus.

BDAR atitiktį įrodantys dokumentai gali būti skirstomi į:

- Dokumentus, kurie skelbiami viešai;
- Vidinius dokumentus.

Dokumentai, skelbiami viešai, skirti „išoriniams“ duomenų subjektams. Toliau pateikiamos tokių dokumentų tipinės rūšys, trumpas aprašymas ir informacija dėl tokių dokumentų privalomumo (taikymo).

„Išorinio“ dokumento rūšis	Trumpas aprašymas	Informacija dėl privalomumo (privalomas, rekomenduotinas esant tam tikroms sąlygoms)
Privatumo politika (privatumo pranešimas)	Aprašomi asmens duomenų tvarkymo tikslai, terminai, duomenų subjekto teisės ir jų įgyvendinimas, kitos sąlygos, įskaitant duomenų tvarkytojus, duomenų gavėjus ir kt. Taip pat nurodomos duomenų subjekto teisės. Skelbiama atitinkamame tinklapyje, aplikacijoje ar pan.	Privaloma tais atvejais, jei atitinkamame tinklapyje (aplikacijoje) renkate asmens duomenis. Rekomenduotina skelbti privatumo politiką ir tais atvejais, kai tinklapyje nerenkami asmens duomenys, tačiau Jūs, kaip duomenų valdytojas, pageidaujate viešai paskelbti apie Jūsų įmonės atliekamą asmens duomenų tvarkymą
Sutartis su klientu (fiziniu asmeniu)	Aprašoma asmens duomenų tvarkymo procedūra, duomenų subjekto teisės ir jų įgyvendinimo tvarka	Privaloma sutartyje su klientu (fiziniu asmeniu) (jei teikiamos paslaugos) nurodyti sąlygas dėl asmens duomenų tvarkymo
Duomenų subjekto sutikimo forma, pvz., dėl tiesioginės rinkodaros	Aprašomos sutikimo sąlygos	Privaloma, jei tvarkomi asmens duomenys, pvz., tiesioginės

		rinkodaros tikslu, vadovaujantis sutikimu
Sutarties su duomenų tvarkytoju forma	Aprašomos pagal BDAR privalomos sąlygos susitarimams su duomenų tvarkytojais (gali būti atskiras susitarimas arba nuostatos į paslaugų sutartis)	Privaloma, jei samdote duomenų tvarkytoją ar tvarkytojus
Asmens duomenų teikimo sutarties forma	Aprašomos asmens duomenų teikimo sąlygos (duomenų teikimo tikslas, teikiami duomenys, teisėto tvarkymo sąlygos, duomenų teikimo tvarka ir kt.)	Privaloma, jei teikiate duomenis kitiems duomenų gavėjams (nuolatos). Vienkartinis teikimas gali būti įforminamas ir pagal motyvuotą vienkartinį kreipimąsi
Asmens duomenų teikimo sąlygos duomenų valdytojams	Aprašomos asmens duomenų teikimo sąlygos	Privalomos, jei teikiate asmens duomenis už EEE ribų kitam duomenų valdytojui
Asmens duomenų teikimo sąlygos duomenų tvarkytojams	Aprašomos asmens duomenų teikimo sąlygos	Privalomos, jei teikiate asmens duomenis už EEE ribų kitam duomenų tvarkytojui
Privatumo pranešimas aktyvaus duomenų subjekto informavimo tikslu	Pateikiama pagrindinė informacija apie asmens duomenų tvarkymą (tikslai, pagrindai, asmens duomenų tvarkymo terminai, duomenų subjekto teisės, jų įgyvendinimas ir kt.)	Privalomas, kai duomenų subjektai neturi reikiamos informacijos ir reikia užtikrinti duomenų subjektų informuotumą

Pastaba: gali būti naudojami ir kiti rekomenduojami dokumentai. Lentelėje pateikiami tik pagrindiniai dokumentai, užtikrinantys atitiktį pagal BDAR.

Vidiniai dokumentai skirti reglamentuoti tam tikroms procedūroms, susijusioms su BDAR atitiktimi. Su šiais dokumentais privaloma supažindinti darbuotojus ir pasilikti susipažinimo įrodymus. Naujai įdarbinamiems darbuotojams taip pat privaloma susipažinti su „vidinių“ dokumentų paketu. Toliau pateikiamos vidinių dokumentų tipinės rūšys, trumpas aprašymas ir informacija dėl tokių dokumentų privalomumo.

„Vidinio“ dokumento rūšis	**Trumpas aprašymas**	**Informacija dėl privalomumo (privalomas, rekomenduotinas esant tam tikroms sąlygoms)**
Asmens duomenų tvarkymo taisyklės (ar kitas analogiškas dokumentas, kuris gali būti ir skirtingo pavadinimo)	Aprašomi asmens duomenų tvarkymo tikslai, teisėto tvarkymo sąlygos, asmens duomenų tvarkymo terminai, duomenų subjekto teisės ir jų įgyvendinimo procedūra, kitos asmens duomenų tvarkymo sąlygos, įskaitant darbuotojų asmens duomenų tvarkymą. *Pastaba:* darbuotojų asmens duomenų tvarkymas gali būti	Privalomos. Galima tvirtinti ir kitokio pavadinimo dokumentą ar keletą dokumentų, tačiau svarbu tenkinti turinio reikalavimus

	reglamentuojamas ir atskiroje tvarkoje – Darbuotojų duomenų tvarkymo politikoje	
Duomenų tvarkymo veiklos įrašai	Fiksuojamas vykdomų asmens duomenų tvarkymo operacijų registras. VDAI rekomenduojama forma prieinama viešai[5]	Privalomi
Duomenų inventorizacijos failas	Aprašomos informacinės sistemos, taip pat kiti būdai, kuriais tvarkomi asmens duomenys, nurodant sistemos pavadinimą, kokie asmens duomenys tvarkomi, atsakingą asmenį ir kt.	Rekomenduotinas
Darbuotojo sutikimas	Nors darbuotojas laikytinas silpnesne šalimi ir negali duoti sutikimo savo noru, visgi gali būti atvejų, kai darbuotojas gali laisvai apsispręsti ir duoti sutikimą savo noru, pvz., dėl nuotraukų skelbimo	Rekomenduotinas tais atvejais, kai darbuotojas gali duoti sutikimą savo noru, pvz., dėl nuotraukų skelbimo
Poveikio duomenų apsaugai vertinimo procedūra	Nustatoma procedūra, kokiais atvejais ir kaip atliekamas bei fiksuojamas poveikio duomenų apsaugai vertinimas. Gali būti ne atskira tvarka, o kaip Asmens duomenų tvarkymo taisyklių dalis. VDAI rekomenduojama pavyzdinė poveikio duomenų apsaugai vertinimo ataskaitos forma prieinama čia[6]	Privaloma
Darbuotojų duomenų tvarkymo politika	Aprašomas darbuotojų duomenų tvarkymas	Privaloma (tačiau ne kaip atskiras dokumentas, gali būti ir Asmens duomenų tvarkymo taisyklių dalis)
Asmens duomenų saugumo pažeidimų procedūra	Nustatoma procedūra, kaip fiksuojami, tiriami asmens duomenų saugumo pažeidimai, kokiais atvejais pranešama VDAI bei kokiais atvejais – duomenų subjektui (-ams). Gali būti ne atskira tvarka, o kaip Asmens duomenų tvarkymo taisyklių dalis.	Privaloma

[5] VDAI 2018 m. Rekomendacija dėl duomenų tvarkymo veiklos įrašų.
[6] VDAI 2018 m. Pavyzdinė poveikio duomenų apsaugai atlikimo forma.

	Pranešimo apie pažeidimą VDAI rekomenduojama forma prieinama čia[7]	
Asmens duomenų saugumo pažeidimų registras	Registruojami asmens duomenų saugumo pažeidimai, juos aprašant	Privalomas
Vaizdo stebėjimo tvarka	Aprašomas vykdomas vaizdo stebėjimas, duomenų subjekto teisių įgyvendinimo procedūros ir kt.	Privaloma, jei vykdote vaizdo stebėjimą (atskira tvarka neprivaloma, nuostatos gali būti ir kitų dokumentų sudedamoji dalis)
IT saugumo politika	Aprašomos techninės ir organizacinės asmens duomenų saugumo priemonės	Privaloma (atskiras dokumentas nėra privalomas, tačiau Jūs privalote įmonėje aprašyti ir patvirtinti taikomas asmens duomenų saugumo priemones. Tokios priemonės gali būti ir kaip Asmens duomenų tvarkymo taisyklių dalis)

Pastaba: gali būti naudojami ir kiti rekomenduojami dokumentai. Lentelėje pateikiami tik pagrindiniai dokumentai, užtikrinantys BDAR atitiktį.

Tiek išorinių, tiek vidinių dokumentų nuostatos turėtų būti aiškios, išsamios ir lengvai suprantamos duomenų subjektui.

KIEK LAIKO TURIU SAUGOTI ASMENS DUOMENIS?

BDAR 5 straipsnio 1 dalies e punktas įtvirtina asmens duomenų saugojimo trukmės apribojimo principą.

Asmens duomenys saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu tai yra būtina tais tikslais, kuriais asmens duomenys buvo surinkti.

Išimtiniais atvejais asmens duomenis galima saugoti ilgiau archyvavimo tikslais, viešojo intereso labui arba mokslinių ar istorinių tyrimų tikslais, tačiau turi būti imamasi techninių ir organizacinių priemonių, kurios užtikrintų tokių duomenų saugumą (pvz., šifravimo ar pan.).

KAS NUSTATO DUOMENŲ SAUGOJIMO TERMINĄ?

BDAR įtvirtina tik bendrąjį principą dėl asmens duomenų saugojimo termino.

Konkretūs asmens duomenų saugojimo terminai gali būti įtvirtinti teisės aktuose (nacionaliniuose ar tarptautiniuose teisės aktuose) arba juos nustatyti turi pats duomenų valdytojas (įmonė).

Įmonei nustatant duomenų saugojimo terminą reikėtų atsižvelgti į tikslus, dėl kurių įmonei reikia tvarkyti duomenis, ir į visas teisines prievoles saugoti duomenis nustatytą laikotarpį. Taigi, duomenų valdytojas, įvertinęs atliekamą asmens duomenų tvarkymą ir tokio tvarkymo tikslus (duomenų saugojimo terminas gali skirtis priklausomai nuo duomenų tvarkymo tikslo), turi **išsiaiškinti, ar teisės aktai nenustato asmens duomenų saugojimo termino** (pvz., nacionaliniuose darbo, mokesčių ar kovos su sukčiavimu

[7] VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) patvirtinta Pranešimo apie duomenų saugumo pažeidimą forma.

įstatymuose nustatytą reikalavimą savo darbuotojų asmens duomenis saugoti nustatytą laikotarpį, produkto garantijos trukmę ir pan.).

Pavyzdžiai

- Sveikatos priežiūros įstaigos įpareigotos saugoti pacientų asmens duomenis Lietuvos Respublikos sveikatos ministro įsakyme „Dėl Lietuvos Respublikos sveikatos apsaugos ministro 1999 m. lapkričio 29 d. įsakymo Nr. 515 „Dėl Sveikatos priežiūros įstaigų veiklos apskaitos ir atskaitomybės tvarkos“ pakeitimo“ nustatytais terminais.
- Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo 19 straipsnio 9 dalyje numatyta, kad kliento tapatybę patvirtinančių dokumentų kopijos, sąskaitų ir (ar) sutarčių dokumentacija (dokumentų originalai) turi būti saugoma 10 metų nuo sandorių ar dalykinių santykių su klientu pabaigos dienos. Šio straipsnio 10 punkte nurodyta, kad kliento tapatybę patvirtinančių dokumentų kopijos, naudos gavėjo tapatybės duomenys, išmokos gavėjo tapatybės duomenys, tiesioginio vaizdo perdavimo (tiesioginės vaizdo transliacijos) įrašas, kiti duomenys, gauti kliento tapatybės nustatymo metu, sąskaitų ir (ar) sutarčių dokumentacija (dokumentų originalai) turi būti saugomi 8 metus nuo sandorių ar dalykinių santykių su klientu pabaigos dienos.

KOKS GALI BŪTI SAUGOJIMO TERMINAS?

Teisės aktuose gali būti nurodytas:

- **Maksimalus asmens duomenų saugojimo terminas.** Duomenų valdytojas šiuo atveju asmens duomenų negali saugoti ilgiau, negu yra nurodyta teisės akte, tačiau jis gali pasirinkti trumpesnį asmens duomenų saugojimo terminą. Pažymėtina, kad duomenų valdytojas privalo nusistatyti konkretų asmens duomenų saugojimo terminą, kuris negali viršyti teisės aktuose nurodyto maksimalaus termino;
- **Konkretus privalomas asmens duomenų saugojimo terminas.** Tuo atveju, jei teisės aktai neįtvirtina asmens duomenų saugojimo terminų, pagrįstą ir protingą asmens duomenų saugojimo terminą privalo nusistatyti pats duomenų valdytojas, vadovaudamasis BDAR 5 straipsnyje nustatytais principais.

Duomenų saugojimo terminai gali skirtis priklausomai nuo duomenų tvarkymo tikslo ir duomenų pobūdžio, pvz., vaizdo duomenis gali būti tikslinga saugoti kelias savaites, o sutarties vykdymo tikslu renkamus duomenis – keletą metų.

Asmens duomenų saugojimo terminas gali būti:

- Konkretus (pvz., 1 metai nuo duomenų subjekto sutikimo gavimo) arba
- Apibrėžtas tam tikrų aplinkybių atsiradimu ar išnykimu (pvz., 10 metų nuo sutarties galiojimo pabaigos).

Terminas gali būti nurodomas kalendorine data arba metais, mėnesiais, savaitėmis ar dienomis (pvz., iki 2015 m. sausio 1 d., 3 metai, 1 mėnuo, 2 savaitės, 10 kalendorinių dienų ir t. t.). Duomenų valdytojas turi nustatyti, nuo kada pradedamas skaičiuoti šis terminas (pvz., nuo sutarties sudarymo, nuo telefono pokalbio įrašo padarymo, nuo asmens duomenų gavimo dienos).

Pavyzdžiai

- Internetinėje parduotuvėje klientų asmens duomenys saugomi 1 metus nuo kliento paskutinio prisijungimo prie kliento paskyros.
- Parduotuvėje vykdomo vaizdo stebėjimo duomenys saugomi 14 kalendorinių dienų.
- Įmonėje vykdomo pokalbių telefonu įrašymo duomenys saugomi 2 mėnesius.

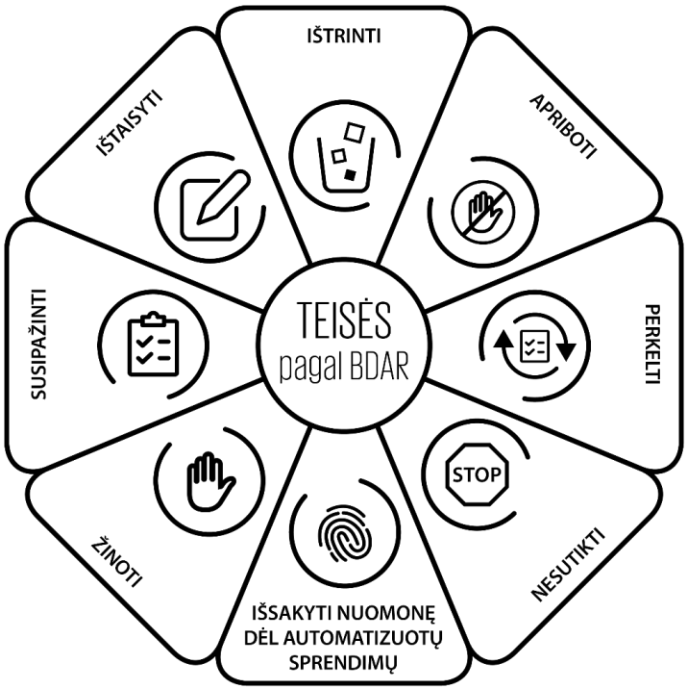
KAIP ELGTIS PASIBAIGUS DUOMENŲ SAUGOJIMO TERMINUI?

Pasibaigus nustatytiems duomenų saugojimo terminams, asmens duomenis privalote sunaikinti arba anonimizuoti. Todėl svarbu įdiegti procedūras, užtikrinančias, kad duomenys, pasibaigus jų saugojimo terminui, toliau nebebūtų tvarkomi.

Pavyzdžiai

Jūsų įmonė vykdo įdarbinimo agentūros veiklą, todėl renka darbo ieškančių asmenų gyvenimo aprašymus. Už savo tarpininkavimo paslaugas gaunate tam tikrą mokestį. Duomenis planuojate saugoti 10 metų, tačiau neturite jokių priemonių, kaip atnaujinti saugomus gyvenimo aprašymus. Saugojimo laikotarpis neatrodo proporcingas tikslui – rasti asmenims darbą trumpam arba vidutinės trukmės laikotarpiui. Be to, tai, kad reguliariai neprašote atnaujinti gyvenimo aprašymų, sumažina kai kurių paieškų veiksmingumą, jeigu asmuo pradeda ieškoti darbo po tam tikro laiko (pvz., asmuo gali būti įgijęs naujų kvalifikacijų).

DUOMENŲ SUBJEKTO TEISĖS IR JŲ ĮGYVENDINIMO TVARKA



BENDROSIOS DUOMENŲ SUBJEKTO TEISIŲ ĮGYVENDINIMO SĄLYGOS

Ar teisės įgyvendinamos nemokamai?

Įgyvendinant asmens teises visa informacija, pranešimai teikiami ir visi veiksmai atliekami nemokamai. Tačiau, jeigu asmens prašymai yra akivaizdžiai nepagrįsti arba neproporcingi, pvz., dėl jų pasikartojančio pobūdžio, Jūs galite elgtis dvejopai:

- Imti *pagrįstą* mokestį, atsižvelgdami į administracines išlaidas, už informacijos ar pranešimo teikimą arba prašomų veiksmų vykdymą; arba
- Atsisakyti imtis veiksmų pagal prašymą.

Svarbu įsidėmėti, kad pareiga įrodyti, kad prašymas yra akivaizdžiai nepagrįstas arba neproporcingas, tenka Jums. Paprastai, kaip tinkama įrodymų pateikimo priemonė, būtų laikomas **motyvuotas** atsakymas duomenų subjektui dėl atsisakymo įgyvendinti jo teises. Šį atsakymą, prireikus, galėsite pateikti priežiūros institucijai – VDAI.

Asmens tapatybės nustatymas ir atstovavimas

Jei turite pagrįstų abejonių dėl prašymą pateikusio fizinio asmens tapatybės, Jūs galite paprašyti pateikti papildomos informacijos, reikalingos norint patvirtinti asmens, kurio duomenis tvarkote, tapatybę (pvz., paspausti patvirtinimo nuorodą, įvesti vartotojo vardą ar slaptažodį ir pan.). Prašydami papildomos

informacijos Jūs turėtumėte jos prašyti tik tiek, kiek Jums yra būtina siekiant identifikuoti fizinį asmenį. Taigi turi būti išlaikytas proporcingumas.

Asmuo, kurio duomenys tvarkomi, savo teises gali įgyvendinti pats arba per atstovą. Jei asmens vardu į Jus kreipiasi asmens atstovas, jis savo prašyme turi nurodyti savo vardą, pavardę, duomenis ryšiui palaikyti, taip pat atstovaujamo asmens vardą, pavardę, informaciją apie tai, kokią asmens teisę ir kokia apimtimi pageidaujama įgyvendinti, ir pridėti atstovavimą patvirtinantį dokumentą ar jo kopiją, patvirtintą teisės aktų nustatyta tvarka.

Terminas, per kurį turi būti įgyvendintos duomenų subjekto teisės

Jeigu gavote fizinio asmens prašymą dėl teisės susipažinti su savo asmens duomenimis, teisės reikalauti ištaisyti duomenis, teisės reikalauti ištrinti duomenis („teisės būti pamirštam“), teisės reikalauti apriboti duomenų tvarkymą, teisės į duomenų perkeliamumą, teisės nesutikti, teisės reikalauti, kad asmeniui nebūtų taikomas automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą, įgyvendinimo, Jūs į jį turite atsakyti **nedelsdami**, tačiau ne vėliau kaip per **vieną mėnesį** nuo prašymo gavimo.

Tam tikromis aplinkybėmis (pvz., didelė duomenų apimtis ar kt.) terminą galima pratęsti dar dviem mėnesiais. Jei terminą būtina pratęsti, tuomet per vieną mėnesį nuo prašymo gavimo privalote pranešti asmeniui, kad terminas bus pratęsiamas ir nurodyti termino pratęsimo priežastį. Svarbu įsidėmėti, kad apie termino pratęsimą fiziniam asmeniui turėtumėte pranešti dar nepasibaigus vieno mėnesio terminui. Be to, reikėtų atkreipti dėmesį, kad, jeigu nesiimate veiksmų pagal duomenų subjekto prašymą, vieno mėnesio terminas **negali** būti pratęstas.

Kalendorinis mėnuo pradedamas skaičiuoti kitą dieną po to, kai įmonė gauna prašymą, net jei ta diena yra savaitgalis arba valstybinė šventė. Terminas baigiasi kito mėnesio atitinkamą dieną.

Jeigu mėnesis, kurio metu baigiasi atsakymo terminas, yra trumpesnis, tai atsakymo diena turėtų būti laikoma paskutinė to mėnesio diena.

Jeigu terminas atsakyti į prašymą baigiasi savaitgalį ar nedarbo dieną, Jūs turite atsakyti į prašymą kitą darbo dieną.

Pavyzdžiai

- Įmonė gauna prašymą rugsėjo 3 d. Terminas pradedamas skaičiuoti kitą dieną, rugsėjo 4 d. Įmonė turi iki spalio 4 d. įvykdyti prašymą. Tačiau, jei pabaigos data yra ne darbo arba šventinė diena, terminas baigiasi kitą darbo dieną.
- Įmonė gauna prašymą kovo 30 d. Terminas pradedamas skaičiuoti kitą dieną, kovo 31 d. Kadangi balandžio mėn. nėra lygiavertės datos, terminas baigiasi balandžio 30 d.

Veiksmai, nusprendus neįgyvendinti duomenų subjekto teisių

Jeigu nesiimate veiksmų pagal duomenų subjekto prašymą, Jūs apie tai duomenų subjektą turėtumėte informuoti **nedelsiant**, tačiau ne vėliau kaip per **vieną mėnesį** nuo prašymo gavimo dienos. Atsakydami duomenų subjektui Jūs turite:

- Pateikti *priežastis* (motyvaciją), dėl kurių nesiimate veiksmų prašymui įgyvendinti;
- Pateikti informaciją, kad duomenų subjektas turi teisę pateikti skundą VDAI arba teismui.

TEISĖ BŪTI INFORMUOTAM

Teisė būti informuotam apibrėžia, kokią informaciją Jūs turite pateikti duomenų subjektams, kai yra renkami ir tvarkomi jų asmens duomenys. Įgyvendindami teisę būti informuotam Jūs kartu įgyvendinate dalį iš teisėtumo, sąžiningumo ir skaidrumo principo kylančių pareigų. Nepamirškite, kad pareiga įrodyti, kad tinkamai informavote duomenų subjektą, kurio duomenis tvarkote, tenka Jums.

Informacija, kuri turi būti pateikta duomenų subjektui

BDAR išskiria du atvejus, kokia informacija turi būti pateikta duomenų subjektui:

- informacija, kuri turi būti pateikta, kai asmens duomenys renkami iš duomenų subjekto;
- informacija, kuri turi būti pateikta, kai asmens duomenys yra gauti ne iš duomenų subjekto.

Kokią informaciją turite pateikti?	Asmens duomenys renkami iš duomenų subjekto	Asmens duomenys yra gauti ne iš duomenų subjekto
Įmonės pavadinimą ir kontaktus	✓	✓
Duomenų apsaugos pareigūno, jeigu taikoma, kontaktinius duomenis	✓	✓
Duomenų tvarkymo tikslą (-us)	✓	✓
Duomenų tvarkymo teisinį pagrindą	✓	✓
Teisėtus interesus, kuriais remiantis tvarkomi asmens duomenys, jei taikoma	✓	✓
Asmens duomenų kategorijas		✓
Asmens duomenų gavėjus arba asmens duomenų gavėjų kategorijas	✓	✓
Informaciją apie ketinimą asmens duomenis perduoti į trečiąją valstybę arba tarptautinei organizacijai[8]	✓	✓
Asmens duomenų saugojimo laikotarpį arba, jei tai neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti	✓	✓
Teisę prašyti, kad įmonė leistų susipažinti su savo asmens duomenimis ir juos ištaisytų arba ištrintų, arba apribotų duomenų tvarkymą, arba teisę nesutikti, kad duomenys būtų tvarkomi, taip pat teisę į duomenų perkeliamumą	✓	✓
Teisę bet kuriuo metu atšaukti sutikimą, jei taikoma	✓	✓
Teisę pateikti skundą priežiūros institucijai (VDAI)	✓	✓
Ar asmens duomenų pateikimas yra teisės aktais arba sutartyje numatytas reikalavimas, ar reikalavimas, kurį būtina įvykdyti norint sudaryti sutartį, taip pat tai, ar asmuo, kurio duomenys tvarkomi, privalo pateikti asmens duomenis, ir informaciją apie	✓	

[8] Be šios informacijos Jūs turite pateikti informaciją apie Europos Komisijos sprendimo dėl tinkamumo buvimą ar nebuvimą, arba BDAR 46, 47 arba 49 straipsnio 1 dalies antroje pastraipoje nurodytų perdavimų atveju – tinkamas arba pritaikytas apsaugos priemones ir būdus, kaip gauti asmens duomenų kopiją arba kur suteikiama galimybė su jais susipažinti.

galimas tokių duomenų nepateikimo pasekmes		
Apie automatizuotą sprendimų priėmimą, įskaitant profiliavimą, apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes asmeniui	✓	✓
Koks yra asmens duomenų kilmės šaltinis, ir, jei taikoma, ar duomenys gauti iš viešai prieinamų šaltinių		✓

Jeigu ketinate tvarkyti asmens duomenis kitu tikslu, negu tas, kuriuo asmens duomenys buvo surinkti, prieš tai privalote pateikti duomenų subjektui, kurio duomenis tvarkysite, informaciją apie tą kitą tikslą ir visą kitą *atitinkamą* papildomą informaciją:

- Asmens duomenų saugojimo laikotarpį arba, jei tai neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti;
- Teisę prašyti susipažinti su savo asmens duomenimis ir juos ištaisyti arba ištrinti, arba apriboti duomenų tvarkymą, arba teisę nesutikti, kad duomenys būtų tvarkomi, taip pat teisę į duomenų perkeliamumą;
- Teisę bet kuriuo metu atšaukti sutikimą;
- Teisę pateikti skundą priežiūros institucijai (VDAI);
- Ar asmens duomenų pateikimas yra teisės aktais arba sutartyje numatytas reikalavimas, ar reikalavimas, kurį būtina įvykdyti norint sudaryti sutartį, taip pat tai, ar asmuo, kurio duomenys tvarkomi, privalo pateikti asmens duomenis, ir informaciją apie galimas tokių duomenų nepateikimo pasekmes;
- Apie automatizuotą sprendimų priėmimą, įskaitant profiliavimą, apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes asmeniui.

Pavyzdys

Asmens duomenys buvo surinkti iš asmens ir tvarkomi elektroninės prekybos tikslu, tačiau, nusprendus asmens duomenis tvarkyti ir tiesioginės rinkodaros tikslu, būtina gauti atskirą sutikimą dėl asmens duomenų tvarkymo tiesioginės rinkodaros tikslu, informuoti asmenį, kurio duomenys tvarkomi, kokiu tikslu asmens duomenys bus tvarkomi, kiek laiko bus saugomi, apie asmens teisę nesutikti, kad asmens duomenys būtų tvarkomi tiesioginės rinkodaros tikslu.

Informacijos pateikimo būdai

Informacija duomenų subjektui gali būti pateikiama įvairiais būdais[9]. Tinkamiausias ir patogiausias informacijos pateikimo būdas tiek Jums, tiek duomenų subjektui priklauso nuo konkrečių asmens duomenų tvarkymo aplinkybių. Įvertinkite duomenų rinkimo kontekstą. Neretai informaciją bus patogiausia pateikti tokiomis pačiomis priemonėmis, kokiomis rinkote asmens duomenis, pvz., informaciją galima pateikti sutartyje, interneto svetainėje, vartotojo paskyroje ar kt.

Rinkdamiesi būdą, kaip pateikti informaciją duomenų subjektui, galite naudotis skirtingomis priemonėmis, pavyzdžiui:

- Lygmeniniu pranešimu. Informacija pateikiama dalimis, išskiriant svarbiausią informaciją viename lygmenyje, o detalesnę – kituose, pvz., pirmiausia pateikiama svarbiausia informacija, o paspaudus mygtuką „skaitykite detaliau“, pateikiama detali informacija;
- Informacijos apie privatumą suvestinėmis (angl. *privacy dashboards*). Suvestinėse pateikiama informacija, kaip tvarkomi asmens duomenys ir jų privatumo nustatymai;

[9] Išsamesnes gaires apie tai, kaip turi būti pateikiama informacija galima rasti 29 straipsnio duomenų apsaugos darbo grupės 2017 m. lapkričio 29 d. *Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairėse* Nr. WP 260, 1 red.

- Reikiamu laiku (angl. *just-in-time*) teikiamais kontekstiniais iškylančiaisiais pranešimais. Aktuali ir svarbiausia informacija pateikiama tuo metu, kai renkami individualios asmens duomenų dalys;
- Standartizuotomis piktogramomis. Kai numatomas duomenų tvarkymas prasmingai apibendrintas piktogramomis lengvai matomu, suprantamu ir aiškiai įskaitomu būdu.

Pavyzdys

Jei įmonė vykdo vaizdo stebėjimą, asmeniui, prieš patenkant į vaizdo stebėjimo lauką, turi būti pateikiama informacija apie vykdomą vaizdo stebėjimą, jį vykdančios įmonės (duomenų valdytojo) pavadinimas, kontaktinė informacija (adresas, el. pašto adresas ir (arba) telefono ryšio numeris, vaizdo stebėjimo tikslas, nuoroda į informacijos šaltinį, kur būtų galima gauti detalesnę informaciją apie vykdomą vaizdo stebėjimą, pvz., nuoroda į interneto svetainę ar kt.

Kita informacija gali būti pateikiama, pvz., įmonės interneto svetainėje, privatumo politikoje, asmens duomenų tvarkymo taisyklėse ar pan.

Informacijos duomenų subjektui pateikimo laikas

Laikas, kada duomenų subjektas turi būti informuotas apie asmens duomenų tvarkymą, priklauso nuo to, iš kur gaunami asmens duomenys bei kaip ketinate juos tvarkyti. Tai atvejais, kai asmens duomenis renkate tiesiogiai iš duomenų subjekto, informacija turi būti pateikta iš karto – duomenų gavimo metu.

Tais atvejais, kai asmens duomenis gaunate ne iš duomenų subjekto, o kito šaltinio, informacija duomenų subjektui turi būti pateikta:

- Per *pagrįstą* laikotarpį, kai gaunami asmens duomenys, ir ne vėliau kaip per *vieną mėnesį*;
- Jeigu asmens duomenis naudosite ryšiams su asmeniu palaikyti – ne vėliau kaip *pirmą kartą* susisiekiant su tuo duomenų subjektu;
- Jei planuojate atskleisti informaciją kitiems (duomenų gavėjams) – ne vėliau kaip atskleidžiant duomenis *pirmą kartą*.

Teisės būti informuotam išimtys

Kai asmens duomenys renkami iš duomenų subjekto, informacija neteikiama tuo atveju, jeigu asmuo tokią informaciją jau turi ir tiek, kiek jos turi.

Gavus asmens duomenis ne iš paties duomenų subjekto, nereikalaujama pateikti informacijos apie jo asmens duomenų tvarkymą, jei:

- Asmuo jau turi informaciją;
- Informacijos pateikimas duomenų subjektui būtų neįmanomas arba pareikalautų neproporcingų pastangų, arba jeigu dėl pareigos informuoti duomenų subjektą gali tapti neįmanoma arba ji gali labai sukliudyti pasiekti tvarkymo tikslus. Tokiais atvejais duomenų valdytojas imasi tinkamų priemonių duomenų subjekto teisėms ir laisvėms ir teisėtiems interesams apsaugoti, įskaitant viešą informacijos paskelbimą. Svarbu atkreipti dėmesį, kad, jeigu tvarkote asmens duomenis dideliu mastu ir naudojatės šia išimtimi, Jūs turėsite atlikti poveikio duomenų apsaugai vertinimą[10];
- ES ar Lietuvos teisės aktais reikalaujama, kad Jūs gautumėte ar atskleistumėte asmens duomenis;
- Jūs privalote išlaikyti asmens duomenų konfidencialumą, nes Jums taikomas profesinės paslapties reikalavimas, kurį reglamentuoja teisės aktai ar įstatai.

TEISĖ SUSIPAŽINTI SU SAVO DUOMENIMIS

Duomenų subjektas, kurio duomenis renkate ir tvarkote, turi teisę susipažinti su *savo* asmens duomenimis ir gauti jų kopiją bei bet kokią susijusią papildomą informaciją

[10] Ši pareiga kyla iš Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo, patvirtinto VDAI direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T-35 (1.12.E).

(pvz., asmens duomenų tvarkymo priežastį, naudojamų asmens duomenų kategorijas ir pan.).

Duomenų subjektas turi teisę iš Jūsų gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis ir gauti informaciją apie:

- Duomenų tvarkymo tikslus;
- Asmens duomenų kategorijas;
- Duomenų gavėjus arba duomenų gavėjų kategorijas, kuriems buvo arba bus atskleisti asmens duomenys;
- Kai įmanoma, numatomą asmens duomenų saugojimo laikotarpį arba, jei neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti;
- Teisę prašyti Jūsų ištaisyti arba ištrinti asmens duomenis ar apriboti su asmeniu susijusių asmens duomenų tvarkymą arba nesutikti su tokiu tvarkymu;
- Teisę pateikti skundą priežiūros institucijai (VDAI);
- Kai asmens duomenys renkami ne iš asmens, visą turimą informaciją apie jų šaltinius;
- Tai, kad naudojamas automatizuotas sprendimų priėmimas (įskaitant profiliavimą) ir informaciją apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes asmeniui.

Pavyzdys

Duomenų subjektas, pasinaudodamas įmonės internetiniu puslapiu, išsinuomojo automobilį. Įmonė duomenų subjekto paprašė pateikti mokėjimo kortelės nuotrauką. Duomenų subjektas paprašė paaiškinti, kokiu tikslu įmonei reikalinga mokėjimo kortelės nuotrauka su joje esančiais asmens duomenimis. Įmonė atsakė, kad mokėjimo kortelės nuotrauka reikalinga, nes tai yra normali praktika. Toks įmonės atsakymas yra netinkamas, įmonė nepateikė *pagrįsto ir aiškaus* atsakymo, kokiu tikslu yra tvarkomi asmens duomenys.

Duomenų subjektas turi teisę susipažinti tik su *savo* asmens duomenimis, todėl turėtumėte įsitikinti asmens, prašančio leisti susipažinti su savo asmens duomenimis, tapatybe, ypač kai tai susiję su interneto paslaugomis ir interneto identifikatoriais, pvz., įmonė, administruojanti internetinę parduotuvę, gavusi asmens prašymą susipažinti su savo asmens duomenimis ir siekdama nustatyti asmens tapatybę, turėtų sutikrinti įmonėje tvarkomus šio asmens duomenis su prašyme pateiktais duomenimis (esant abejonėms, įmonė gali paprašyti asmens pateikti papildomos informacijos, reikalingos norint patvirtinti duomenų subjekto tapatybę).

TEISĖ REIKALAUTI IŠTAISYTI DUOMENIS

Duomenų subjektas, kurio duomenis tvarkote, turi teisę reikalauti, kad nepagrįstai nedelsdami ištaisytumėte netikslius su juo susijusius asmens duomenis. Atsižvelgiant į tikslus, kuriais duomenys buvo tvarkomi, duomenų subjektas turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys, pateikdamas papildomą prašymą.

Prisiminkite, kad Jūs privalote informuoti kitus duomenų valdytojus, kuriems atskleidėte Jums prašymą pateikusio duomenų subjekto asmens duomenis, apie asmens duomenų ištaisymą, *nebent* to padaryti nebūtų įmanoma arba tai pareikalautų neproporcingų pastangų. Duomenų subjektui pageidaujant, turėtumėte informuoti jį apie tuos duomenų gavėjus.

TEISĖ REIKALAUTI IŠTRINTI DUOMENIS („TEISĖ BŪTI PAMIRŠTAM“)

Duomenų subjektas turi teisę reikalauti, kad nepagrįstai nedelsiant būtų ištrinti su juo susiję asmens duomenys. Jūs esate įpareigoti nepagrįstai nedelsdami patenkinti

duomenų subjekto prašymą ir ištrinti jo asmens duomenis (ši teisė, dažnai vadinama *teise būti pamirštam*) šiais atvejais:

- Kai asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi;
- Duomenų subjektas atšaukia sutikimą ir nėra jokio kito teisinio pagrindo tvarkyti duomenis;
- Duomenų subjektas nesutinka su duomenų tvarkymu ir nėra viršesnių teisėtų priežasčių tvarkyti duomenis arba asmuo, kurio duomenys tvarkomi, nesutinka su duomenų tvarkymu tiesioginės rinkodaros tikslu (įskaitant profiliavimą, kiek jis susijęs tokia tiesiogine rinkodara);
- Asmens duomenys buvo tvarkomi neteisėtai;
- Asmens duomenys turi būti ištrinti laikantis ES ir Lietuvos teisės aktuose nustatytos teisinės prievolės;
- Asmens duomenys buvo surinkti *iš vaiko*, kuriam buvo siūlomos *informacinės visuomenės paslaugos*[11].

Teisė reikalauti ištrinti duomenis ypač svarbi tais atvejais, kai asmuo savo sutikimą išreiškė būdamas vaikas ir nevisiškai suvokdamas su duomenų tvarkymu susijusius pavojus. Asmuo turi teisę reikalauti, kad informacija apie jį, kurią jis suteikė būdamas vaikas, būtų ištrinta ir tuo atveju, kai jis nebėra vaikas.

Pavyzdys

Vaikas, norėdamas žaisti internetinius žaidimus, užsiregistravo interneto svetainėje, teikiančioje tokias paslaugas. Taigi, vaiko pateiktus asmens duomenis tvarko šią svetainę administruojanti įmonė. Jeigu vaikas, tapęs pilnamečiu, išreikš norą sunaikinti savo asmens duomenis, interneto svetainę administruojanti įmonė privalės ištrinti asmens duomenis.

Teisės būti pamirštam išimtys

Teisė būti pamirštam nėra absoliuti teisė, tai reiškia, kad ši teisė gali būti neįgyvendinta, jei yra šios sąlygos:

- Asmens duomenų tvarkymas yra būtinas siekiant pasinaudoti teise į saviraiškos ir informacijos laisvę;
- Asmens duomenų tvarkymas yra būtinas, nes Jūs esate įpareigoti tvarkyti asmens duomenis pagal teisės aktus siekdami atlikti užduotį, vykdomą viešojo intereso labui, arba vykdydami Jums pavestas viešosios valdžios funkcijas;
- Kai tvarkyti asmens duomenis būtina arba darbo medicinos tikslais, siekiant įvertinti darbuotojo darbingumą, nustatyti medicininę diagnozę, teikti sveikatos priežiūros arba socialinės rūpybos paslaugas ar gydymą, arba valdyti sveikatos priežiūros ar socialinės rūpybos sistemas ir paslaugas, remiantis teisės aktais arba pagal sutartį su sveikatos priežiūros specialistu[12];
- Archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, jeigu dėl teisės būti pamirštam gali tapti neįmanoma arba ji gali labai sukliudyti pasiekti tvarkymo tikslus;
- Siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus.

[11] Informacinės visuomenės paslaugos – bet kuri informacinės visuomenės paslauga, t. y. paprastai už atlyginimą per atstumą, elektroninėmis priemonėmis ir asmenišku paslaugų gavėjo prašymu teikiama paslauga.

[12] Tik tuo atveju, jeigu asmens duomenis tvarko specialistas, kuriam pagal teisės aktus arba nacionalinių kompetentingų įstaigų nustatytas taisykles taikoma pareiga saugoti profesinę paslaptį, arba duomenys tvarkomi jo atsakomybe, arba kitas asmuo, kuriam pagal teisės aktus arba nacionalinių kompetentingų įstaigų nustatytas taisykles taip pat taikoma pareiga saugoti paslaptį, pvz., gydytojas.

Pavyzdys

Įmonė gauna kliento prašymą ištrinti visus jo asmens duomenis, tačiau bendrovei yra taikomas įstatymas, įpareigojantis 10 metų saugoti visų klientų duomenis, todėl kliento duomenys galės būti ištrinti tik pasibaigus įstatyme nustatytam terminui.

Informavimas apie asmens duomenų (ne)ištrynimą

Kai Jūs asmens duomenis *paskelbėte viešai* ir šie duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi, privalote asmens duomenis ištrinti. Jūs privalote, atsižvelgdami į turimas technologijas ir įgyvendinimo sąnaudas, imtis pagrįstų veiksmų, įskaitant technines priemones, kad *informuotumėte kitus duomenis tvarkančius duomenų valdytojus*, jog duomenų subjektas paprašė, kad tokie duomenų valdytojai ištrintų visas nuorodas į tuos asmens duomenis arba jų kopijas ar dublikatus.

Jūs taip pat privalote informuoti kitus duomenų valdytojus, kuriems atskleidėte Jums prašymą pateikusio duomenų subjekto asmens duomenis, apie asmens duomenų ištrynimą, nebent to padaryti nebūtų įmanoma arba tai pareikalautų neproporcingų pastangų. Duomenų subjektui paprašius, turėtumėte informuoti jį apie tuos duomenų gavėjus.

Jei nusprendėte, kad ištrinti asmens duomenis nėra pagrindo, Jūs turite informuoti duomenų subjektą ir paaiškinti, kodėl manote, kad neturite ištrinti asmens duomenų, ir informuoti apie teisę pateikti skundą dėl šio sprendimo priežiūros institucijai (VDAI) ar teismui.

TEISĖ APRIBOTI DUOMENŲ TVARKYMĄ

Teisė apriboti duomenų tvarkymą suteikia galimybę duomenų subjektui kreipiantis į Jus laikinai apriboti jo asmens duomenų tvarkymą. Tačiau ši teisė nėra absoliuti ir gali būti įgyvendinti esant vienai iš šių sąlygų:

- Duomenų subjektas, kurio duomenys tvarkomi, užginčija duomenų tikslumą tokiam laikotarpiui, per kurį galite patikrinti asmens duomenų tikslumą;
- Asmens duomenų tvarkymas yra *neteisėtas* ir duomenų subjektas, kurio duomenis tvarkote, nesutinka, kad duomenys būtų ištrinti, ir vietoj to prašo apriboti jų naudojimą;
- Jums nebereikia asmens duomenų nustatytais tvarkymo tikslais, tačiau jų reikia duomenų subjektui, kurio duomenis tvarkote, siekiančiam pareikšti, vykdyti arba apginti teisinius reikalavimus;
- Duomenų subjektas, kurio duomenis tvarkote, paprieštaravo duomenų tvarkymui, kol bus patikrinta, ar teisėtos asmens duomenų tvarkymo priežastys, kuriomis Jūs remiatės, yra viršesnės už duomenų subjekto, kurio duomenis tvarkote, priežastis.

Kai duomenų tvarkymas yra apribotas, asmens duomenų negalima tvarkyti, *išskyrus saugojimą*, pvz., perduoti duomenų gavėjams, keisti, trinti ir pan. Tačiau šio reikalavimo galite nesilaikyti ir asmens duomenis galite tvarkyti, jei:

- Gavote duomenų subjekto, kurio duomenis tvarkote, sutikimą;
- Siekiate pareikšti, vykdyti arba apginti teisinius reikalavimus;
- Siekiate apsaugoti kito fizinio ar juridinio asmens teises;
- Duomenys yra reikalingi dėl svarbaus viešojo intereso.

Svarbu taip pat nepamiršti, kad Jūs privalote informuoti kitus duomenų valdytojus, kuriems atskleidėte Jums prašymą pateikusio duomenų subjekto asmens duomenis, apie duomenų apribojimą, *nebent* to padaryti nebūtų įmanoma arba tai pareikalautų neproporcingų pastangų. Duomenų subjektui pageidaujant, turėtumėte informuoti jį apie tuos duomenų gavėjus.

Būdai, kaip gali būti apribotas asmens duomenų tvarkymas

Duomenų subjekto asmens duomenų tvarkymą galite apriboti naudodamiesi šiais būdais (sąrašas nebaigtinis):

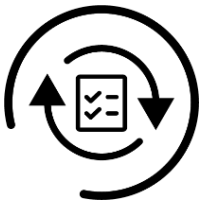
- Laikinai perkelti atrinktus asmens duomenis į kitą tvarkymo sistemą;
- Padaryti asmens duomenis neprieinamus informacinės sistemos naudotojams;
- Laikinai išimti viešai paskelbtus asmens duomenis iš interneto svetainės.

Pavyzdys

Duomenų subjektas kreipėsi į įmonę su prašymu apriboti jo asmens duomenų tvarkymą, nes mano, kad įmonės tvarkomoje informacinėje sistemoje duomenys yra netikslūs. Vykdant duomenų subjekto prašymą informacinėje sistemoje, konkretaus duomenų subjekto byloje, yra pažymima, kad asmens duomenų tvarkymas apribotas, tokiu būdu užtikrinant, kad asmens duomenys nebus ištrinti, pakeisti, pateikti kitoms įmonėms ir pan.

Veiksmai panaikinant asmens duomenų tvarkymo apribojimą

Jeigu duomenų subjekto prašymas apriboti duomenų tvarkymą buvo patenkintas, tai prieš panaikindami apribojimą tvarkyti asmens duomenis, Jūs apie tai turite informuoti duomenų subjektą, kurio asmens duomenų tvarkymą buvote apribojęs. Taip pat, kaip ir duomenų apribojimo atveju, prieš panaikindami apribojimą, Jūs turite informuoti kitus duomenų valdytojus, kuriems atskleidėte Jums prašymą pateikusio duomenų subjekto asmens duomenis, *nebent* to padaryti nebūtų įmanoma arba tai pareikalautų neproporcingų pastangų.



TEISĖ Į DUOMENŲ PERKELIAMUMĄ

Duomenų subjektas turi teisę į duomenų perkeliamumą[13], jei Jums duomenų subjektas asmens duomenis pateikė susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu bei Jūs juos tvarkote su jo **sutikimu** arba vykdydami **sutartį**. Be to, ši duomenų subjekto teisė gali būti įgyvendinti tik, jei asmens duomenis tvarkote *automatizuotomis priemonėmis ir kai tai techniškai įmanoma*. Šios teisės įgyvendinimas neturi daryti neigiamo poveikio kitų teisėms ir laisvėms.

Asmuo, kurio asmens duomenis tvarkote, turi teisę susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu:

- Gauti savo asmens duomenų kopiją; ir (ar)
- Prašyti, kad persiųstumėte asmens duomenis kitam duomenų valdytojui, kai tai techniškai įmanoma.

Pavyzdys

Įmonė, tvarkanti internetinį socialinį tinklą, esant asmens prašymui turi perkelti jo asmens duomenis naujajam internetiniam socialiniam tinklui, įskaitant nuotraukas.

TEISĖ NESUTIKTI

Duomenų subjektas turi teisę dėl su jo konkrečiu atveju susijusių priežasčių *bet kuriuo metu* nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi, kai toks asmens duomenų tvarkymas vykdomas remiantis *užduotimi, vykdoma viešojo intereso labui, Jums pavestomis viešosios valdžios funkcijomis arba teisėtais Jūsų arba trečiosios šalies interesais, įskaitant* ir profiliavimą, atliekamą remiantis paminėtais pagrindais.

Asmeniui išreiškus nesutikimą dėl jo asmens duomenų tvarkymo, Jūs privalote nutraukti asmens duomenų tvarkymą, išskyrus šiuos atvejus:

- Jei įrodote, kad asmens duomenys turi būti toliau tvarkomi dėl įtikinamų teisėtų priežasčių, kurios yra viršesnės už asmens, kurio asmens duomenis tvarkote, interesus, teises ir laisves;

[13] Daugiau informacijos rasite 29 straipsnio duomenų apsaugos darbo grupės 2017 m. balandžio 5 d. Teisės į duomenų perkeliamumą gairėse Nr. WP 242 rev.01.

- Siekiate pareikšti, vykdyti ar apginti teisinius reikalavimus.

Asmuo, kurio duomenys tvarkomi, apie nurodytą teisę aiškiai informuojamas ne vėliau kaip pirmą kartą susisiekiant su juo, ir ši informacija pateikiama aiškiai ir atskirai nuo visos kitos informacijos.

Jeigu asmuo kreipiasi į Jus ir nesutinka, kad jo asmens duomenys būtų tvarkomi tiesioginės rinkodaros tikslais, Jūs privalote nemokamai patenkinti asmens prašymą ir nutraukti asmens duomenų tvarkymą, įskaitant ir profiliavimą, kiek jis susijęs su tiesiogine rinkodara. Šiuo atveju, pirmiau nurodytos išimtys, kada teisė nesutikti gali būti neįgyvendinta, **negali** būti taikomos.

Pavyzdys

Asmuo internetinėje bilietų pardavimo įmonėje nusipirko du bilietus į savo mėgstamos grupės koncertą. Vėliau jis informuojamas apie jo nedominančius koncertus ir renginius. Asmuo informuoja internetinę bilietų pardavimo įmonę, kad daugiau nebenori gauti pasiūlymų. Įmonė turėtų nutraukti asmens duomenų tvarkymą tiesioginės rinkodaros tikslais ir nebesiųsti jokių pasiūlymų. Ši paslauga privalo būti nemokama.

BDAR nustato specialius reikalavimus, jeigu asmens duomenis tvarkote mokslinių ar istorinių tyrimų arba statistiniais tikslais. Tokiu atveju asmuo dėl su jo konkrečiu atveju susijusių priežasčių turi teisę nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi, *išskyrus*, kai asmens duomenis tvarkote siekdami atlikti užduotį, vykdomą dėl viešojo intereso priežasčių.

AUTOMATIZUOTAS ATSKIRŲ SPRENDIMŲ PRIĖMIMAS, ĮSKAITANT PROFILIAVIMĄ

BDAR riboja automatizuotų atskirų sprendimų priėmimą, įskaitant profiliavimą, jei dėl to duomenų subjektui kyla *teisinės pasekmės* arba kuris jam panašiu būdu daro *didelį poveikį*.[14]

Sprendimų priėmimas tik automatizuotu būdu reiškia, kad sprendimai bus priimami technologinėmis priemonėmis, tokiomis kaip algoritmai, *be jokio žmogaus įsikišimo*.

Profiliavimas atliekamas tada, kai vertinami duomenų subjekto asmeniniai aspektai, kad būtų padarytos prognozės, net jeigu nebus priimtas joks sprendimas, pvz., jeigu įmonė vertina asmens savybes (kaip antai, amžių, lytį ar ūgį) arba skirsto į tam tikras kategorijas, tai reiškia, kad asmeniui taikomas profiliavimas.

Tačiau ribojimas dėl automatizuoto atskirų sprendimų priėmimo, įskaitant profiliavimą, **netaikomas, jeigu** sprendimas:

- Yra *būtinas*, siekiant sudaryti arba vykdyti sutartį tarp asmens ir Jūsų;
- Yra leidžiamas teisės aktais, kurie taikomi Jums;
- Yra pagrįstas aiškiu asmens, kurio duomenis tvarkote, sutikimu.

Išskyrus atvejus, kai automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą, yra leidžiamas teisės aktais, Jūs turite:

- Suteikti duomenų subjektui galimybę reikalauti, kad sprendimą peržiūrėtų žmogus;
- Suteikti duomenų subjektui galimybę išreikšti savo nuomonę ir ginčyti priimtą sprendimą.

Pavyzdys

Įmonėje, sprendžiant, ar samdyti darbuotoją, naudojamas testas, kurio atsakymai įvertinami ir sprendimas pateikiamas be žmogaus įsikišimo, naudojant iš anksto nustatytus kriterijus ir algoritmus. Tokiu atveju asmuo turėtų būti informuojamas apie automatizuotą sprendimą, jam turėtų būti suteikta

[14] Daugiau informacijos apie šią teisę rasite 29 straipsnio darbo grupės 2018 m. vasario 6 d. Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairėse Nr. WP251.

galimybė, kad jį peržiūrėtų žmogus ir jis galėtų pareikšti savo nuomonę ir ginčyti automatizuotą sprendimą.

Automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą, grindžiamas *specialių kategorijų* asmens duomenų tvarkymu, galimas, jeigu esate nustatę tinkamas priemones asmens teisėms bei laisvėms ir teisėtiems interesams apsaugoti ir asmuo davė savo aiškų sutikimą arba tvarkyti duomenis būtina dėl svarbaus viešojo intereso priežasčių, remiantis teisės aktais.

DUOMENŲ VALDYTOJŲ PAREIGOS

Asmens duomenų tvarkymas yra grindžiamas Jūsų, kaip duomenų valdytojo, bei Jūsų pasitelktų duomenų tvarkytojų, atskaitomybe, todėl BDAR *pagal vykdomo asmens duomenų tvarkymo aplinkybes*, be jau anksčiau šiose gairėse aptartų pareigų, nustato šias pareigas:

- Paskirti **duomenų apsaugos pareigūną** (žr. skyrių „Duomenų apsaugos pareigūno skyrimas“);
- Jeigu pasitelkiate duomenų tvarkytoją, jo atliekamą asmens duomenų tvarkymą reglamentuoti **sutartimi**;
- Tvarkyti **duomenų tvarkymo veiklos įrašus**, kuriuose būtų detaliai aprašytas atliekamas asmens duomenų tvarkymas (žr. VDAI rekomendaciją „Dėl duomenų tvarkymo veiklos įrašų“);
- *Prieš* pradedant tvarkyti asmens duomenis, atlikti numatytų duomenų tvarkymo operacijų **poveikio asmens duomenų apsaugai vertinimą** (žr. skyrių „Poveikio duomenų apsaugai vertinimas“);
- Pranešti apie **asmens duomenų saugumo pažeidimą** VDAI, kai dėl jo gali kilti pavojus fizinių asmenų teisėms ir laisvėms, ir duomenų subjektui, kai dėl jo gali kilti *didelis* pavojus fizinių asmenų teisėms ir laisvėms (žr. VDAI rekomendaciją „Dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos“).

DUOMENŲ APSAUGOS PAREIGŪNO SKYRIMAS

Kada turi būti skiriamas duomenų apsaugos pareigūnas?

Jūs *privalote* paskirti DAP[15], esant bent vienam iš šių atvejų:

1. Asmens duomenis tvarko **valdžios institucija ar įstaiga**, išskyrus teismus, t. y. valstybės ir savivaldybių institucijos ir įstaigos, įmonės ir viešosios įstaigos, finansuojamos iš valstybės ar savivaldybių biudžetų bei valstybės pinigų fondų ir Lietuvos Respublikos viešojo administravimo įstatymo nustatyta tvarka įgaliotos atlikti viešąjį administravimą arba teikiančios asmenims viešąsias ar administracines paslaugas ar vykdančios kitas viešąsias funkcijas.
2. Jūsų **pagrindinė veikla** yra asmens duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina **reguliariai** ir **sistemingai dideliu mastu stebėti** duomenų subjektus. Jūsų *pagrindinė* veikla suprantama kaip svarbiausia veikla Jūsų tikslams pasiekti, kurioje asmens duomenų tvarkymas sudaro *neatskiriamą* Jūsų veiklos dalį ar nėra atliekamas kaip *papildoma* veikla. Vertindami, ar vykdote *reguliarų ir sistemingą stebėjimą*, turėtumėte atsižvelgti į tai, ar duomenų tvarkymas: atliekamas tam tikrais intervalais konkrečiu laikotarpiu; vykstantis nuolat; yra pasikartojantis tam tikrais periodais; vykstantis pagal tam tikrą sistemą; yra iš anksto suplanuotas, metodiškas; yra vykdomas kaip strategijos dalis. Nustatyti, ar duomenų tvarkymą vykdote *dideliu mastu*, gali padėti šie veiksniai – susijusių duomenų subjektų konkretus skaičius arba gyventojų skaičiaus procentinė dalis; tvarkomų asmens duomenų kiekis ir (ar) intervalas; asmens duomenų tvarkymo veiklos trukmė ir pastovumas; geografinė asmens duomenų tvarkymo aprėptis ir pan. Atminkite, kad DAP turite paskirti, kai yra **visos** aptartos sąlygos.

[15] Daugiau informacijos dėl DAP skyrimo rasite 29 straipsnio darbo grupės 2016 m. gruodžio 13 d. *Duomenų apsaugos pareigūnų gairėse*.

3. Jūsų **pagrindinė veikla** yra **specialių kategorijų asmens duomenų** tvarkymas **dideliu mastu**. Specialių kategorijų asmens duomenims priskiriami duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose, taip pat genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie asmens lytinį gyvenimą ar lytinę orientaciją. Pagrindinė veikla ir didelis mastas turėtų būti vertinamas atsižvelgiant į pirmiau aptartus kriterijus.

4. Jūsų **pagrindinė veikla** yra asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas **dideliu mastu**. Pagrindinė veikla ir didelis mastas turėtų būti vertinamas atsižvelgiant į pirmiau aptartus kriterijus.

Pavyzdžiai, kai „asmens duomenų tvarkymas – pagrindinė veikla“

- Privati apsaugos paslaugų įmonė vykdo prekybos centrų ir viešųjų erdvių vaizdo stebėjimą. Vaizdo stebėjimas yra įmonės pagrindinė veikla, kuri savo ruožtu yra susijusi su asmens duomenų tvarkymu. Taigi, ši įmonė turi paskirti DAP.
- Privačios sveikatos priežiūros įstaigos pagrindinė veikla – teikti sveikatos priežiūros paslaugas viso miesto ir rajono gyventojams. Sveikatos priežiūros įstaiga, siekdama tinkamai teikti šias paslaugas, pagal teisės aktus privalo tvarkyti tam tikrus pacientų asmens duomenis. Taigi, asmens duomenų tvarkymas būtų laikomas pagrindine ir neatsiejama sveikatos priežiūros įstaigos veikla. Vertinant tai, kad sveikatos paslaugos teikiamos viso miesto ir rajono mastu, manytina, kad asmens duomenų tvarkymas būtų vykdomas dideliu mastu. Pagal teisės aktus sveikatos priežiūros įstaiga pildo asmens sveikatos istoriją, o tai vertintina kaip reguliarus ir sistemingas asmens stebėjimas. Taigi, aptariamu atveju sveikatos priežiūros įstaiga turi paskirti duomenų apsaugos pareigūną.
- Visos įmonės vykdo tam tikrą veiklą, pvz., moka darbo užmokestį savo darbuotojams arba vykdo standartinę informacinių sistemų priežiūros veiklą. Tai yra pagrindinei įmonės veiklai reikalingų pagalbinių funkcijų pavyzdžiai. Nors ši veikla yra reikalinga arba būtina, ji paprastai laikoma pagalbinėmis funkcijomis, o ne pagrindine veikla, todėl tokiais atvejais DAP neturėtų būti skiriamas.

Pavyzdžiai, kai „asmens duomenys tvarkomi dideliu mastu“

- Asmuo, užsiimantis individualia veikla, internete prekiauja savo užauginta produkcija viename mieste ir naudojasi informacinių technologijų paslaugas teikiančios įmonės paslaugomis, kuri prižiūri šio asmens internetinį tinklalapį bei teikia tikslinės reklamos ir tiesioginės rinkodaros paslaugas individualia veikla užsiimančio asmens klientams. Tokio asmens, užsiimančio individualia veikla, atliekamas asmens duomenų tvarkymas nebus laikomas didelio masto, tačiau IT paslaugas teikiančios įmonės, kaip duomenų tvarkytojo, kuris turi daug tokio pobūdžio klientų, veikla, atsižvelgiant į aptarnaujamų klientų ir jų duomenų subjektų skaičių, gali būti laikoma kaip vykdoma dideliu mastu ir tokia įmonė turės paskirti DAP.
- Įmonė, teikianti odontologines paslaugas, įsikūrusi Pasvalio mieste. Jos klientai (pacientai) yra tik šio miesto gyventojai. Įmonėje dirba penki darbuotojai – odontologai. Vertinant duomenų subjektų skaičių, geografinę duomenų tvarkymo veiklos aprėptį ir pan. aspektus, toks pacientų asmens duomenų tvarkymas neturėtų būti laikomas kaip vykdomas dideliu mastu ir tokia įmonė neturės pareigos paskirti DAP.

Pavyzdys, kai „asmens duomenų tvarkymas susijęs su reguliariu ir sistemingu stebėjimu“

- Įmonė lojalumo programos vykdymo tikslu tvarko klientų asmens duomenis, įskaitant ir jų pirkimo istorijos duomenis. Klientai gali būti nustatyti pagal jų pirkimo įpročius, jie yra profiliuojami, siekiant išanalizuoti ar prognozuoti jų asmeninius pomėgius, elgesį, įpročius ir pan. Tokiu atveju laikytina, kad vykdoma reguliari ir sisteminga duomenų subjektų – klientų, elgesio stebėsena ir DAP paskirti yra būtina.

Net kai pagal BDAR nereikalaujama paskirti DAP, Jums gali būti naudinga jį paskirti savanoriškai. Be to, Jūs, nors ir neprivalėdami paskirti DAP ar nenorėdami jo paskirti savanoriškai, galite įdarbinti asmenis arba samdyti išorės konsultantus, kuriems būtų pavestos su asmens duomenų apsauga susijusios

užduotys. Šiuo atveju svarbu užtikrinti, kad nekiltų nesusipratimų dėl tokių asmenų pareigų pavadinimo ir statuso. Todėl visuose įmonės vidaus pranešimuose ir bendraujant su VDAI, duomenų subjektais ir (ar) plačiąja visuomene reikėtų aiškiai nurodyti, kad šis darbuotojas ar išorinis konsultantas nėra DAP.

Kas gali būti duomenų apsaugos pareigūnu?

DAP gali būti skiriamas:

- **Jūsų darbuotojas.** Šiuo atveju privalo būti užtikrinta, kad dėl DAP atliekamų pareigų ir (ar) vykdomų užduočių *nekiltų interesų konfliktas*, t. y. DAP negali būti skiriamas darbuotojas, kuris nustato asmens duomenų tvarkymo tikslus ir priemones. Dėl kiekvienos įmonės specifinės struktūros į tai turi būti atsižvelgiama kiekvienu konkrečiu atveju. Paprastai interesų konfliktą galinčiomis sukelti pareigomis laikomos, pvz., įmonės vadovo, operacijų vadovo, vyriausiojo finansininko, rinkodaros padalinio vadovo, žmogiškųjų išteklių, informacinių technologijų padalinio vadovo ar kitos panašios pareigos.
- **Išorinis paslaugų teikėjas**, t. y. atlikti DAP užduotis, sudarant paslaugų teikimo sutartį, pavedama individualia veikla užsiimančiam fiziniam asmeniui, advokatui ar kitam juridiniam asmeniui. Šiuo atveju taip pat privalo būti užtikrinama, kad dėl DAP vykdomų užduočių ar užimamų pareigų nekiltų interesų konfliktas (pvz., šis asmuo negali atstovauti įmonei teismuose, kai nagrinėjamos bylos, susijusios su duomenų apsauga). Jei DAP funkcijas atlieka išorinis paslaugų teikėjas – kitas juridinis asmuo, rekomenduotina aiškiai paskirstyti užduotis duomenų apsaugos pareigūno darbuotojams ir vieną asmenį paskirti už klientą atsakingu kontaktiniu asmeniu.

Atkreipkite dėmesį, kad, skirdami DAP, turėtumėte atsižvelgti į jo profesines ir asmenines savybes, gebėjimą atlikti DAP užduotis, duomenų apsaugos teisės ir praktikos ekspertinių žinių turėjimą (pvz., atliekamų asmens duomenų tvarkymo operacijų supratimą, informacinių technologijų ir duomenų saugumo išmanymą ir t. t.).

Duomenų apsaugos pareigūno užduotys

DAP atlieka šias užduotis:

- Stebi, kaip Jūs laikotės BDAR reikalavimų ir informuoja Jus bei duomenis tvarkančius darbuotojus apie prievoles asmens duomenų apsaugos srityje, konsultuoja šiais klausimais, pvz., DAP nagrinėja ir tikrina, ar duomenų tvarkymo veikla atitinka BDAR reikalavimus, teikia rekomendacijas;
- Bendradarbiauja su priežiūros institucija (VDAI) ir atlieka kontaktinio asmens funkciją priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais;
- Teikia konsultacijas dėl poveikio duomenų apsaugai vertinimo ir stebi jo atlikimą, pvz., konsultuoja, ar reikia atlikti poveikio duomenų apsaugai vertinimą, kokia metodika vadovautis, kokias apsaugos priemones taikyti, siekiant sumažinti riziką duomenų subjektų teisėms ir interesams ir t. t.;
- Vertina su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus;
- Atlieka kitas Jūsų pavestas funkcijas, susijusias su asmens duomenų tvarkymu, pvz., tvarko duomenų tvarkymo veiklos įrašus ir kt.

DAP turi būti sudarytos sąlygos veiksmingai atlikti savo užduotis, jam turi būti suteikta pakankama autonomija ir ištekliai šioms užduotims veiksmingai atlikti. Taip pat DAP negali gauti jokių nurodymų dėl savo užduočių vykdymo. Be to, svarbu prisiminti, kad pagal BDAR DAP negali būti atleistas arba baudžiamas dėl jam nustatytų užduočių atlikimo, pvz., DAP gali manyti, kad tam tikras duomenų tvarkymas gali kelti didelę riziką, ir gali patarti Jums atlikti poveikio duomenų apsaugai vertinimą, tačiau Jūs nesutinkate su duomenų apsaugos pareigūno vertinimu. Tokiu atveju DAP negalima atleisti už tai, kad jis suteikė šią konsultaciją.

DAP tiesiogiai atsiskaito duomenų valdytojo arba duomenų tvarkytojo aukščiausio lygio vadovybei.

Kokia duomenų apsaugos pareigūno informacija ir kur turi būti skelbiama?

Jūs privalote **paskelbti** (pvz., įmonės interneto svetainėje) DAP kontaktinius duomenis ir **pranešti juos** VDAI. Taip pat rekomenduotina apie paskirtą DAP pranešti įmonės darbuotojams, pvz., pateikiant DAP duomenis intranete, vidaus telefonų kataloge ar nurodant įmonės struktūros schemoje.

VDAI teikiamame pranešime apie paskirtą DAP turi būti nurodoma ši informacija:

- Duomenų valdytojo (duomenų tvarkytojo) pavadinimas ir kiti rekvizitai;
- DAP vardas ir pavardė;
- DAP pareigos (jei DAP yra duomenų valdytojo darbuotojas) arba juridinio asmens pavadinimas (jei DAP yra kito juridinio asmens darbuotojas);
- DAP kontaktiniai duomenys (pašto adresas, telefono ryšio numeris ir (ar) elektroninio pašto adresas, kitos ryšių priemonės).

Pranešimas VDAI apie DAP paskyrimą teikiamas šia tvarka.

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

Tais atvejais, kai dėl duomenų tvarkymo rūšies fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, prieš pradedant tvarkyti asmens duomenis BDAR nustato pareigą atlikti numatytų duomenų tvarkymo operacijų PDAV[16].

PDAV tikslas yra padėti sistemingai ir visapusiškai išanalizuoti Jūsų įmonės vykdomą asmens duomenų tvarkymą, padėti nustatyti ir sumažinti galinčias kilti grėsmes fizinių asmenų teisėms ir laisvėms bei įvertinti, ar likusios grėsmės yra pagrįstos ir pateisinamos.

Atliekant PDAV reikia atsižvelgti į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus bei vertinti ne tik asmens duomenų tvarkymo atitiktį reikalavimams, bet taip pat įvairaus pobūdžio pavojus fizinių asmenų teisėms ir laisvėms, įskaitant bet kokios žymios socialinės ar ekonominės, fizinės, turtinės ar neturtinės žalos tikimybę tiek atskiriems asmenims, tiek bendruomenėms ar socialinėms grupėms. Siekiant įvertinti pavojaus lygį būtina atsižvelgti tiek į žalos atsiradimo tikimybę, tiek į poveikio fiziniam asmeniui sunkumą.

Svarbu įtraukti PDAV į Jūsų įmonės vidinius procesus, kad priklausomai nuo vertinimo rezultato būtų galima koreguoti planuojamas asmens duomenų tvarkymo operacijas. PDAV yra ne vienkartinis veiksmas, o tęstinis procesas, nes duomenų tvarkymas turi būti peržiūrimas nuolatos.

Kada privalo būti atliktas poveikio duomenų apsaugai vertinimas?

PDAV turi būti atliekamas tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms **gali kilti didelis pavojus**. Tai reiškia, kad, nors poveikio duomenų apsaugai vertinimas dar neatliktas, Jūs turite įvertinti aplinkybes, kurios gali sąlygoti *didelį* pavojų fizinių asmenų teisėms ir laisvėms.

Sąvoka „fizinių asmenų teisės bei laisvės“, visų pirma, yra susijusi su teise į asmens duomenų apsaugą ir teise į privatumą, tačiau taip pat gali apimti kitas pagrindines žmogaus teises ir laisves, pvz., žodžio laisvę, minties laisvę, judėjimo laisvę, diskriminacijos draudimą, sąžinės ir tikėjimo laisvę ir kitas pagrindines žmogaus teises ir laisves.

Pavojus fizinių asmenų teisėms ir laisvėms gali kilti, kai dėl asmens duomenų tvarkymo arba dėl galimo asmens duomenų saugumo pažeidimo fiziniams asmenims gali būti sunkiau naudotis savo teisėmis ir laisvėmis, fizinis asmuo gali patirti atskirtį arba diskriminaciją, finansinius nuostolius, gali būti pakenkta jo reputacijai arba atsirasti kitokie rimti padariniai kasdieniam fizinio asmens gyvenimui.

29 straipsnio darbo grupė išskiria devynis kriterijus, kurie leidžia įvertinti, ar gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms:

[16] Detalesnė informacija apie PDAV pateikiama 29 straipsnio darbo grupės 2017 m. balandžio 4 d. Poveikio duomenų apsaugai vertinimo (PDAV) gairėse, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų.

1. Vertinimas arba balų skyrimas;
2. Automatizuotas sprendimų, sukeliančių teisinį arba panašų rimtą poveikį, priėmimas;
3. Sisteminga stebėsena;
4. Neskelbtinų duomenų arba labai asmeniškų duomenų tvarkymas;
5. Didelio masto duomenų tvarkymas;
6. Duomenų rinkinių siejimas ir derinimas;
7. Su pažeidžiamais duomenų subjektais susijusių asmens duomenų tvarkymas;
8. Asmens duomenų tvarkymas naudojant inovatyvias technologijas ar organizacinius sprendimo būdus arba egzistuojančių technologijų panaudojimas nauju būdu;
9. Kelio užkirtimas duomenų subjektams naudotis savo teisėmis, paslaugomis arba sudaryti sutartis.

Paprastai Jūs turėtumėte atlikti PDAV, kai asmens duomenų tvarkymas atitinka du iš pirmiau nurodytų kriterijų. Kuo daugiau kriterijų atitinka asmens duomenų tvarkymo operacija, tuo labiau tikėtina, kad dėl jos kils didelis pavojus fizinių asmenų teisėms ir laisvėms.

Be to, BDAR išskiria šiuos atvejus, kad turi būti atliktas PDAV:

1. *Sistemingas ir išsamus* su fiziniais asmenimis susijusių *asmeninių aspektų vertinimas,* kuris yra grindžiamas *automatizuotu* tvarkymu, įskaitant profiliavimą, ir kuriuo remiantis *priimami sprendimai,* kuriais *padaromas* su fiziniu asmeniu susijęs teisinis *poveikis* arba kurie *daro panašų didelį poveikį* fiziniam asmeniui.

Asmeninių aspektų vertinimas reiškia aspektų, susijusių su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu, vertinimu.

Profiliavimas reiškia informacijos apie duomenų subjektą (ar duomenų subjektų grupę) rinkimą ir jo (jų) savybių ar elgesio įvertinimą, siekiant priskirti jį (juos) tam tikrai kategorijai ar grupei asmenų bei tokiu būdu prognozuoti ar numatyti jų savybes ar elgesį. Pavyzdžiui, įmonė, naudodama lojalumo programą ir analizuodama šia programa besinaudojančių klientų pirkimų istorija, kuria klientų elgesio arba rinkodaros profilius.

Automatizuotas sprendimų priėmimas yra būdas priimti sprendimą techninių priemonių pagalba be žmogaus dalyvavimo, pvz., finansų įstaiga automatizuotai priima sprendimą dėl paskolos suteikimo tam tikram asmeniui.

Teisinis sprendimo poveikis reiškia, kad sprendimas turi poveikį asmens teisėms, pvz., teisei bendrauti su kitais asmenimis, balsuoti rinkimuose ar imtis teisinių veiksmų, arba turi įtakos asmens teisiniam statusui arba sutartinėms teisėms. Pavyzdžiui, sutarties nutraukimas, tam tikrų socialinių išmokų skyrimas arba atsisakymas paskirti, atsisakymas suteikti pilietybę ir pan.

Panašus didelis poveikis reiškia, kad nors sprendimas neturi poveikio asmens teisėms ir pareigoms, poveikis asmeniui vis dėlto gali būti didelis. Pavyzdžiui, automatinis atsisakymas suteikti kreditą, elektroninė darbuotojų atranka.

2. Specialių kategorijų asmens duomenų arba asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas *dideliu mastu*.

Tikslaus tvarkomų duomenų kiekio ar atitinkamų asmenų skaičiaus, kuriems esant būtų laikytina, kad asmens duomenų tvarkymas atliekamas dideliu mastu, nėra. Tačiau vertinant, ar asmens duomenys yra tvarkomi dideliu mastu, rekomenduotina atsižvelgti į šiuos veiksnius: susijusių duomenų subjektų konkretų skaičių arba atitinkamo gyventojų skaičiaus procentinę dalį; įvairių tvarkomų duomenų vienetų kiekį ir (arba) intervalą; duomenų tvarkymo veiklos trukmę arba pastovumą; geografinę duomenų tvarkymo veiklos aprėptį (pvz., ar asmens duomenys tvarkomi regioniniu, nacionaliniu ar tarpvalstybiniu lygmeniu).

3. *Sistemingas viešos vietos stebėjimas dideliu mastu*. Didelis mastas turėtų būti vertinamas remiantis pirmiau nurodytais kriterijais.

Sistemingas asmens duomenų tvarkymas atliekamas tam tikrais intervalais, nuolat tebevykstantis, pasikartojantis tam tikrais periodais, yra organizuotas, planuotas, metodiškas ar pan.

Vieša vieta reiškia bet kurią visuomenės nariui atvirą vietą, pvz., aikštę, prekybos centrą, gatvę, turgavietę, traukinių stotį ir pan.

Stebėjimo sąvoka apima visų formų stebėjimą, taip pat stebėjimą ir profiliavimą internete.

VDAI taip pat yra nustačiusi asmens duomenų tvarkymo operacijų, kada *privalo* būti atliktas PDAV, sąrašą, į kurį patenka šios asmens duomenų tvarkymo operacijos:

1. Asmens duomenų tvarkymas vykdomas mokslinių ar istorinių tyrimų tikslais bent vienu iš šių atvejų: kai be duomenų subjekto sutikimo tvarkomi specialių kategorijų asmens duomenys arba asmens duomenų tvarkymas vykdomas susiejant ar derinant duomenų rinkinius; kai tvarkomi nepilnamečių asmenų duomenys; kai tvarkomas asmens kodas;
2. Asmens duomenų tvarkymas dideliu mastu, kai asmens duomenys gauti ne iš duomenų subjekto bei informacijos apie asmens duomenų tvarkymą, pateikimas yra neįmanomas arba tam reikėtų neproporcingų pastangų, arba jeigu dėl tokio informacijos pateikimo gali tapti neįmanoma arba jis gali labai sukliudyti pasiekti tvarkymo tikslus;
3. Asmens duomenų tvarkymas, kai duomenų gavėjų, kuriems buvo atskleisti asmens duomenys, informavimas apie asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą, nėra įmanomas arba pareikalautų neproporcingų pastangų;
4. Biometrinių duomenų, kuriais siekiama konkrečiai nustatyti fizinio asmens tapatybę, tvarkymas duomenų subjektų stebėsenos ar kontrolės tikslais arba kai tvarkomi pažeidžiamų duomenų subjektų asmens duomenys;
5. Genetinių duomenų tvarkymas vykdant duomenų subjekto savybių vertinimą arba balų skyrimą, įskaitant profiliavimą ir prognozavimą;
6. Asmens vaizdo duomenų tvarkymas, kai vaizdo stebėjimas vykdomas bent vienu iš šių atvejų: patalpose ir (ar) teritorijose, kurios nėra duomenų valdytojo valdomos nuosavybės ar kitais teisėtais pagrindais; sveikatos priežiūros, socialinės globos, įkalinimo įstaigose ir kitose įstaigose, kuriose paslaugos yra teikiamos pažeidžiamiems asmenims; kartu su garso įrašymu;
7. Pokalbių telefonu įrašymas;
8. Asmens duomenų tvarkymas naudojant inovatyvias technologijas arba egzistuojančias technologijas panaudojant nauju būdu, kai tvarkomi pažeidžiamų duomenų subjektų asmens duomenys;
9. Vaikų asmens duomenų tvarkymas tiesioginės rinkodaros tikslais, vaikų asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, arba kai vaikams tiesiogiai yra siūlomos informacinės visuomenės paslaugos;
10. Darbuotojų asmens duomenų tvarkymas stebėsenos ar kontrolės tikslais: asmens vaizdo ir (ar) garso duomenų tvarkymas darbo vietoje ir (ar) duomenų valdytojo patalpose ar teritorijose, kuriose dirba jo darbuotojai; asmens duomenų, susijusių su darbuotojų, komunikacijos, elgesio, vietos ar judėjimo stebėsena, tvarkymas.

Atkreipkite dėmesį, kad PDAV gali būti atliekamas dėl vienos arba dėl kelių panašių duomenų tvarkymo operacijų. Keli duomenų valdytojai gali atlikti vieną PDAV.

Kaip atliekamas poveikio duomenų apsaugai vertinimas?

BDAR nustatyti minimalūs poveikio duomenų apsaugai turinio reikalavimai:

- Numatytų duomenų tvarkymo operacijų aprašymas ir duomenų tvarkymo tikslai;
- Duomenų tvarkymo operacijų reikalingumo ir proporcingumo vertinimas;
- Duomenų subjektų teisėms ir laisvėms kylančių pavojų vertinimas;
- Numatomos priemonės pavojams pašalinti ir kuriomis įrodoma, kad laikomasi BDAR.

Pavyzdinė poveikio duomenų apsaugai atlikimo forma:
https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzd_PDAV_forma.docx

Kada reikia kreiptis į Valstybinę duomenų apsaugos inspekciją?

Jeigu atlikus PDAV būtų nustatyta, kad, tvarkant duomenis **gali kilti didelis pavojus, jei nesiimtumėte priemonių pavojui sumažinti,** Jūs, prieš pradėdami tvarkyti asmens duomenis, turite kreiptis į VDAI **dėl išankstinės konsultacijos**.

Kreipdamiesi dėl išankstinės konsultacijos į VDAI, turite:

- Nurodyti numatyto asmens duomenų tvarkymo tikslus ir priemones;
- Nurodyti nustatytas priemones bei apsaugos priemones duomenų subjektų teisėms ir laisvėms apsaugoti;
- Pateikti atliktą poveikio duomenų apsaugai vertinimą;
- Nurodyti duomenų apsaugos pareigūno kontaktinius duomenis (kai taikoma);
- Nurodyti atitinkamas duomenų tvarkymo procese dalyvaujančio duomenų valdytojo, bendrų duomenų valdytojų ir duomenų tvarkytojų atsakomybės sritis, visų pirma, kai duomenys tvarkomi įmonių grupėje (kai taikoma);
- Bet kokią kitą VDAI prašomą informaciją.

Išsami išankstinių konsultacijų tvarka yra pateikiama VDAI direktoriaus įsakymu patvirtintose Išankstinių konsultacijų teikimo taisyklėse.

ASMENS DUOMENŲ SAUGUMAS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI

Duomenų saugumas yra **pažeidžiamas, kai įvyksta su duomenimis, už kuriuos Jūsų įmonė yra atsakinga, susijęs saugumo incidentas,** dėl kurio pažeidžiamas duomenų konfidencialumas, prieinamumas ar vientisumas.

Galimi asmens duomenų saugumo pažeidimo (toliau – Pažeidimo) tipai:

- **Konfidencialumo Pažeidimas** – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;
- **Prieinamumo Pažeidimas** – kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba sunaikinami asmens duomenys;
- **Vientisumo Pažeidimas** – kai asmens duomenys pakeičiami be leidimo ar netyčia.
- Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

Atsakingas asmuo, sužinojęs apie galimą Pažeidimą, turėtų kaip įmanoma greičiau atlikti pirminį tyrimą, išsiaiškinti ir nustatyti, ar Pažeidimas iš tikrųjų įvyko, bei kokios galimos pasekmės asmenims (t. y. įvertinti riziką).

Priklausomai nuo Pažeidimo pobūdžio (tipo), atliekant pirminį tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, turėtų būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės, pvz., duomenų srauto ir prisijungimų analizės įrankiai bei kt.

Vertinant riziką, kuri gali atsirasti dėl Pažeidimo, turėtų būti atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turėtų būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos **kriterijus**:

1. Pažeidimo tipą;
2. Asmens duomenų pobūdį, apimtis (pvz., specialių kategorijų asmens duomenys);
3. Kaip lengvai identifikuojamas fizinis asmuo;
4. Pasekmių rimtumą fiziniams asmenims;
5. Specialias fizinio asmens savybes (pvz., duomenys, susiję su vaikais ar kitais pažeidžiamais asmenimis);
6. Nukentėjusiųjų fizinių asmenų skaičių;
7. Specialias duomenų valdytojo savybes (pvz., veiklos pobūdį).

Vertinant riziką, turėtų būti laikoma, kad Pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno

sužalojimą, materialinę ar nematerialinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

Įvertinus riziką rekomenduotina nustatyti, kad yra:

- Žema rizikos tikimybė;
- Vidutinė rizikos tikimybė;
- Didelė (aukšta) rizikos tikimybė.

Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo atsakingas asmuo turėtų pateikti (duomenų valdytojo) vadovui (ar jo įgaliotam asmeniui). Duomenų valdytojo vadovas (ar jo įgaliotas asmuo) turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimu.

Atsakingas asmuo, visų pirma, turėtų imtis visų tinkamų techninių ir organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų ir tuomet pateikti Pranešimą VDAI.

PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI

Nustačius, kad Pažeidimas buvo ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, atsakingas asmuo nedelsdamas, ne vėliau kaip per 72 val. nuo sužinojimo apie Pažeidimą, turėtų pranešti apie tai VDAI.

Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą VDAI, rekomenduotina pranešti.

Jeigu, priklausomai nuo Pažeidimo pobūdžio, duomenų valdytojui yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu (pvz., dar nėra išsiaiškinta Pažeidimo apimtis), ir per 72 val. nuo sužinojimo apie Pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, Pranešimui reikalinga informacija galėtų būti teikiama etapais. Esant galimybei, apie informacijos teikimą etapais VDAI turėtų būti informuota teikiant pirminį Pranešimą.

Jeigu po Pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio Pažeidimo, apie tai nedelsiant turėtų būti informuojama VDAI ir pažymėta specialiame žurnale.

Jeigu Pažeidimas paveikia fizinių asmenų duomenis daugiau negu vienoje valstybėje narėje ir yra reikalinga pranešti priežiūros institucijai, duomenų valdytojas turėtų pranešti vadovaujančiai priežiūros institucijai (BDAR preambulės 55 punktas). Jeigu duomenų valdytojas abejoja, kuri priežiūros institucija yra vadovaujanti, bet Pažeidimas įvyko Lietuvos Respublikoje, tuomet jis turėtų pranešti VDAI. Šiuo atveju, teikiant Pranešimą, rekomenduotina nurodyti, ar toks Pažeidimas apima ir kitose valstybėse narėse esančias duomenų valdytojo buveines, ir kuriose valstybėse narėse esančius duomenų subjektus Pažeidimas galėjo paveikti.

PRANEŠIMAS DUOMENŲ SUBJEKTUI

Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, atsakingas asmuo nedelsdamas (rekomenduojama per 72 val.) apie tai turėtų pranešti duomenų subjektui, kurio teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus.

VDAI informavimas apie Pažeidimą neatleidžia duomenų valdytojo nuo pareigos informuoti duomenų subjektą.

Pranešime duomenų subjektui aiškia ir paprasta kalba turėtų būti pateikiama:

- Pažeidimo pobūdžio aprašymas;
- Duomenų apsaugos pareigūno arba kito kontaktinio asmens vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;
- Tikėtinų Pažeidimo pasekmių aprašymas;

- Priemonių, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas Pažeidimas, įskaitant (kai tinkama) priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pvz., kad apie Pažeidimą yra informuota VDAI ir, kad yra gautas patarimas dėl Pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);
- Kita reikšminga informacija, susijusi su Pažeidimu, kuri, duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.

Duomenų subjektai apie Pažeidimą turėtų būti informuoti tiesiogiai, pvz., siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan. Šis pranešimas turėtų būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai.

Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia, jeigu:

- Duomenų valdytojas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;
- Iš karto po Pažeidimo duomenų valdytojas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;
- Tai pareikalautų neproporcingai daug pastangų susisiekti su asmenimis (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl Pažeidimo arba nežinomi). Tokiu atveju vietoj to apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

Pavyzdys

Buvo atskleisti tekstilės įmonės darbuotojų duomenys, įskaitant asmeninius adresus, šeimos sudėtį, mėnesinį darbo užmokestį ir paraiškas dėl medicininių išlaidų kompensavimo. Tokiu atveju tekstilės įmonė apie pažeidimą privalo pranešti priežiūros institucijai. Kadangi į asmens duomenis patenka neskelbtini duomenys, kaip antai sveikatos duomenys, įmonė turi pranešti ir darbuotojams.

Pavyzdys

Debesijos paslaugas teikianti įmonė prarado kelis standžiuosius diskus, kuriuose yra keliems klientams priklausančių asmens duomenų. Apie šį pažeidimą ji turi pranešti savo klientams iš karto po to, kai apie jį sužino. Tuomet klientai turi pranešti VDAI ir fiziniams asmenims, priklausomai nuo to, kokius duomenis tvarkė duomenų tvarkytojas.

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

Visus Pažeidimus, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, turėtumėte registruoti duomenų valdytojo žurnale (toliau – Žurnalas).

Informacija apie Pažeidimą į Žurnalą turėtų būti įvedama nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika (rekomenduotina ne ilgiau kaip per 5 darbo dienas). Esant būtinybei, Žurnale esanti informacija turėtų būti papildoma ir (ar) koreguojama.

Žurnale turėtų būti nurodoma:

- Visi su Pažeidimu susiję faktai – Pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;
- Pažeidimo poveikis ir pasekmės;
- Taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;
- Priežastys dėl su Pažeidimu susijusių sprendimų priėmimo (pvz., kodėl duomenų valdytojas nusprendė nepranešti apie Pažeidimą VDAI ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad tikėtina, jog Pažeidimas negali sukelti pavojaus fizinių asmenų teisėms ir laisvėms, arba kokią sąlygą įvykdė, kuomet pranešti apie Pažeidimą duomenų subjektui nereikia);
- Pranešimo VDAI pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);

- Informacija, susijusi su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta ir pan.);
- Kita reikšminga informacija, susijusi su Pažeidimu (pvz., kad tyrimo metu nustatyta, jog faktiškai Pažeidimo nebuvo, o buvo tik saugumo incidentas).

Žurnalas turėtų būti tvarkomas raštu, įskaitant elektroninę formą, ir saugomas pagal duomenų valdytojo patvirtintą dokumentų saugojimo tvarką.

Turėtumėte paskirti asmenį (darbuotoją), atsakingą už Žurnalo pildymą.

Remdamasi Žurnale pateikta informacija, VDAI turi galėti patikrinti, kaip įgyvendinama duomenų valdytojo prievolė pranešti apie Pažeidimus.

Rekomenduotina periodiškai peržiūrėti Žurnale esančius įrašus ir numatyti, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip bus kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje analogiški Pažeidimai nesikartotų.

KITOS PAREIGOS, SUSIJUSIOS SU ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAIS

1. Duomenų valdytojas ir duomenų tvarkytojas privalo informuoti darbuotojus apie jų pareigą pranešti apie galimus Pažeidimus ir supažindinti juos su nustatyta pranešimų apie Pažeidimus pateikimo tvarka.
2. Duomenų valdytojas ir duomenų tvarkytojas turėtų paskirti asmenį ar skyrių, atsakingą už Pažeidimų valdymą (toliau – Atsakingas asmuo), pvz., už Pažeidimų tyrimą, pranešimų VDAI ir duomenų subjektui teikimą, prevencinių priemonių įdiegimo kontrolę ir pan.
3. Duomenų valdytojo ir duomenų tvarkytojo darbuotojas, sužinojęs ar pats nustatęs galimą Pažeidimą arba kai informacija apie galimą Pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio, privalo nedelsdamas apie tai informuoti Atsakingą asmenį (priklausomai nuo organizacijos dydžio, pobūdžio ar pan.). Pranešimas galėtų būti pateikiamas žodžiu, raštu ar elektroninėmis priemonėmis.
4. Duomenų tvarkytojas, sužinojęs apie Pažeidimą, turėtų nedelsdamas (rekomenduotina ne ilgiau kaip per 24 val.) apie tai pranešti duomenų valdytojui. Apie tokią pareigą duomenų valdytojas turėtų iš anksto informuoti duomenų tvarkytoją (pvz., sudaromoje duomenų tvarkymo sutartyje).
5. Duomenų tvarkytojas apie Pažeidimą gali pranešti tiesiogiai VDAI, jeigu tai yra aiškiai numatyta duomenų tvarkymo sutartyje su duomenų valdytoju. Tačiau bet kuriuo atveju teisinę prievolę pranešti VDAI turi duomenų valdytojas.
6. Atsakingas asmuo apie Pažeidimą taip pat turėtų informuoti duomenų apsaugos pareigūną (jeigu toks yra paskirtas) bei laiku ir tinkamai suteikti jam visą informaciją, susijusią su galimu Pažeidimu.

Labai svarbu, kad Jūs, kaip organizacija, **įgyvendintumėte tinkamas technines ir organizacines priemones**, kad būtų išvengta galimų duomenų apsaugos pažeidimų.

PRITAIKYTOJI IR STANDARTIZUOTOJI DUOMENŲ APSAUGA

Pagal BDAR preambulę, kad galėtų įrodyti, jog laikosi šio reglamento, duomenų valdytojas turėtų priimti vidaus nuostatas ir **įgyvendinti priemones, kuriomis, visų pirma, būtų paisoma pritaikytosios ir standartizuotosios duomenų apsaugos principų**.

Pritaikytoji duomenų apsauga (angl. *privacy by design*). BDAR 25 str. 1 d. reikalauja, kad duomenų valdytojas įgyvendintų tinkamas technines ir organizacines priemones, kaip antai, pseudonimų suteikimą, kuriomis siekiama veiksmingai įgyvendinti duomenų apsaugos principus, kaip antai, duomenų kiekio mažinimo principą, ir į duomenų tvarkymą integruoti būtinas apsaugos priemones, kad jis atitiktų šio reglamento reikalavimus ir apsaugotų duomenų subjektų teises.

BDAR reikalauja, kad šios priemonės būtų įgyvendintos:

- Tiek nustatant duomenų tvarkymo priemones;
- Tiek paties duomenų tvarkymo metu.

Tokios priemonės turi būti įgyvendintos atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms.

Pavyzdys

Jūsų įmonė ketina vykdyti naują projektą, kurio metu bus tvarkomi asmens duomenys. Dar iki projekto pradžios turi būti įvertinti asmens duomenų apsaugos reikalavimai ir suprojektuotos reikiamos asmens duomenų saugumo organizacinės techninės priemonės. Jei dėl asmens duomenų tvarkymo duomenų subjektams gali kilti didelė rizika, įvertinimas turi būti atliekamas vykdant poveikio duomenų apsaugai vertinimą. Daugiau apie tai skyriuje „Poveikio duomenų apsaugai vertinimas“.

Standartizuotoji duomenų apsauga (angl. *privacy by default*). BDAR reikalauja, kad duomenų valdytojas įgyvendintų tinkamas technines ir organizacines priemones, kuriomis užtikrintų, kad standartizuotai būtų tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui.

Ši prievolė taikoma surinktų asmens duomenų kiekiui, jų tvarkymo apimčiai, jų saugojimo laikotarpiui ir jų prieinamumui. Visų pirma, tokiomis priemonėmis užtikrinama, kad standartizuotai be fizinio asmens įsikišimo su asmens duomenimis negalėtų susipažinti neribotas fizinių asmenų skaičius.

Pavyzdys

Jūsų įmonė tvarko asmens duomenis keliais tikslais (paslaugų teikimas, darbuotojų duomenų tvarkymas vidaus administravimo tikslu ir pan.). Tvarkant asmens duomenis, kiekvieno tikslo atveju turi būti nustatyti konkretūs asmens duomenų tvarkymo terminai, o prieigos teisės turi būti priskiriamos priklausomai nuo darbuotojo atliekamų funkcijų, pagal principą „būtina žinoti“.

ORGANIZACINIAI IR TECHNINIAI ASMENS DUOMENŲ SAUGUMO REIKALAVIMAI

BDAR nenustato konkrečių asmens duomenų saugumo organizacinių ir techninių priemonių, tačiau įveda bendrą taisyklę ir pareigą: duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas.

BDAR 32 str. pateikiami **kriterijai**, pagal kuriuos tokios priemonės turėtų būti nustatytos. Kriterijai yra tokie:

- Techninių galimybių išsivystymo lygis;
- Įgyvendinimo sąnaudos;
- Duomenų tvarkymo pobūdis, aprėptis, kontekstas ir tikslais;
- Duomenų tvarkymo keliami įvairios tikimybės ir rimtumo pavojai fizinių asmenų teisėms ir laisvėms.

BDAR pateikiamos asmens duomenų saugumo priemonės, kurios gali būti taikomos apsaugant asmens duomenis:

- Pseudonimų suteikimas asmens duomenims ir jų šifravimas;
- Gebėjimas užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;
- Gebėjimas laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju;
- Reguliarus techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesas.

Tai nėra privalomos priemonės, tačiau reikia atkreipti dėmesį, kad BDAR kontekste šios priemonės yra vienos iš svarbesnių.

Asmens duomenų saugumo lygis atskirose įmonėse gali skirtis. Pagal BDAR nustatant tinkamo lygio saugumą, visų pirma, atsižvelgiama į pavojus, kurie kyla dėl duomenų tvarkymo, visų pirma, dėl netyčinio arba neteisėto persiųstų, saugomų ar kitaip tvarkomų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

Pavyzdys

Jūsų įmonė tvarko bendruosius darbuotojų asmens duomenis (vardas, pavardė, asmens kodas, adresas ir pan.), taip pat Jūsų įmonė teikia elektroninės prekyvietės paslaugas, susijusias su medicininiais preparatais. Antruoju atveju asmens duomenų tvarkymas susijęs su asmenimis, kurie serga specifiniais susirgimais ir jiems reikia specialios priežiūros ir atitinkamų medicininių preparatų. Šiems duomenims apsaugoti reikia taikyti aukštesnį saugumo lygį, kadangi jų atskleidimas, neteisėtas panaudojimas ir kt. gali padaryti didesnę žalą fizinių asmenų teisėms ir laisvėms. Tokios aukštesnio lygio saugumo priemonės galėtų apimti rizikos vertinimą, prasiskverbimo testus ir pan.

VDAI parengė **„Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams“**. Šiose gairėse VDAI rekomenduoja 20 minimalių organizacinių ir techninių duomenų saugumo reikalavimų, pakankamų tose organizacijose, kurių tvarkomų asmens duomenų saugumo rizika, susijusi su pavojais fizinių asmenų teisėms ir laisvėms, yra žema. Taigi, šiuos reikalavimus privalo įgyvendinti kiekviena asmens duomenis tvarkanti organizacija ar asmuo, o daugelis imtis ir papildomų, kad užtikrintų tinkamą savo tvarkomų asmens duomenų saugumo lygį.

10 minimalių reikalavimų dėl tinkamų organizacinių duomenų saugumo priemonių:

1. **Asmens duomenų saugumo politika ir procedūros.** Asmens duomenų ir jų tvarkymo saugumas organizacijoje turi būti dokumentuotas kaip informacijos saugumo politikos dalis.
2. **Vaidmenys ir atsakomybės.** Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal saugumo politiką.
3. **Prieigos valdymo politika.** Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės.
4. **Išteklių ir turto valdymas.** Organizacija turi turėti IT išteklių, naudojamų asmens duomenims tvarkyti, registrą, o registro tvarkymas turi būti priskirtas konkrečiam asmeniui.
5. **Pakeitimų valdymas.** Organizacija turi užtikrinti, kad visi IT sistemų pakeitimai būtų stebimi ir registruojami konkretaus asmens.
6. **Duomenų tvarkytojai.** Prieš pradedant asmens duomenų tvarkymo veiklą, duomenų valdytojai ir duomenų tvarkytojai turėtų apibrėžti, dokumentuoti ir suderinti tarpusavio formalumus. Duomenų tvarkytojas privalo nedelsdamas pranešti duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus.
7. **Asmens duomenų saugumo pažeidimai ir incidentai.** Turi būti nustatytas reagavimo į incidentus planas su išsamia tvarka. Apie asmens duomenų pažeidimus turi būti nedelsiant pranešama vadovybei. Turi būti nustatyta pranešimo apie pažeidimus kompetentingoms institucijoms, tarp jų ir VDAI, bei duomenų subjektams tvarka.
8. **Veiklos tęstinumas.** Organizacija turi nustatyti pagrindines procedūras, kurių reikia laikytis incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas.
9. **Personalo konfidencialumas.** Organizacija turi užtikrinti, kad visi darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu. Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus.
10. **Mokymai.** Organizacija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi dėl atitinkamų duomenų apsaugos reikalavimų ir teisinių įsipareigojimų rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų dažnumas: *kartą per metus*.

10 minimalių reikalavimų dėl tinkamų techninių duomenų saugumo priemonių:

1. **Prieigų kontrolė ir autentifikavimas.** Turi būti įdiegta ir įgyvendinta bei visiems IT sistemos naudotojams taikoma Prieigų kontrolės sistema. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras. Dėmesio! Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas. Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio. Organizacija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi dėl atitinkamų duomenų apsaugos reikalavimų ir teisinių įsipareigojimų rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų dažnumas: kartą per metus.
2. **Techninių žurnalų įrašai ir stebėsena.** Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, taikomajai programai, naudojamai asmens duomenų apdorojimui. Techniniuose žurnaluose turi būti matomi visi įmanomi prieigų prie asmens duomenų įrašų tipai (pvz., data, laikas, peržiūrėjimas, keitimas, panaikinimas). Siūlomas saugojimo terminas: *ne mažiau kaip 6 mėnesiai*. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį.
3. **Tarnybinių stočių, duomenų bazių apsauga.** Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi apdoroti tik tuos asmens duomenis, kurie yra reikalingi darbui, atitinkančiam duomenų apdorojimo tikslus.
4. **Darbo stočių apsauga.** Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti saugos nustatymų. Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos *ne rečiau kaip kas savaitę*. Naudotojams negalima turėti privilegijų diegti, šalinti, administruoti neautorizuotos programinės įrangos. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam, neveiksniam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Siūlomas neaktyvios sesijos laikas: *ne daugiau kaip 15 min.* Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.
5. **Tinklo ir komunikacijos sauga.** Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS, SSL).
6. **Atsarginės kopijos.** Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susaistytos su rolėmis ir pareigomis. Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų. Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą, išsamumą. Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Siūlomas atsarginių kopijų darymo dažnumas: *kasdien – pridedamoji kopija*; *kas savaitę – pilna kopija*.
7. **Mobilieji, nešiojami įrenginiai.** Mobiliųjų ir nešiojamų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimąsi. Mobilieji, nešiojami įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti. Mobilieji įrenginiai turi būti adekvataus prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims apdoroti.
8. **Programinės įrangos sauga.** Informacinėse sistemose naudojama programinė įranga (asmens duomenims apdoroti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.

9. **Duomenų naikinimas, šalinimas.** Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Tais atvejais, kai to padaryti neįmanoma (pvz., CD, DVD laikmenos ir pan.), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti. Popierius ir nešiojamos duomenų laikmenos, kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinami tam skirtais smulkintuvais.

10. **Fizinė sauga.** Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.

Daugiau informacijos apie bazinius rekomenduojamus saugumo reikalavimus galite rasti VDAI parengtose Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gairėse asmens duomenų valdytojams ir tvarkytojams. Šiose gairėse pateikti reikalavimai paaiškinti atsižvelgiant į du itin aktualius skaitmeninės erdvės saugumo dokumentus – informacinių technologijų saugumo standartą LST EN ISO/IEC 27001:2017 ir BDAR. Šių reikalavimų įgyvendinimas padės organizacijoms užtikrinti BDAR atitiktį. Be kita ko, svarbu atkreipti dėmesį, kad VDAI atliekant tikrinimus organizacijose, nepriklausomai nuo organizacijų dydžio ar sektoriaus, bus svarbu, ar įgyvendintos bent jau šios minimalios priemonės, prisidedančios prie asmens duomenų ir privatumo apsaugos užtikrinimo.

2019 m. paskelbtas asmens duomenų saugumo ir rizikos nustatymo gairių projektas, su kuriuo galite susipažinti čia:

Atkreiptinas dėmesys, kad kuriant (diegiant) ar vertinant turimas organizacines ir technines saugumo priemones, turite visapusiškai atsižvelgti į „pobūdį, aprėptį, kontekstą bei tikslus“ ir riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms. BDAR įpareigoja **visais atvejais atlikti rizikos vertinimą**.

ASMENS DUOMENŲ TVARKYMO YPATUMAI

ASMENS DUOMENŲ PERDAVIMAS

BDAR nenustato tvarkos, kaip turi būti perduodami asmens duomenys duomenų gavėjams, esantiems ES valstybėse narėse ar EEE valstybėse. Todėl, įgyvendindami iš atskaitomybės principo kylančias pareigas, asmens duomenis turėtumėte perduoti tik pagal duomenų gavėjo prašymą (vienkartinio asmens duomenų teikimo atveju) ar pagal asmens duomenų teikimo sutartį (daugkartinio asmens duomenų teikimo atveju), pvz., gavę prašymą pateikti asmens duomenis Jūs turite įvertinti, ar prašyme yra nurodyta asmens duomenų teisėto tvarkymo sąlyga, kuria remiantis prašoma asmens duomenų, kokiu tikslu jų prašoma bei nurodyta asmens duomenų teikimo apimtis ir kitos svarbios aplinkybės asmens duomenų atskleidimui konkrečiu atveju.

Asmens duomenų perdavimui į trečiąsias valstybes BDAR nustato atskiras taisykles:

1. Asmens duomenys gali būti perduodami remiantis Europos Komisijos priimtu sprendimu dėl tinkamumo;
2. Jei nėra priimtas Europos Komisijos sprendimas dėl tinkamumo, asmens duomenys perduodami taikant tinkamas apsaugos priemones nustatytas:
   - Įmonėms privalomomis taisyklėmis;
   - Europos Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis;
   - Priežiūros institucijos priimtomis standartinėmis duomenų apsaugos sąlygomis, kurias patvirtina Europos Komisija;
   - Patvirtintu elgesio kodeksu;
   - Patvirtintu sertifikavimo mechanizmu;
   - Sutartimi (gavus priežiūros institucijos leidimą).
3. Jei nėra priimtas Europos Komisijos sprendimas dėl tinkamumo arba nenustatytos tinkamos apsaugos priemonės, asmens duomenys gali būti perduodami, kai:
   - Duomenų subjektas aiškiai sutiko su siūlomu duomenų perdavimu;

- Duomenų perdavimas yra *būtinas* duomenų subjekto ir duomenų valdytojo sutarčiai vykdyti arba ikisutartinėms priemonėms, kurių imtasi duomenų subjekto prašymu, įgyvendinti;
- Duomenų perdavimas yra *būtinas*, kad būtų sudaryta arba įvykdyta *duomenų subjekto interesais* sudaroma duomenų valdytojo ir kito fizinio ar juridinio asmens sutartis;
- Duomenų perdavimas yra būtinas dėl svarbių viešojo intereso priežasčių;
- Duomenų perdavimas yra būtinas siekiant pareikšti, vykdyti ar ginti teisinius reikalavimus;
- Duomenų perdavimas yra būtinas, kad būtų apsaugoti gyvybiniai duomenų subjekto arba kitų asmenų interesai, jeigu duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo.

DARBUOTOJŲ ASMENS DUOMENŲ TVARKYMO YPATUMAI

Tos pačios asmens duomenų tvarkymo taisyklės galioja, tiek kai tvarkote klientų asmens duomenis, tiek darbuotojų asmens duomenis. Tačiau yra tam tikrų specifinių taisyklių, kurių turite laikytis tvarkydami darbuotojų asmens duomenis:

- Draudžiama tvarkyti *kandidato*, pretenduojančio eiti pareigas arba atlikti darbo funkcijas, *ir darbuotojo* asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas, išskyrus atvejus, kai šie asmens duomenys būtini norint patikrinti, ar asmuo atitinka įstatymuose ir įgyvendinamuosiuose teisės aktuose nustatytus reikalavimus pareigoms eiti arba darbo funkcijoms atlikti, pvz., įstatymu nustatyti nepriekaištingos reputacijos reikalavimai, kurie susiję su tam tikrų nusikalstamų veikų padarymu;
- Jūs galite rinkti kandidato, pretenduojančio eiti pareigas arba atlikti darbo funkcijas, asmens duomenis, susijusius su kvalifikacija, profesiniais gebėjimais ir dalykinėmis savybėmis, iš buvusio darbdavio *prieš tai informavęs* kandidatą, o iš esamo darbdavio – *tik kandidato sutikimu*;
- Tvarkant vaizdo ir (ar) garso duomenis darbo vietoje ir Jūsų patalpose ar teritorijose, kuriose dirba darbuotojai, tvarkant asmens duomenis, susijusius su darbuotojų elgesio, buvimo vietos ar judėjimo stebėsena, šie darbuotojai apie tokį jų asmens duomenų tvarkymą turi būti *informuojami pasirašytinai ar kitu informavimo faktą įrodančiu būdu*, pvz., naudojantis informacinėmis sistemomis, pateikiant BDAR nurodytą informaciją. Svarbu atkreipti dėmesį, kad informavimas *nėra laikytinas* darbuotojo sutikimu tvarkyti asmens duomenis.

Tam tikri asmens duomenų tvarkymo ypatumai yra susiję su tinkamo teisėto asmens duomenų tvarkymo pagrindo pasirinkimu, kai yra tvarkomi darbuotojų asmens duomenys. Dėl darbdavio ir darbuotojo santykiams būdingos priklausomybės (galios disbalanso) nėra tikėtina, kad darbuotojas galėtų neduoti savo darbdaviui sutikimo, kad būtų tvarkomi jo asmens duomenys, be baimės ar realios rizikos patirti neigiamą poveikį dėl savo nesutikimo, pvz., kad darbo vietoje būtų pradėtos naudoti stebėsenos sistemos ar kad būtų užpildytos vertinimo formos, nejusdamas jokio spaudimo su tuo sutikti. Todėl dėl darbdavio ir darbuotojo santykių pobūdžio daugeliu asmens duomenų tvarkymo darbe atvejų darbuotojų sutikimas *negali ir neturėtų būti teisėtas duomenų tvarkymo pagrindas*. Tačiau tai nereiškia, kad niekada negalima remtis sutikimu, kaip teisėtu duomenų tvarkymo pagrindu, darbuotojai gali duoti laisvą sutikimą, kai nepatirtų visiškai jokių neigiamų pasekmių nepriklausomai nuo to, ar sutikimą duotų, ar ne[17].

BIOMETRINIŲ DUOMENŲ TVARKYMO YPATUMAI

Biometriniai duomenys – po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima *konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę*, kaip antai, veido atvaizdai arba daktiloskopiniai (pvz., piršto atspaudas) duomenys[18]. Biometriniai duomenys priskiriami prie specialių kategorijų asmens duomenų, todėl pagal bendrą taisyklę jų tvarkymas yra draudžiamas, išskyrus esant BDAR numatytoms sąlygoms.

[17] Daugiau informacijos apie sutikimą rasite 29 straipsnio darbo grupės 2017 m. lapkričio 28 d. gairėse dėl sutikimo pagal Reglamentą 2016/679 Nr. WP259 red. 01.

[18] Daugiau informacijos apie biometrinių duomenų tvarkymą galite rasti 29 straipsnio darbo grupės 2012 m. balandžio 27 d. nuomonėje Nr. 3/2012 Dėl biometrinių technologijų pokyčių.

Tai, ar tvarkydami asmens duomenis galite naudoti biometrinius duomenis, priklauso nuo Jūsų atliekamų konkrečių asmens duomenų tvarkymo operacijų ir jomis siekiamų tikslų.

Manytina, kad geriau suprasti biometrinių duomenų tvarkymo ypatumus galėtų padėti VDAI atlikti sporto klubų patikrinimai. Aptariamu atveju, sporto klubai tvarkė savo klientų ir darbuotojų piršto atspaudo *modelius* (binarinius (dvejetainius) kodus), t. y. ne piršto atspaudo atvaizdą, praėjimo į sporto klubus ir darbo vietą kontrolės tikslais. Tiek klientų, tiek darbuotojų piršto atspaudo modeliai buvo tvarkomi remiantis sutikimu. Iš šių patikrinimų išplaukia keletas išvadų:

- Tvarkyti piršto atspaudo modelį su aiškiu klientų sutikimu galima, tačiau tam, kad sutikimas būtų laikomas duotu laisva valia, turi būti suteikiamas alternatyvus tapatybės nustatymo būdas, kuriuo nenaudojami biometriniai duomenys (pvz., praėjimo kortelė);
- Darbuotojų piršto atspaudo modelių tvarkymas remiantis sutikimu yra *negalimas*. Tokiam tvarkymui turi būti ieškoma kitos teisėto asmens duomenų tvarkymo sąlygos, pvz., tai gali būti aptarta kolektyvinėje sutartyje ar tvarkyti duomenis yra būtina dėl svarbaus viešojo intereso priežasčių, remiantis teisės aktų reikalavimais;
- Pasirinkus tvarkyti biometrinius duomenis, būtina taikyti tinkamas technines ir organizacines saugumo priemones, pvz., techninės, programinės ir tinklo įrangos inventorizavimo ir atnaujinimo įgyvendinimas, užtikrinimas, kad darbuotojai gebėtų konfidencialiai tvarkyti informaciją tiek techniniu, tiek asmeninio sąžiningumo požiūriu ir kad jie būtų tinkamai išmokyti informacinių technologijų sistemų saugumo kontrolės.

Taigi, tvarkydami biometrinius duomenis Jūs turite įvertinti, kokius duomenis, kokius tikslu ir kokiu būdu tvarkysite, kokiomis teisėto asmens duomenų tvarkymo sąlygomis remsitės bei turėsite skirti ypatingą dėmesį užtikrindami jų saugumą.

ASMENS KODO TVARKYMAS

Asmens kodas yra vienas iš asmens duomenų elementų – BDAR pateikiamame asmens duomenų apibrėžime minimas ir asmens kodas (pateikiamas kaip asmens identifikavimo numeris): „asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma, pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.“

Praktikoje yra susidariusi neteisinga nuomonė, kad asmens kodas yra specialus duomuo. Svarbu atkreipti dėmesį, kad asmens kodas yra įprastas asmens duomuo, tačiau jis gali būti laikomas tiesioginiu identifikatoriumi. Tai reiškia, kad asmens kodo, kurį turi asmuo, negali turėti niekas kitas toje pačioje valstybėje – pagal Lietuvos Respublikos gyventojų registro įstatymo 8 str. 2 d. asmens kodas yra unikalus ir nekeičiamas.

To paties straipsnio 3 d. nustatyta, kad asmens kodo struktūra jo suteikimo metu yra tokia: pirmasis skaitmuo atitinka lytį ir gimimo šimtmetį, antrasis ir trečiasis – gimimo metų du paskutinius skaitmenis, ketvirtasis ir penktasis – gimimo mėnesį, šeštasis ir septintasis – gimimo dieną, aštuntasis, devintasis ir dešimtasis – gimusiųjų tą pačią dieną įrašymo į Gyventojų registrą eilės numerį, vienuoliktasis skaitmuo yra pirmųjų dešimties skaitmenų kontrolinis skaičius.

Taigi, nors asmens kodas yra paprasta duomuo, dėl jo paminėtų ypatumų, atskleidžiančių kai kuriuos privataus gyvenimo aspektus, asmens kodo tvarkymas faktiškai gali kelti šiek tiek didesnes rizikas. Todėl asmens kodo tvarkymui gali būti taikomi papildomi reikalavimai.

Šiuo metu asmens kodo tvarkymui nustatomi kai kurie specialūs reikalavimai, daugiau informacijos apie tai pateikiama žemiau.

Kokius reikalavimus nustato BDAR asmens kodo tvarkymui?

BDAR faktiškai nenustato jokių reikalavimų asmens kodo tvarkymui – palieka galimybę asmens kodo tvarkymą reglamentuoti nacionaliniu lygiu.

BDAR 87 str. nustato, kad valstybės narės gali tiksliau apibrėžti konkrečias sąlygas, kuriomis tvarkomas nacionalinis asmens identifikavimo numeris ar bet kuris kitas bendro taikymo identifikatorius. Tuo atveju nacionalinis asmens identifikavimo numeris ar bet kuris kitas bendro taikymo identifikatorius naudojamas, tik jei laikomasi tinkamų duomenų subjekto teisių ir laisvių apsaugos priemonių pagal šį reglamentą.

Nacionaliniai reikalavimai asmens kodo tvarkymui?

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo reikalavimai asmens kodo tvarkymui (3 str.):

1. Asmens kodas gali būti tvarkomas, kai yra nors viena iš Reglamento (ES) 2016/679 6 straipsnio 1 dalyje nurodytų asmens duomenų tvarkymo teisėtumo sąlygų;
2. Draudžiama asmens kodą skelbti viešai;
3. Draudžiama tvarkyti asmens kodą tiesioginės rinkodaros tikslais.

Taigi, asmens kodą galite tvarkyti, kai yra bent viena iš asmens duomenų tvarkymo teisėtumo sąlygų (šios sąlygos paminėtos skyriuje „Teisėto asmens duomenų tvarkymo sąlygos“). Tačiau dėl asmens kodo tvarkymo, kaip ir dėl kitų asmens duomenų tvarkymo, reikėtų laikytis duomenų minimizavimo principo, t. y. netvarkyti asmens kodo, jei tai nėra būtina.

Pavyzdys

Jūsų įmonė interneto svetainėje renka asmens duomenis tiesioginei rinkodarai vykdyti ir sutikimo formoje prašo asmens kodo. Toks reikalavimas būtų neteisėtas, nes tiesioginės rinkodaros tikslu negalima tvarkyti asmens kodo. Vietoje asmens kodo galima prašyti nurodyti kitus duomenis, pvz., ryšio duomenis, kurie kartu su vardu ir pavarde padės identifikuoti konkretų asmenį.

Pavyzdys

Asmens kodo reikalavimas siekiant asmeniui apsipirkti elektroninėje parduotuvėje taip pat būtų perteklinis. Elektroninės parduotuvės paslaugas galima teikti ir netvarkant asmens kodo, o siekiant atsiskaityti už įsigytas prekes ir (ar) paslaugas, asmuo pats suveda atsiskaitymo duomenis.