2018-09-05

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).

Bendrasis duomenų apsaugos reglamentas yra **tiesioginio taikymo** Europos Sąjungos teisės aktas, taigi duomenų valdytojai ir duomenų tvarkytojai privalo užtikrinti, kad asmens duomenų tvarkymas atitiktų tiek jo nuostatas, tiek ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo nuostatas.

Bendrasis duomenų apsaugos reglamentas įtvirtina duomenų valdytojo atskaitomybės principą, kuris reiškia, kad duomenų valdytojas (duomenų tvarkytojas) yra atsakingas už tai, kad būtų laikomasi šio reglamento nuostatų ir turi **sugebėti įrodyti**, kad jų laikomasi.

Bendrojo duomenų apsaugos reglamento taikymas priklauso **ne nuo Jūsų įmonės dydžio**, bet nuo atliekamo asmens duomenų tvarkymo pobūdžio. Kita vertus, ne visos BDAR nustatytos prievolės taikomos mažoms ir vidutinėms įmonėms, pvz., įmonėms, kuriose dirba mažiau kaip 250 darbuotojų, nereikia tvarkyti duomenų tvarkymo veiklos įrašų (išskyrus numatytas išimtis). Duomenų apsaugos pareigūną įmonės turi paskirti tik tuomet, jeigu pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai dideliu mastu stebėti asmenis (duomenų subjektus), kai dideliu mastu tvarkomi specialių kategorijų duomenys ir t. t.

Valstybinė duomenų apsaugos inspekcija, prisidėdama prie asmens duomenų apsaugos reformos įgyvendinimo Lietuvoje, parengė informaciją įmonėms ir fiziniams asmenims, savo profesinėje veikloje tvarkantiems asmens duomenis (t. y. **duomenų valdytojams** ir **duomenų tvarkytojams**), kuri padėtų taikyti naują asmens duomenų apsaugos teisinį reguliavimą praktikoje.

Norint geriau suprasti BDAR reikalavimus ir kaip juos tinkamai įgyvendinti praktikoje, rekomenduojame susipažinti su Direktyvos 95/46/EB 29 straipsnio darbo grupės, kuri nuo 2018 m. gegužės 25 d. reformuota į Europos duomenų apsaugos valdybą, parengtomis gairėmis bei nuomonėmis dėl asmens duomenų tvarkymo ir privatumo apsaugos. Šiuo metu dalis šių dokumentų prieinami anglų kalba, tačiau ateityje bus pateikti ir oficialūs vertimai į lietuvių kalbą.

Europos duomenų apsaugos valdybos parengtus dokumentus galite rasti šiais adresais:

- http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360;
- https://www.ada.lt/go.php/lit/Metodine-informacija.

PASTABA. Rengiant metodinę medžiaga remtasi Bendruoju duomenų apsaugos reglamentu, Europos Komisijos pateikiama informacija, Direktyvos 95/46/EB 29 straipsnio darbo grupės gairėmis ir kitų šalių praktika.

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

EDAV – Europos duomenų apsaugos valdyba

ES – Europos Sąjunga

VDAI – Valstybinė duomenų apsaugos inspekcija

TURINYS

KAS YRA ASMENS DUOMENYS?

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.

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

2. BDAR nustatomos taisyklės, **susijusios tik su fizinių asmenų apsauga**, tvarkant jų asmens duomenis. Mirusių asmenų duomenų tvarkymui BDAR nuostatos netaikomas.

3. 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., pagal 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

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.

Atkreiptinas dėmesys į tai, kad Europos Sąjungos Teisingumo Teismas 2017 m. kovo 9 d. sprendime byloje Nr. C-398/15 pažymėjo, kad su asmenų, kurie yra įgalioti atstovauti bendrovei jos santykiuose su trečiosiomis šalimis ir teisminiuose procesuose, taip pat su asmenų, kurie dalyvauja atliekant bendrovės administravimo, priežiūros ir kontrolės darbus, tapatybe susiję duomenys yra asmens duomenys, kaip jie suprantami pagal 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo. Minėtame sprendime Europos Sąjungos Teisingumo Teismas taip pat pastebėjo, jog iš Teisingumo Teismo jurisprudencijos matyti, kad aplinkybė, jog ši informacija priskirtina prie profesinės veiklos srities, nereiškia, kad ji nėra asmens duomenys.

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 mirusį asmenį nėra asmens duomenys, todėl mirusių asmenų duomenų tvarkymui BDAR netaikomas.

Mirusių asmenų duomenų tvarkymui BDAR nuostatos netaikomas.

- 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 galima 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 galima 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.

AR AŠ TVARKAU 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 ir tokiu atveju jai taikomi BDAR nustatyti reikalavimai.

Duomenų tvarkymas – tai plati sąvoka, **apimanti visus įmanomus veiksmus su asmens duomenimis**, tokius kaip rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

BDAR taikomas, kai asmens duomenys renkami, naudojami ir saugomi:

- **Automatiniu būdu** – skaitmenine forma (pvz., informacinėje sistemoje, naudojant vaizdo kameras ir kt.);
- **Neautomatiniu būdu** – susistemintame rinkinyje popierine forma (pvz., kartotekose ir kt.).

Pavyzdžiai

- Personalo valdymas ir darbo užmokesčio administravimas;
- Prieiga prie kontaktų duomenų bazės, kurioje yra asmens duomenų, ir (arba) galimybė naudotis šia duomenų baze;
- Tiesioginės rinkodaros (reklaminių) elektroninių laiškų siuntimas;
- Dokumentų, kuriuose yra asmens duomenų, naikinimas;
- Prekyba elektroninėje erdvėje (el. parduotuvė);
- Asmens nuotraukos skelbimas interneto svetainėje;
- Vaizdo įrašymas (apsauginė vaizdo stebėjimo sistema);
- Duomenų saugojimas duomenų bazėje, „Excel“ lentelėje, informacinėje sistemoje, popieriniame žurnale;
- Duomenų gavimas iš registrų, bankų ar kt.;
- Duomenų teikimas kurjerių tarnyboms, draudimo įmonėms;
- Duomenų paskelbimas skelbimų lentoje, internete;
- Telefoninių pokalbių įrašymas ir saugojimas ir kt.

Svarbu: viena įmonė gali tvarkyti asmens duomenis ir keliais tikslais, pvz., personalo duomenų tvarkymas, sveikatos priežiūros paslaugų teikimo, turto apsaugos (jei vykdomas vaizdo stebėjimas).

Atkreiptinas dėmesys, kad *darbuotojų duomenų tvarkymas* taip pat yra laikomas asmens duomenų tvarkymu, kuriam taikomas BDAR.

Pavyzdys

Bendrovė, surinkusi kandidatų užimti tam tikras pareigas asmens duomenis, po atrankos laimėjusio kandidato duomenis automatiniu būdu tvarko tikslu suformuoti darbuotojo asmens bylą.

Pastebėtina, kad personalo valdymo tikslu gali būti tvarkomi ne tik darbuotojo, bet ir trečiojo asmens, pvz., darbuotojo vaikų ar kitų šeimos narių ir pan., duomenys.

Pavyzdys

Lietuvos Respublikos darbo kodekso 138 straipsnio 3 dalyje numatyta, kad darbuotojams, auginantiems neįgalų vaiką iki aštuoniolikos metų arba du vaikus iki dvylikos metų, suteikiama viena papildoma poilsio diena per mėnesį (arba sutrumpinamas darbo laikas dviem valandomis per savaitę), o auginantiems tris ir daugiau vaikų iki dvylikos metų – dvi dienos per mėnesį (arba sutrumpinamas darbo laikas keturiomis valandomis per savaitę), mokant darbuotojui jo vidutinį darbo užmokestį. Šiuo atveju, darbdavys, kaip duomenų valdytojas, tvarko duomenis apie darbuotojų turimus vaikus iki dvylikos metų, siekdamas įgyvendinti darbuotojo teisę į papildomą poilsio dieną.

AR MAN TAIKOMAS BENDRASIS DUOMENŲ APSAUGOS REGLAMENTAS?

Kai įmonė renka, saugo ar kitokiu būdu tvarko asmens duomenis apie savo darbuotojus ar savo klientus, jai taikomos BDAR nuostatos.

BDAR yra aktualus visoms įmonėms, kurios turi klientų duomenų bazes, vykdo tiesioginę rinkodarą (pvz., siunčia naujienlaiškius), vykdo vaizdo stebėjimą patalpose, renka ir saugo savo darbuotojų asmens duomenis ar kitų įmonių perduotus duomenis ir pan.

BDAR yra taikomas, kai asmens duomenis tvarko (renka, saugo ar atlieka kitus duomenų tvarkymo veiksmus):

- Juridinis asmuo (įmonė, įstaiga, organizacija ar pan.);
- Fizinis asmuo, besiverčiantis profesine ar komercine veikla.

BDAR taikomas visiems asmens duomenims, susijusiems su profesinę veiklą vykdančiais fiziniais asmenimis, pvz., įmonės darbuotojais, pvz., darbo el. pašto adresams, tokiems kaip vardas.pavarde@įmone.eu, arba darbuotojų darbo telefono numeriams.

Jeigu asmens duomenis socialiniuose tinkluose tvarko (skelbia) fizinis asmuo, vykdydamas ne asmeninę ar namų ūkio priežiūros, o profesinę ar komercinę veiklą, pvz., versdamasis individualia veikla, arba juridinis asmuo, tuomet tokiam asmens duomenų tvarkymui taikomos BDAR nuostatos.

Pažymėtina, kad duomenų valdytojams arba duomenų tvarkytojams, kurie suteikia priemones asmens duomenų tvarkymui vykdant pirmiau nurodytą asmeninę ar namų ūkio priežiūros veiklą, pvz., socialinių tinklų valdytojams, BDAR taip pat yra taikomas.

Pavyzdžiai

Individualiojoje 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 priklausančioje 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 aksesuarų ar avalynės prekyba internetu. Kad galėtumėte vykdyti savo veiklą renkate klientų (fizinių asmenų) asmens duomenis (kontaktinius duomenis, pirkimo istoriją (ką ir kada pirko), tokiu atveju Jūs laikomas asmens duomenų valdytoju ir Jums taikomas BDAR.

BDAR taikomas asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam automatizuotomis priemonėmis (pvz., informacinėje sistemoje, naudojant vaizdo kameras) ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis (pvz., kartotekose).

Bendrojo duomenų apsaugos reglamento teritorinis taikymas

BDAR taikomas asmens duomenų tvarkymui, kai:

- Asmens duomenis tvarko ES esanti įmonė, vykdydama savo veiklą, neatsižvelgiant į tai, ar duomenys tvarkomi ES, ar ne.

- ES esančių duomenų subjektų asmens duomenis tvarko ES neįsisteigusi įmonė ir duomenų tvarkymo veikla yra susijusi su prekių arba paslaugų siūlymu tokiems duomenų subjektams ES (nepaisant to, ar už šias prekes arba paslaugas duomenų subjektui reikia mokėti) arba stebi fizinių asmenų elgesį ES.
- Asmens duomenis tvarko įmonė, įsisteigusi ne ES, o vietoje, kurioje pagal viešąją tarptautinę teisę taikoma valstybės narės teisė.

Bendrojo duomenų apsaugos reglamento taikymo išimtys

BDAR netaikomas asmens duomenų tvarkymui, kai:

- 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. Tačiau jeigu asmuo naudojasi asmens duomenimis ne asmeniniais tikslais, o, pvz., socialinei, kultūrinei ar finansinei veiklai, privaloma laikytis asmens duomenų apsaugos teisės akto.
- Tvarkomi *mirusių asmenų duomenys*;
- Tvarkomi *juridinių asmenų duomenys* (*išskyrus juridinių asmenų darbuotojų*). Atkreiptinas dėmesys, kad informacija, susijusi su vienanare įmone, gali būti laikoma asmens duomenimis, jeigu pagal ją galima nustatyti fizinio asmens tapatybę.
- Duomenis tvarko *kompetentingos valdžios institucijos nusikalstamų veikų prevencijos, tyrimo, nustatymo ar patraukimo baudžiamojon atsakomybėn už jas, baudžiamųjų sankcijų vykdymo, įskaitant* apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją, tikslais;
- Duomenys tvarkomi vykdant veiklą, kuriai ES teisė netaikoma.

Pavyzdžiai

Kai BDAR taikomas

Lietuvos Respublikoje įsisteigusi įmonė teikia kelionių paslaugas Baltijos šalyse esantiems klientams ir tuo tikslu tvarko fizinių asmenų asmens duomenis.

Jūsų įmonė yra nedidelė mokslo įstaiga, veikianti internetu ir įsisteigusi ES nepriklausančioje šalyje. Jos pagrindinė tikslinė grupė yra ispanų ir portugalų kalbų universitetai ES. Įmonė nemokamai konsultuoja įvairių universitetinių kursų klausimais, o studentai, kurie nori naudotis jūsų internetine medžiaga, privalo turėti naudotojo vardą ir slaptažodį. Jūsų įmonė suteikia naudotojo vardą ir slaptažodį studentams užpildžius registracijos formą.

Kai BDAR netaikomas

Asmuo pasinaudoja savo asmenine adresų knygele, kad elektroniniu paštu pakviestų draugus į vakarėlį (išimtis dėl namų ūkio).

IT paslaugas teikianti įmonė, įsteigta ES nepriklausančioje šalyje, teikia IT priežiūros paslaugas klientams ES ir už ES ribų. Paslaugos aprašomos kinų kalba, todėl tikėtina, kad skirtos ne ES piliečiams. Jeigu IT įmonės paslaugos nėra konkrečiai skirtos fiziniams asmenims ES, jai netaikomos BDAR nustatytos taisyklės.

KADA GALIMA TVARKYTI ASMENS DUOMENIS?

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).

Įmonė turi 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 vienareikšmiais 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 vienareikšmiais 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:

- Duomenų valdytojas **turi 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 Civiliniame kodekse ir kituose teisės aktuose nustatytus reikalavimus, o sutarties sudarymui ir vykdymui reikalingas asmens duomenų tvarkymas turi atitikti BDAR nustatytus asmens duomenų tvarkymo principus – asmens duomenys turi būti:

- Tvarkomi vadovaujantis teisėtumo, sąžiningumo ir skaidrumo principais;
- Renkami nustatytais, aiškiai apibrėžtais ir teisėtais tikslais;
- Tik būtinos apimties;
- Tikslūs ir prireikus atnaujinami;
- Laikomi tokia forma, kad asmens tapatybę galima būtų nustatyti ne ilgiau, negu tai būtina sutartyje nustatytiems tikslams pasiekti;
- Tvarkomi tokiu būdu, kad naudojant atitinkamas technines ir organizacines priemones, būtų užtikrintas tinkamas asmens duomenų saugumas.

Įmonė turi 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 įmonė asmens duomenis tvarko vykdydama jai 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 Respublikos 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.

Įmonė privalo 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 tvarkymas gali būti grindžiamas įmonės teisėtais interesais.

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

- 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, reikėtų 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.

JEI PASITELKIU ĮMONĘ (ASMENĮ) ATLIKTI TAM TIKRUS ASMENS DUOMENŲ TVARKYMO VEIKSMUS?

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 įmonė pasitelkia duomenų tvarkytoją atlikti tam tikrus asmens duomenų tvarkymo veiksmus, tarp jų 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 turi būti konkrečiai apibrėžta asmens duomenų tvarkymo apimtis ir aiškiai nurodytos duomenų tvarkytojų pareigos ir atsakomybės:

- 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 turėtų būti nustatyta, 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 įstatais 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 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 įmonės (duomenų valdytojai), sudarydamos sutartis su duomenų tvarkytojais, turėtų būti itin atidūs: sutartyse konkrečiai ir aiškiai įtvirtinti reikalavimus duomenų tvarkymui, detalizuoti 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.

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 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 duomenys privalo būti sunaikinti. Todėl svarbu įdiegti procedūras, užtikrinančias, kad duomenys, pasibaigus jų saugojimo terminui, toliau nebebūtų tvarkomi.

Pavyzdys

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

BDAR įtvirtina šias teises asmenims, kurių asmens duomenis įmonė renka ir toliau naudoja:

- Teisė būti informuotam;
- Teisė susipažinti su savo asmens duomenimis;
- Teisė reikalauti ištaisyti duomenis;
- Teisė reikalauti ištrinti duomenis („teisė būti pamirštam“);
- Teisė reikalauti apriboti duomenų tvarkymą;
- Teisė į duomenų perkeliamumą;
- Teisė nesutikti;
- Teisė reikalauti, kad asmeniui nebūtų taikomas automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą.

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, visų pirma dėl jų pasikartojančio pobūdžio, įmonė gali imti pagrįstą mokestį, atsižvelgdama į administracines išlaidas, už informacijos ar pranešimo teikimą arba prašomų veiksmų vykdymą, arba atsisakyti imtis veiksmų pagal prašymą.

Įmonei tenka pareiga įrodyti, kad prašymas yra akivaizdžiai nepagrįstas arba neproporcingas.

Asmens tapatybės nustatymas ir atstovavimas

Jei įmonė turi pagrįstų abejonių dėl prašymą pateikusio fizinio asmens tapatybės, įmonė gali paprašyti pateikti papildomos informacijos, reikalingos norint patvirtinti asmens, kurio duomenis tvarko, tapatybę (pvz., paspausti patvirtinimo nuorodą, įvesti vartotojo vardą ar slaptažodį).

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

Per kiek laiko įmonė turi įgyvendinti asmens teises?

Įmonė *per vieną mėnesį* nuo prašymo gavimo privalo atsakyti į 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.

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 privalu pranešti asmeniui, kad terminas bus pratęsiamas ir nurodyti termino pratęsimo priežastį.

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.

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.

Ką įmonė turi padaryti, jeigu ji nusprendė neįgyvendinti asmens teisės?

Nedelsiant, tačiau ne vėliau kaip per vieną mėnesį nuo prašymo gavimo dienos **informuoti asmenį apie:**

- Priežastis, dėl kurių nesiima veiksmų;
- Teisę pateikti skundą VDAI arba teismui.

TEISĖ BŪTI INFORMUOTAM

Kai įmonė renka ir tvarko asmens duomenis, ji privalo pateikti duomenų subjektui **šią informaciją**:

- Įmonės pavadinimą, kontaktinius duomenis;
- Duomenų apsaugos pareigūno, jeigu taikoma, kontaktinius duomenis;
- Duomenų tvarkymo tikslus, dėl kurių ketinama tvarkyti asmens duomenis;
- Duomenų tvarkymo teisinį pagrindą;
- Jei yra, asmens duomenų gavėjus arba asmens duomenų gavėjų kategorijas;
- Kai taikoma, apie įmonės ketinimą asmens duomenis perduoti į trečiąją valstybę (nepriklausančią ES).

Taip pat kitą informaciją, būtiną duomenų tvarkymo sąžiningumui ir skaidrumui užtikrinti:

- 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 pateikti skundą VDAI ar teismui;
- Ar asmens duomenų pateikimas yra teisės aktais arba sutartyje numatytas reikalavimas, 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.

Informacija asmeniui turi būti pateikiama glausta, skaidria ir suprantama forma, aiškia ir paprasta kalba.

Kada įmonė turėtų pateikti asmenims informaciją apie jų duomenų tvarkymą?

Laikas, kada asmuo turi būti informuotas apie duomenų tvarkymą, priklauso nuo to, iš kur gaunami duomenys bei kokius veiksmus ketinama atlikti:

1) Kai įmonė renka asmens duomenis iš asmens, informacija turi būti pateikta iš karto, duomenų gavimo metu.
2) Kai įmonė gauna asmens duomenis iš kito šaltinio, informacija asmeniui turi būti pateikta:
   - Per pagrįstą laikotarpį, kai gaunami asmens duomenys, ir ne vėliau kaip per vieną mėnesį;
   - Jeigu asmens duomenys bus naudojami ryšiams su asmeniu palaikyti – ne vėliau kaip pirmą kartą susisiekiant su tuo asmeniu.
   - Jei planuojama atskleisti informaciją kitiems – ne vėliau kaip atskleidžiant duomenis pirmą kartą.

Informacija gali būti pateikiama sutartyje, interneto svetainėje ar kt., svarbiausia aiškiai ir lengvai asmeniui prieinama forma.

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

- Asmuo jau turi informaciją;
- Informacijos teikimas asmeniui būtų neįmanomas;
- Informacijos teikimas asmeniui pareikalautų neproporcingų pastangų;
- Įmonės pagal įstatymus reikalaujama gauti ar atskleisti asmens duomenis;
- Įmonei taikomas profesinės paslapties reikalavimas, kurį reglamentuoja įstatymai, kurie apima asmens duomenis.

Asmuo turi būti informuojamas apie jo asmens duomenų tvarkymą, o įmonė turi pareigą įrodyti, kad ji tinkamai informavo asmenį, kurio duomenis tvarko.

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.

Jeigu įmonė ketina tvarkyti asmens duomenis kitu tikslu, negu tas, kuriuo asmens duomenys buvo surinkti, prieš tai privalu pateikti asmeniui, kurio duomenis tvarkys, informaciją apie tą kitą tikslą ir visą kitą atitinkamą papildomą informaciją.

Nurodyta informacija neteikiama tuo atveju, jeigu asmuo tokią informaciją jau turi.

Pavyzdys

Asmens duomenys buvo surinkti iš asmens ir tvarkomi elektroninės prekybos tikslu, tačiau, nusprendus asmens duomenis tvarkyti ir tiesioginės rinkodaros tikslu, būtina 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 ir gauti atskirą sutikimą dėl asmens duomenų tvarkymo tiesioginės rinkodaros tikslu.

TEISĖ SUSIPAŽINTI SU SAVO DUOMENIMIS

Asmuo, kurio duomenis renkate ir tvarkote, turite teisę susipažinti su savo duomenimis ir gauti jų kopiją bei bet kokią susijusią papildomą informaciją (kaip antai, asmens duomenų tvarkymo priežastį, naudojamų asmens duomenų kategorijas ir pan.).

Asmuo turi teisę iš įmonės 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;
- Apie asmenį turimą informaciją;
- Duomenų gavėjus arba duomenų gavėjų kategorijas, kuriems buvo arba bus atskleisti asmens duomenys, visų pirma – duomenų gavėjus trečiosiose valstybėse arba tarptautinėse organizacijose;
- Kai įmanoma, numatomą asmens duomenų saugojimo laikotarpį arba, jei neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti;
- Teisę prašyti įmonės ištaisyti arba ištrinti asmens duomenis ar apriboti su asmeniu susijusių asmens duomenų tvarkymą arba nesutikti su tokiu tvarkymu;
- Teisę pateikti skundą 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

Įmonė asmeniui, kurio duomenys tvarkomi, pagal jo prašymą turi pateikti visą saugomą informaciją. Pavyzdžiui, internetinė parduotuvė turi pateikti, kada asmuo, kurio duomenys tvarkomi, pirmą kartą pradėjo naudotis paslaugomis, kada ir ką pirko, kokias prekes grąžino bei kada ir kokia suma pinigų grąžinta ar atsisakyta priimti grąžintas prekes.

Privalu patikrinti asmens, prašančio leisti susipažinti su savo asmens duomenimis, tapatybę, 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

Asmuo, kurio duomenys tvarkomi, turi teisę reikalauti, kad įmonė nepagrįstai nedelsdama ištaisytų netikslius su juo susijusius asmens duomenis. Atsižvelgiant į tikslus, kuriais duomenys buvo tvarkomi, asmuo turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys, pateikdamas papildomą prašymą.

Pavyzdys

Jei prašymą asmuo, kurio duomenys tvarkomi, pateikia žodžiu, rekomenduotina užsirašyti bet kokį žodinį prašymą bei pateikti rašytinį atsakymą, nes tokiu būdu bus galima pateikti įrodymus apie informacijos keitimo priežastis.

TEISĖ REIKALAUTI IŠTRINTI DUOMENIS („TEISĖ BŪTI PAMIRŠTAM“)

Asmuo turi teisę reikalauti, kad įmonė nepagrįstai nedelsdama ištrintų su juo susijusius asmens duomenis, o įmonė yra įpareigota nepagrįstai nedelsdama ištrinti asmens duomenis (ši teisė, dažnai vadinama **teise būti pamirštam**, taikoma ir **internetinėje erdvėje**) šiais atvejais:

- Kai asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi;
- Asmuo atšaukia sutikimą ir nėra jokio kito teisinio pagrindo tvarkyti duomenis;
- Asmuo nesutinka su duomenų tvarkymu ir nėra viršesnių teisėtų priežasčių tvarkyti duomenis arba asmuo, kurio duomenys tvarkomi, nesutinka su duomenų tvarkymu tiesioginės rinkodaros tikslu.
- Asmens duomenys buvo tvarkomi neteisėtai;
- Asmens duomenys turi būti ištrinti laikantis įstatymuose nustatytos teisinės prievolės;
- Asmens duomenys buvo surinkti *iš vaiko*, kuriam buvo siūlomos *informacinės visuomenės paslaugos.*

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.

Kai įmonė asmens duomenis paskelbė viešai ir šie duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi, privaloma asmens duomenis ištrinti. Įmonė privalo, atsižvelgdama į turimas technologijas ir įgyvendinimo sąnaudas, imtis pagrįstų veiksmų, įskaitant technines priemones, *kad informuotų kitas duomenis tvarkančias įmones*, jog asmuo paprašė, kad tokios įmonės ištrintų visas nuorodas į tuos asmens duomenis arba jų kopijas ar dublikatus.

Kada įmonė gali neištrinti asmens duomenų?

Reikėtų nepamiršti, kad teisė būti pamirštam nėra absoliuti teisė, t. y. kad turi būti saugomos ir kitos teisės bei įgyvendinamos nustatytos pareigos, todėl ši teisė gali būti neįgyvendinta:

- Siekiant pasinaudoti teise į saviraiškos ir informacijos laisvę;
- Įmonės įpareigotos tvarkyti asmens duomenis pagal teisės aktus siekiant atlikti užduotį, vykdomą viešojo intereso labui, arba vykdant įmonei pavestas viešosios valdžios funkcijas;
- Kai tvarkyti duomenis būtina profilaktinės arba darbo medicinos tikslais, dėl viešojo intereso priežasčių visuomenės sveikatos srityje ir specialių kategorijų asmens duomenis;

- Archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais;
- Siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus.

Pavyzdys

Greitųjų kreditų bendrovė gauna kliento prašymą uždaryti visas sąskaitas ir 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.

Įmonei nusprendus, kad ištrinti asmens duomenis nėra pagrindo, ji vis tiek turi informuoti pareiškėją ir paaiškinti, kodėl ji mano, kad neturi ištrinti duomenų ir informuoti apie teisę pateikti skundą dėl šio sprendimo VDAI ar teismui.

Kam įmonė turi pranešti apie asmens duomenų ištaisymą ar ištrynimą?

Įmonės taip pat privalo imtis pagrįstų veiksmų, kad informuotų kitas įmones, kurios tvarko asmens duomenis, kad asmuo prašo ištrinti bet kokias nuorodas į savo asmens duomenis ar jų kopijas.

Informacija turėtų būti pateikiama kiekvienam duomenų gavėjui, kuriam buvo atskleisti asmens duomenys, įmonė praneša apie bet kokį asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą, nebent to padaryti nebūtų įmanoma arba tai pareikalautų neproporcingų pastangų. Asmeniui pageidaujant, įmonė informuoja asmenį apie tuos duomenų gavėjus.

TEISĖ APRIBOTI DUOMENŲ TVARKYMĄ

Duomenų tvarkymo apribojimas yra saugomų asmens duomenų žymėjimas siekiant apriboti jų tvarkymą ateityje.

Pavyzdys

Informacinėje sistemoje konkretaus asmens byloje yra pažymima, kad asmens duomenų tvarkymas apribotas, tokiu būdu užblokuojama galimybė šio asmens duomenis ištrinti, pakeisti, pateikti kitoms įmonėms ir pan.

Asmuo, kurio duomenys tvarkomi, turi teisę reikalauti, kad įmonė apribotų duomenų tvarkymą, kai yra vienas iš šių atvejų:

- Asmuo, kurio duomenys tvarkomi, užginčija duomenų tikslumą tokiam laikotarpiui, per kurį įmonė gali patikrinti asmens duomenų tikslumą;
- Asmens duomenų tvarkymas yra neteisėtas ir asmuo, kurio duomenys tvarkomi, nesutinka, kad duomenys būtų ištrinti, ir vietoj to prašo apriboti jų naudojimą;
- Įmonei nebereikia asmens duomenų nustatytais tvarkymo tikslais, tačiau jų reikia asmeniui, kurio duomenys tvarkomi, siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus;
- Asmuo, kurio duomenys tvarkomi, papriešTaravo duomenų tvarkymui, kol bus patikrinta, ar įmonės teisėtos asmens duomenų tvarkymo priežastys yra viršesnės už asmens, kurio duomenys tvarkomi, priežastis.

Kai duomenų tvarkymas yra apribotas remiantis aukščiau nurodytais pagrindais, tokius asmens duomenis galima tvarkyti, išskyrus saugojimą, tik gavus asmens, kurio duomenys tvarkomi, sutikimą arba

siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus, arba apsaugoti kito fizinio ar juridinio asmens teises, arba dėl svarbaus viešojo intereso.

Kokiu būdu įmonė gali apriboti asmens duomenų tvarkymą?

Būdai, kuriais ribojamas asmens duomenų tvarkymas, galėtų, būti tokie:

- Laikinai perkelti atrinktus duomenis į kitą tvarkymo sistemą, padaryti atrinktus asmens duomenis neprieinamus naudotojams;
- Laikinai išimti paskelbtus duomenis iš interneto svetainės;
- Automatiniuose susistemintuose rinkiniuose duomenų tvarkymo ribojimas iš esmės turėtų būti užtikrinamas techninėmis priemonėmis taip, kad asmens duomenys nebūtų toliau tvarkomi ir jų nebebūtų galima pakeisti;
- Tai, kad asmens duomenų tvarkymas yra apribotas, sistemoje turėtų būti aiškiai nurodyta.

Prieš panaikindama apribojimą kam ir kada įmonė turi pranešti?

Įmonė, prieš panaikindama apribojimą tvarkyti duomenis, informuoja asmenį, kurio duomenys tvarkomi.

TEISĖ Į DUOMENŲ PERKELIAMUMĄ

Ši teisė taikoma, kai asmuo duomenis pateikė savo **sutikimu** arba tvarkyti asmens duomenis reikia vykdant **sutartį**.

Teisė į duomenų perkeliamumą taikoma, kai duomenys yra tvarkomi automatizuotomis priemonėmis ir kai tai techniškai įmanoma. Asmuo, kurio duomenys tvarkomi, turi teisę gauti susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu su juo susijusius asmens duomenis, kuriuos jis pateikė įmonei, ir turi teisę persiųsti tuos duomenis kitai įmonei, o įmonė, kuriai asmens duomenys buvo pateikti, turi nesudaryti tam kliūčių.

Jei techniškai įmanoma, asmuo gali prašyti, kad jo asmens duomenys būtų tiesiogiai persiųsti kitai įmonei, kurios paslaugomis asmuo nori naudotis.

Pavyzdys

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

Pavyzdys

Finansų įstaigos neprivalo atsakyti į prašymą perkelti asmens duomenis, tvarkomus vykdant jų prievoles užkirsti kelią pinigų plovimui bei kitiems finansiniams nusikaltimams ir juos aptikti, kadangi duomenys tokiu atveju yra tvarkomi įstatymų pagrindu.

Kokie yra pagrindiniai teisės į duomenų perkeliamumą elementai, kada galioja teisė į duomenų perkeliamumą, kaip asmuo, kurio duomenys tvarkomi teisės taikomos duomenų perkeliamumui, kaip turi būti suteikiami perkeliami duomenys, kada galima netaikyti teisės į duomenų perkeliamumą, plačiau

aiškinama Direktyvos 95/46/EB 29 straipsnio duomenų apsaugos darbo grupės patvirtintose gairėse dėl duomenų perkeliamumo, kurias galima rasti adresu: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

TEISĖ NESUTIKTI

Asmuo (duomenų subjektas) turi teisę dėl **su juo konkrečiu atveju susijusių priežasčių** bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi, kai toks duomenų tvarkymas vykdomas siekiant atlikti **užduotį, vykdomą viešojo intereso labui** arba vykdant duomenų valdytojui **pavestas valdžios funkcijas** ar **siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų**, išskyrus, kai duomenų subjekto interesai yra viršesni, ypač, kai duomenų subjektas yra vaikas.

Įmonė turi informuoti asmenį apie teisę nesutikti, kad būtų tvarkomi jo asmens duomenys.

Asmeniui išreiškus nesutikimą dėl su juo susijusių asmens duomenų tvarkymo, įmonė privalo nutraukti asmens duomenų tvarkymą, išskyrus atvejus, kai įmonė įrodo, kad duomenys turi būti toliau tvarkomi dėl įtikinamų teisėtų priežasčių, kurios yra viršesnės už asmens, kurio duomenys tvarkomi interesus, teises ir laisves, arba siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus. *Pareiga įrodyti, kad įtikinamas teisėtas įmonės interesas yra viršesnis už asmens, kurio duomenys tvarkomi, interesus arba pagrindines teises ir laisves, tenka įmonei.*

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

Pavyzdys

Kai asmens duomenys tvarkomi tiesioginės rinkodaros tikslais, asmuo, kurio duomenys tvarkomi, turi teisę bet kuriuo metu nesutikti automatizuotomis priemonėmis, kad su juo susiję asmens duomenys būtų tvarkomi rinkodaros tikslais, įskaitant profiliavimą, kiek jis susijęs su tokia tiesiogine rinkodara.

Kai asmuo, kurio duomenys tvarkomi, prieštarauja duomenų tvarkymui tiesioginės rinkodaros tikslais, asmens duomenys tokiais tikslais negali būti tvarkomi.

Jeigu asmuo nesutinka, kad jo asmens duomenys būtų tvarkomi tiesioginės rinkodaros tikslais, įmonė privalo nemokamai patenkinti asmens prašymą ir nutraukti asmens duomenų tvarkymą.

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 reklaminės medžiagos. Įmonė turėtų nutraukti asmens duomenų tvarkymą tiesioginės rinkodaros tikslais ir nebesiųsti jokių pasiūlymų. Ši paslauga privalo būti nemokama.

Tačiau įmonė gali toliau tvarkyti asmens duomenis, nepaisydama asmens prieštaravimų, jeigu:

- Duomenys tvarkomi mokslinių ar istorinių tyrimų ir statistinių duomenų rinkimo tikslais ir jie yra būtini vykdant užduotį viešojo intereso labui;
- Duomenys tvarkomi remiantis teisėtais interesais arba vykdant užduotį viešojo intereso labui vykdant viešosios valdžios funkcijas ir įmonė gali įrodyti, kad įtikinamas teisėtas interesas yra viršesnis už asmens interesus, teises ir laisves.

NE VIEN AUTOMATIZUOTAS ATSKIRŲ SPRENDIMŲ PRIĖMIMAS, ĮSKAITANT PROFILIAVIMĄ

Asmuo, kurio duomenys tvarkomi, turi teisę reikalauti, kad jam nebūtų taikomas vien tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam kyla teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį.

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

Profiliavimas atliekamas tada, kai vertinami asmens 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.

Profiliavimas ir automatizuotas sprendimų priėmimas yra įprasta praktika įvairiuose sektoriuose, pvz., bankininkystės, finansų, mokesčių ir sveikatos priežiūros. Jis gali būti efektyvesnis, tačiau ne toks skaidrus.

Pavyzdžiai

Biotechnologijų bendrovė tiesiogiai vartotojams siūlo atlikti genetinius tyrimus, siekiant įvertinti ir prognozuoti su liga susijusį ir (arba) sveikatai gresiantį pavojų.

Bendrovė, remdamasi jos svetainės naudojimu arba naršymu joje, kuria asmenų elgesio arba rinkodaros profilius.

Automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą, galimas, jeigu sprendimas:

- Yra būtinas siekiant sudaryti arba vykdyti sutartį tarp asmens ir įmonės;
- Yra leidžiamas teisės aktais, kurie taikomi įmonei ir kuriais taip pat nustatomos tinkamos priemonės asmens teisėms bei laisvėms ir teisėtiems interesams apsaugoti; arba
- Yra pagrįstas aiškiu asmens, kurio duomenys tvarkomi, sutikimu.

Automatizuotas atskirų sprendimų priėmimas, grindžiamas specialių kategorijų asmens duomenų tvarkymu, galimas kai:

- Asmuo davė savo aiškų sutikimą;
- Tvarkyti duomenis būtina dėl svarbaus viešojo intereso priežasčių, remiantis įstatymais.

Abiem šiais atvejais priimtas sprendimas turi apsaugoti asmens teises ir laisves tinkamomis apsaugos priemonėmis. Įmonė turi bent jau informuoti apie asmens teisę reikalauti žmogaus įsikišimo ir sudaryti reikalingus procedūrinius susitarimus.

Išskyrus atvejus, kai automatizuotas sprendimas yra pagrįstas įstatymu, įmonė privalo:

- Informuoti asmenį apie automatizuotą sprendimų priėmimą;
- Suteikti asmeniui teisę reikalauti, kad automatizuotą sprendimą peržiūrėtų asmuo;
- Suteikti asmeniui galimybę ginčyti automatizuotą sprendimą.

Pavyzdys

Jeigu greitųjų kreditų bendrovė automatizuotai priima sprendimą dėl vartojamosios paskolos suteikimo tam tikram asmeniui, tas asmuo turėtų būti informuojamas apie automatizuotą sprendimą bei jam turėtų būti suteikta galimybė ginčyti sprendimą ir prašyti, kad jį peržiūrėtų žmogus.

DUOMENŲ VALDYTOJŲ PAREIGOS

Asmens duomenų tvarkymas, vadovaujantis BDAR, turi būti grindžiamas įmonių, kaip duomenų valdytojų bei jų pasitelktų duomenų tvarkytojų, skaidrumu ir atskaitomybe, todėl, siekiant įrodyti BDAR laikymąsi, įtvirtinamos naujos pareigos įmonėms, atsižvelgiant į jų atliekamą asmens duomenų tvarkymą:

- Paskirti **duomenų apsaugos pareigūną** (žr. skyrių „Ar privalau paskirti duomenų apsaugos pareigūną?“, 34 p.);

- Tvarkyti **duomenų tvarkymo veiklos įrašus**, kuriuose būtų detaliai aprašytas atliekamas asmens duomenų tvarkymas (žr. VDAI „Rekomendaciją dėl duomenų tvarkymo veiklos įrašų“: https://www.ada.lt/go.php/lit/Rekomendacija-del-duomenu-tvarkymo-veiklos-irau-2018-m);

- Prieš pradedant tvarkyti duomenis, atlikti numatytų duomenų tvarkymo operacijų **poveikio asmens duomenų apsaugai vertinimą** (žr. skyrių „Ar privalau atlikti poveikio duomenų apsaugai vertinimą?“, 38 p.) (aktualu tais atvejais, kai numatoma tvarkyti jautrius duomenis ar atlikti profiliavimą) ir kreiptis dėl išankstinės konsultacijos, kai, atlikus poveikio duomenų apsaugai vertinimą, nustatoma, kad tvarkant duomenis kiltų didelis pavojus, jei įmonė nesiimtų priemonių pavojui sumažinti;

- Pranešti VDAI ir asmeniui apie **asmens duomenų saugumo pažeidimą** (žr. VDAI parengtą „Rekomendaciją dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos“: https://www.ada.lt/go.php/lit/Rekomendacija-del-asmens-duomenu-saugumo-pazeidimu-nustatymo-tyrimo-praneimo-apie-juos-ir-dokumentavimo-tvarkos-2018-m).

BDAR taip pat skatina parengti **elgesio kodeksus** (žr. skyrių „Kas yra elgesio kodeksai?“, 43 p.), kuriais būtų siekiama padėti tinkamai taikyti BDAR, atsižvelgiant į konkrečius įvairių su duomenų tvarkymu susijusių sektorių ypatumus ir į konkrečius labai mažų, mažųjų ir vidutinių įmonių poreikius.

AR PRIVALAU PASKIRTI DUOMENŲ APSAUGOS PAREIGŪNĄ?

BDAR 37–39 straipsniai reglamentuoja DAP statusą, užduotis bei skyrimo sąlygas.

Kada turi būti skiriamas duomenų apsaugos pareigūnas?

DAP *privalo* būti paskirtas, 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. Įmonės **pagrindinė veikla** yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina **reguliariai** ir **sistemingai dideliu mastu stebėti** duomenų subjektus (tai reiškia, kad duomenų tvarkymas yra būtinas siekiant vykdyti pagrindines funkcijas bei duomenų tvarkymas atliekamas tam tikrais intervalais, nuolat tebevykstantis, pasikartojantis tam tikrai periodais, yra organizuotas, planuotas, metodiškas ar pan.).

3. Įmonės pagrindinė veikla yra **specialių kategorijų duomenų** tvarkymas **dideliu mastu**. Pagal BDAR 9 straipsnio 1 dalį 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.

4. Įmonės pagrindinė veikla yra asmens duomenų apie **apkaltinamuosius nuosprendžius ir nusikalstamas veikas** tvarkymas **dideliu mastu** (pagal BDAR 10 straipsnį).

Tikslaus tvarkomų duomenų kiekio ar atitinkamų asmenų skaičiaus, kuriems esant būtų laikytina, kad asmens duomenų tvarkymas atliekamas dideliu mastu, nėra. Vertinant ar asmens duomenys yra tvarkomi *dideliu mastu*, rekomenduotina atsižvelgti į šiuos veiksnius:

- Susijusių duomenų subjektų skaičių – 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).

Pavyzdys, kai „asmens duomenų tvarkymas – pagrindinė veikla“

Privačios sveikatos priežiūros įstaigos pagrindinė veikla – teikti sveikatos priežiūros paslaugas viso miesto ar 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 sveikatos priežiūros įstaigos veikla. Vertinant tai, kad sveikatos paslaugos teikiamos viso miesto ar rajono mastu, manytina, kad asmens duomenų tvarkymas vykdomas dideliu mastu. Pažymėtina, kad kiekvieno paciento atžvilgiu pagal teisės aktus yra pildoma asmens sveikatos istorija, o tai vertintina kaip reguliarus ir sistemingas asmens stebėjimas. Taigi, aptariamu atveju sveikatos priežiūros įstaiga turi paskirti duomenų apsaugos pareigūną.

Privati apsaugos paslaugų įmonė vykdo tam tikrų privačių 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 taip pat turi paskirti DAP.

Visos įmonės vykdo tam tikrą veiklą, pvz., moka darbo užmokestį savo darbuotojams arba vykdo standartinę IT sistemų priežiūros veiklą. Tai yra pagrindinei įmonės veiklai arba pagrindiniam verslui reikalingų pagalbinių funkcijų pavyzdžiai. Nors ši veikla yra reikalinga arba būtina, ji paprastai laikoma pagalbinėmis funkcijomis, o ne pagrindine veikla, todėl šiuo atveju DAP neturi būti skiriamas.

Pavyzdys, kai „asmens duomenys tvarkomi didelis mastu“

Asmuo, užsiimantis individualia veikla, internete prekiauja savo užauginta produkcija viename mieste ir naudojasi IT 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 didelio masto ir tokia įmonė turės pareigą paskirti DAP.

Įmonė, teikianti odontologines paslaugas, įsikūrusi Pasvalio mieste. Jos klientai (pacientai) yra tik šio miesto gyventojai. Įmonėje dirba 5 (penki) darbuotojai – odontologai. Vertinant duomenų subjektų skaičių, geografinę duomenų tvarkymo veiklos aprėptį ir pan. aspektus, toks pacientų asmens duomenų tvarkymas gali nebūti laikomas dideliu mastu ir tokia įmonė neturės pareigos paskirti DAP.

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

Bendrovė lojalumo programos vykdymo tikslu tvarko klientų asmens duomenis, įskaitant ir jų pirkimo istorijos duomenis. Fiziniai asmenys gali būti nustatyti pagal jų pirkimo įpročius, gali būti taikomi asmens duomenų tvarkymo metodai, kuriais jiems suteikiamas profilis, ypač siekiant priimti su jais susijusius sprendimus arba išanalizuoti ar prognozuoti jų asmeninius pomėgius, elgesį, įpročius ir pan. Taigi, šiuo atveju laikytina, kad vykdoma duomenų subjekto elgesio stebėsena ir DAP paskirti yra būtina.

DAP paskyrimo kriterijai yra taikomi *tiek duomenų valdytojams, tiek duomenų tvarkytojams*. Atsižvelgiant į tai, kas atitinka privalomo paskyrimo kriterijus, kai kuriais atvejais DAP paskirti privalo tik duomenų valdytojas arba tik duomenų tvarkytojas, o kitais atvejais – ir duomenų valdytojas, ir duomenų tvarkytojas.

Net kai pagal BDAR nereikalaujama paskirti DAP, įmonei kartais gali būti naudinga jį paskirti savanoriškai.

Be to, niekas neužkerta kelio įmonei, kuri teisiškai neprivalo paskirti DAP ir nepageidauja jo paskirti savanoriškai, vis tiek įdarbinti darbuotojų arba samdyti išorės konsultantų, kuriems būtų pavestos su asmens duomenų apsauga susijusios užduotys. Šiuo atveju svarbu užtikrinti, kad nekiltų nesusipratimų dėl jų pareigybės pavadinimo, statuso, pareigų ir užduočių. Todėl visuose įmonės vidaus pranešimuose ir bendraujant su valstybinėmis institucijomis, duomenų subjektais ir (ar) plačiąja visuomene reikėtų aiškiai nurodyti, kad šis asmuo ar konsultantas nėra DAP.

Kas gali būti duomenų apsaugos pareigūnas?

DAP gali būti:

- **Duomenų valdytojo (duomenų tvarkytojo) darbuotojas**. Šiuo atveju privalo būti užtikrinama, kad DAP vykdant jo užduotis ir pareigas dėl jų vykdymo *nekiltų interesų konfliktas*, t. y. DAP negali įmonėje eiti pareigų, pagal kurias jis turėtų nustatyti asmens duomenų tvarkymo tikslus ir priemones. Dėl kiekvienos įmonės specifinės struktūros į tai turi būti atsižvelgiama kiekvienu konkrečiu atveju. Kaip interesų konfliktą galinčios sukelti pareigybės yra tokios vadovybės pareigybės, kaip, pvz., įmonės

vadovas, generalinis direktorius, operacijų vadovas, vyriausiasis finansininkas, rinkodaros padalinio vadovas, žmogiškųjų išteklių arba IT padalinio vadovas.

- **Išorinis paslaugų teikėjas** (t. y. atlikti DAP užduotis pagal paslaugų teikimo sutartį, sudarytą su asmeniu ar įmone, pvz., kitu juridiniu asmeniu ar pan.). Šiuo atveju taip pat privalo būti užtikrinama, kad DAP vykdant jo užduotis ir pareigas dėl jų vykdymo 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, svarbu, kad kiekvienas jo narys vykdytų visus taikytinus BDAR reikalavimus, todėl rekomenduotina paslaugų sutartimi aiškiai paskirstyti užduotis išorinio DAP grupės nariams ir vieną asmenį paskirti už klientą atsakingu vadovaujančiu kontaktiniu asmeniu.

Skiriant asmenį DAP, rekomenduotina atsižvelgti į jo profesines savybes, gebėjimą atlikti savo užduotis, duomenų apsaugos teisės ir praktikos ekspertinių žinių turėjimą (pvz., atliekamų duomenų tvarkymo operacijų supratimą, informacinių technologijų ir duomenų saugumo išmanymą ir t. t.).

Duomenų apsaugos pareigūno užduotys

- Stebėti, kaip duomenų valdytojas (duomenų tvarkytojas) laikosi BDAR nuostatų ir informuoti jį bei duomenis tvarkančius darbuotojus apie jų prievoles asmens duomenų apsaugos srityje, konsultuoti juos šiais klausimais *(pvz., nagrinėti ir tikrinti ar duomenų tvarkymo veikla atitinka reikalavimus, teikti rekomendacijas ir t. t.)*;
- Bendradarbiauti su priežiūros institucija ir atlikti kontaktinio asmens funkciją priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais, įskaitant BDAR 36 straipsnyje nurodytas išankstines konsultacijas, ir prireikus konsultuoti visais kitais klausimais;
- Teikti konsultacijas dėl poveikio duomenų apsaugai vertinimo ir stebėti jo atlikimą *(pvz., konsultuoti 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.)*;
- Vertinti su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus;
- Atlikti kitas duomenų valdytojo (duomenų tvarkytojo) pavestas funkcijas, susijusias su asmens duomenų tvarkymu *(pvz., tvarkyti 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.

Kokia duomenų apsaugos pareigūno informacija ir kur turi būti skelbiama?

Duomenų valdytojas (duomenų tvarkytojas) privalo **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 gali būti teikiamas *raštu* (tiesiogiai atvykus į VDAI, atsiųsti paštu ar per pasiuntinį) ar e*lektroniniu būdu* (el. pašto adresu ada@ada.lt (prisegant pasirašytą raštą) arba naudojantis VDAI elektronine paslaugų sistema *https://www.ada.lt/go.php/lit/Pranesimas-apie-duomenu-apsaugos-pareiguna-bdar/4/1*.

Daugiau informacijos, susijusios su DAP paskyrimu, statusu ir jo vykdomomis užduotimis galite rasti Direktyvos 95/46/EB 29 straipsnio darbo grupės 2016 m. gruodžio 13 d. priimtose Duomenų apsaugos pareigūnų gairėse (WP 243) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

AR PRIVALAU ATLIKTI POVEIKIO DUOMENŲ APSAUGAI VERTINIMĄ?

BDAR 35 straipsnis numato pareigą duomenų valdytojui prieš pradedant tvarkyti duomenis atlikti poveikio duomenų apsaugai vertinimą, siekiant įvertinti didelio pavojaus konkrečią tikimybę ir rimtumą, atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus bei pavojaus šaltinius.

Kas yra poveikio duomenų apsaugai vertinimas?

Poveikio duomenų apsaugai vertinimas yra būdas sistemingai ir visapusiškai išanalizuoti Jūsų įmonės vykdomą asmens duomenų tvarkymą bei padėti nustatyti ir sumažinti duomenų apsaugos grėsmes.

Poveikio duomenų apsaugai tikslas – ne visiškai panaikinti grėsmes, bet padėti jas sumažinti bei įvertinti, ar likusios grėsmės yra pagrįstos ir pateisinamos.

Atliekant poveikio duomenų apsaugai vertinimą reikia 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 žalos tikimybę. Būtina vertinti 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 asmeniui sunkumą.

Svarbu įtraukti poveikio duomenų apsaugai vertinimą į Jūsų įmonės vidinius procesus, kad priklausomai nuo vertinimo rezultato būtų galima koreguoti planus. Poveikio duomenų apsaugai vertinimas yra ne vienkartinis veiksmas, o besitęsiantis procesas, nes duomenų tvarkymas turi būti nuolatos peržiūrimas.

Kada privalo būti atliktas poveikio duomenų apsaugai vertinimas?

Poveikio duomenų apsaugai vertinimas **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, būtina išanalizuoti aplinkybes, kurios gali sąlygoti didelį pavojų ar poveikį fiziniams asmenims.

Poveikio duomenų apsaugai vertinimas gali būti atliekamas dėl vienos arba dėl kelių panašių duomenų tvarkymo operacijų. Keli duomenų valdytojai gali atlikti vieną poveikio duomenų apsaugai vertinimą.

Kas yra „didelis pavojus fizinių asmenų teisėms bei laisvėms“?

Sąvoka „fizinių asmenų teisės bei laisvės“ visų pirma yra susijusi su teisėmis į duomenų apsaugą ir privatumą, tačiau taip pat gali apimti kitas pagrindines teises, pvz., žodžio laisvę, minties laisvę, judėjimo laisvę, diskriminacijos draudimą, teisę į laisvę, sąžinės ir tikėjimo laisvę. Pavojus – tai scenarijus, kuriame aprašomas įvykis ir jo padariniai, įvertinti atsižvelgiant į jų rimtumą ir tikimybę. Taigi, **pavojumi fizinių asmenų teisėms bei laisvėms laikytina**, kai dėl duomenų tvarkymo arba dėl galimo duomenų saugumo pažeidimo duomenų subjektams gali būti sunkiau naudotis savo teisėmis ir laisvėmis, duomenų subjektas gali patirti atskirtį arba diskriminaciją, finansinius nuostolius, gali būti pakenkta jo reputacijai arba atsirasti kitokie rimti padariniai kasdieniam fizinio asmens gyvenimui.

Pavyzdžiai

Informacijos apie tai, kad asmuo serga tam tikromis ligomis, atskleidimas gali lemti asmens galimybę įsidarbinti ar gauti paaukštinimą.

Buvimo vietos informacijos rinkimas gali būti susijęs su judėjimo laisvės apribojimu.

Tam tikri atvejai, kai gali kilti „didelis pavojus fizinių asmenų teisėms bei laisvėms“ ir kada, visų pirma, privalo būti atliktas poveikio duomenų apsaugai vertinimas yra numatyti BDAR. Taip pat VDAI viešai paskelbs duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašą (šio sąrašo projektas pateiktas derinti EDAV):

Remiantis BDAR, poveikio duomenų apsaugai vertinimas turi būti atliekamas šiais atvejais:

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.

Ką reiškia „asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą“?

Asmeninių aspektų vertinimas vykdomas, visų pirma, remiantis aspektais, susijusiais su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu.

Profiliavimas reiškia informacijos apie asmenį (ar grupę asmenų) 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.

Pavyzdžiai

Biotechnologijų bendrovė tiesiogiai vartotojams siūlo atlikti genetinius tyrimus, siekiant įvertinti ir prognozuoti su liga susijusį ir (arba) sveikatai gresiantį pavojų.

Bendrovė, remdamasi jos svetainės naudojimu arba naršymu joje, kuria elgesio arba rinkodaros profilius.

Ką reiškia „automatizuotas sprendimų priėmimas“?

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.

Ką reiškia „sprendimai, kuriais padaromas su fiziniu asmeniu susijęs teisinis poveikis arba kurie daro panašų didelį poveikį fiziniam 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. BDAR 9 straipsnio 1 dalyje nurodytų specialių kategorijų duomenų arba 10 straipsnyje nurodytų asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu.

Kas yra specialių kategorijų asmens duomenys?

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.

Kas yra duomenų 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 skaičių – 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.

Kas yra duomenų tvarkymas dideliu mastu, nurodyta pirmiau.

Ką reiškia „sistemingas stebėjimas“?

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

Ką reiškia „vieša vieta“?

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

Kas yra „stebėjimas“?

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

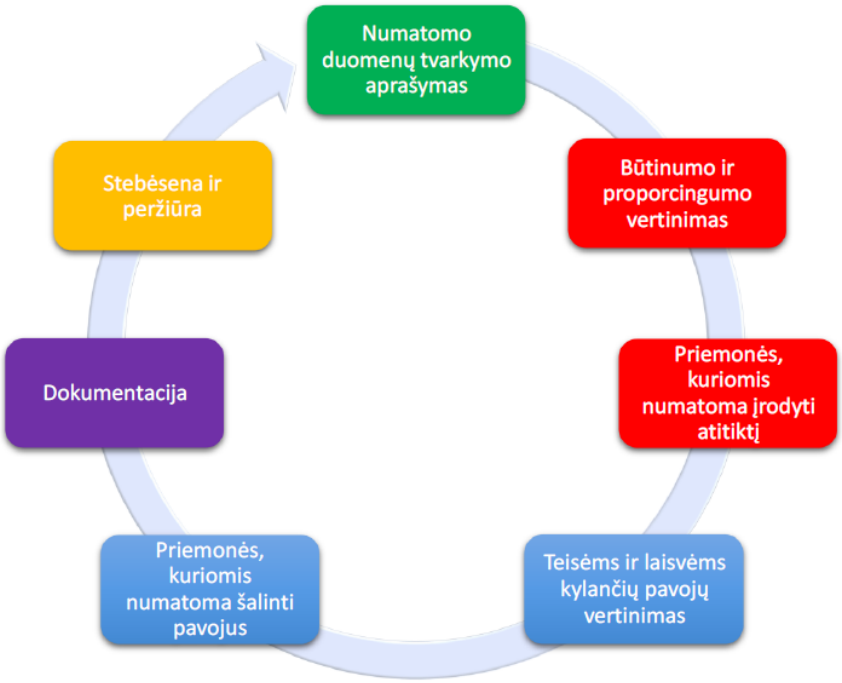
Kaip atliekamas poveikio duomenų apsaugai vertinimas?

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;
  - kuriomis įrodoma, kad laikomasi šio reglamento.

Pavyzdinė poveikio duomenų apsaugai atlikimo forma:
https://www.ada.lt/go.php/lit/Pavyzdine-poveikio-duomenu-apsaugai-atlikimo-forma-2018-m

Šiame paveiksle pavaizduotas bendro pobūdžio pasikartojantis poveikio duomenų apsaugai vertinimo atlikimo procesas:



Kriterijai, kuriais remdamiesi duomenų valdytojai gali įvertinti, ar poveikio duomenų apsaugai vertinimas arba šio vertinimo atlikimo metodika yra pakankamai išsami, kad atitiktų BDAR:

 Pateiktas sisteminis duomenų tvarkymo operacijų aprašymas (35 straipsnio 7 dalies a punktas):
 Atsižvelgiama į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus (90 konstatuojamoji dalis);
 Registruojami asmens duomenys, gavėjai ir asmens duomenų saugojimo laikotarpis;
 Pateikiamas funkcinis duomenų tvarkymo operacijos aprašymas;
 Nustatomas turtas, kuris naudojamas tvarkant asmens duomenis (aparatinė įranga, programinė įranga, tinklai, žmonės, spausdinti dokumentai arba spausdintų dokumentų siuntimo kanalai);
 Atsižvelgiama į atitiktį patvirtintiems elgesio kodeksams (35 straipsnio 8 dalis).

 Įvertinamas būtinumas ir proporcingumas (35 straipsnio 7 dalies b punktas):
 Nustatomos priemonės, kuriomis numatoma užtikrinti atitiktį reglamentui (35 straipsnio 7 dalies d punktas ir 90 konstatuojamoji dalis), atsižvelgiant į:
 priemones, kuriomis prisidedama prie duomenų tvarkymo proporcingumo ir būtinumo remiantis:
 konkrečiu (-iais), aiškiu (-iais) ir teisėtu (-ais) tikslu (-ais) (5 straipsnio 1 dalies b punktas);
 tvarkymo teisėtumu (6 straipsnis);
 adekvačiais, tinkamais ir tik tokiais, kurių reikia siekiant tikslų, duomenimis (5 straipsnio 1 dalies c punktas);
 ribota saugojimo trukme (5 straipsnio 1 dalies e punktas);
 priemones, padedančias užtikrinti duomenų subjektų teises:
 duomenų subjektui teikiama informacija (12, 13 ir 14 straipsniai);
 teisė susipažinti su duomenimis ir teisė į duomenų perkeliamumą (15 ir 20 straipsniai);

 teisė ištaisyti ir ištrinti duomenis (16, 17 ir 19 straipsniai);
 teisė prieštarauti duomenų tvarkymui ir teisė apriboti duomenų tvarkymą (18, 19 ir 21 straipsniai);
 santykiai su duomenų tvarkytojais (28 straipsnis);
 su tarptautiniu (-iais) perdavimu (-ais) susijusios apsaugos priemonės (V skyrius);
 išankstinės konsultacijos (36 straipsnis).

 Valdomi duomenų subjektų teisėms ir laisvėms kylantys pavojai (35 straipsnio 7 dalies c punktas):

 Įvertinama pavojų kilmė, pobūdis, specifika ir rimtumas (plg. 84 konstatuojamąją dalį) arba, konkrečiau tariant, įvertinamas kiekvienas pavojus (neteisėta prieiga prie duomenų, nepageidaujamas duomenų pakeitimas ir duomenų pradanginimas) iš duomenų subjektų perspektyvos:
 atsižvelgiama į pavojų šaltinius (90 konstatuojamoji dalis);
 nustatomas galimas poveikis duomenų subjektų teisėms ir laisvėms tam tikrais atvejais, kai, pvz., prieiga prie duomenų yra neteisėta, duomenys nepageidaujamai pakeičiami arba pradanginami;
 nustatomos grėsmės, dėl kurių gali būti gaunama neteisėta prieiga prie duomenų, jie gali būti nepageidaujamai pakeičiami arba pradanginami;
 įvertinama tikimybė ir rimtumas (90 konstatuojamoji dalis);
 nustatomos priemonės, kuriomis planuojama šalinti šiuos pavojus (35 straipsnio 7 dalies d punktas ir 90 konstatuojamoji dalis);
 dalyvauja suinteresuotosios šalys:
 siekiama konsultuotis su duomenų apsaugos pareigūnu (35 straipsnio 2 dalis);
 kai tinkama, siekiama išsiaiškinti duomenų subjektų arba jų atstovų nuomones (35 straipsnio 9 dalis).

Daugiau informacijos apie poveikio duomenų apsaugai vertinimą galima rasti Direktyvos 95/46/EB 29 straipsnio darbo grupės parengtose gairėse, adresu http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

Ar atliekant poveikio duomenų apsaugai vertinimą reikia kreiptis į Valstybinę duomenų apsaugos inspekciją?

Jeigu atlikus poveikio duomenų apsaugai vertinimą nustatyta, kad tvarkant duomenis **gali kilti didelis pavojus, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti**, įmonė prieš pradėdama tvarkyti duomenis, turi kreiptis į VDAI **dėl išankstinės konsultacijos**.

Išankstinių konsultacijų teikimo tvarką reglamentuoja BDAR 36 straipsnis.

Įmonė, kreipdamasi dėl išankstinės konsultacijos, VDAI turi nurodyti:

- numatyto duomenų tvarkymo tikslus ir priemones;
- nustatytas priemones bei apsaugos priemones duomenų subjektų teisėms ir laisvėms apsaugoti;
- atliktą poveikio duomenų apsaugai vertinimą;
- duomenų apsaugos pareigūno kontaktinius duomenis (kai taikoma);
- 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.

KAS YRA ELGESIO KODEKSAI?

BDAR 40 straipsnis reglamentuoja elgesio kodeksų parengimo sąlygas ir stebėseną.

BDAR rekomenduoja parengti elgesio kodeksus, kurie palengvintų veiksmingą šio reglamento taikymą, atsižvelgiant į tam tikruose sektoriuose atliekamo duomenų tvarkymo ypatumus ir konkrečius labai mažų, mažųjų ir vidutinių įmonių poreikius. Tokiuose elgesio kodeksuose visų pirma galėtų būti nustatomos duomenų valdytojų ir duomenų tvarkytojų prievolės, atsižvelgiant į pavojų, kuris, tvarkant duomenis, gali kilti fizinių asmenų teisėms ir laisvėms.

Kas rengia elgesio kodeksą?

Asociacijos ir kitos įstaigos, atstovaujančios įvairių kategorijų duomenų valdytojams arba duomenų tvarkytojams gali rengti naują elgesio kodeksą arba gali keisti ar išplėsti esamus elgesio kodeksus, kad jie atitiktų BDAR reikalavimus.

Rengiant elgesio kodeksą (iš dalies jį keičiant ar išplečiant), turėtų būti konsultuojamasi su atitinkamais suinteresuotaisiais subjektais, jei įmanoma – su duomenų subjektais, ir atsižvelgiama į tokių konsultacijų metu gautus atsakymus ir pareikštas nuomones.

Kokia informacija gali būti elgesio kodekse?

Elgesio kodeksai turėtų padėti įmonei laikytis BDAR reikalavimų ir gali apimti tokias sritis, kaip:

- Sąžiningas ir skaidrus duomenų tvarkymas;
- Teisėti interesai, kuriais konkrečiomis aplinkybėmis vadovaujasi duomenų valdytojai;
- Asmens duomenų rinkimas;
- Pseudonimų suteikimas asmens duomenims;
- Visuomenės ir duomenų subjektų informavimas;
- Naudojimasis duomenų subjektų teisėmis;
- Vaikų informavimas ir apsauga (įskaitant tėvų sutikimo gavimo mechanizmus);
- BDAR 24 ir 25 straipsniuose nurodytos priemonės bei procedūros ir priemonės, kuriomis užtikrinamas BDAR 32 straipsnyje nurodytas duomenų tvarkymo saugumas;
- Pranešimas apie asmens duomenų saugumo pažeidimus VDAI ir duomenų subjektui;
- Asmens duomenų perdavimas už ES ribų;
- Neteisminis ginčų nagrinėjimas ir kitų ginčų sprendimo procedūros, pagal kurias sprendžiami su duomenų tvarkymu susiję duomenų valdytojų ir duomenų subjektų ginčai, nedarant poveikio duomenų subjektų teisėms pagal BDAR 77 ir 79 straipsnius.

Elgesio kodeksai gali padėti bendrai spręsti klausimus, susijusius su specifiniais labai mažų, mažųjų ir vidutinių įmonių poreikiais, ir padėti jiems dirbti kartu, kad būtų taikomi BDAR reikalavimai, atsižvelgiant į konkrečius jų sektoriui būdingus asmens duomenų tvarkymo niuansus (pvz., asmens duomenų tvarkymas, teikiant odontologines paslaugas pavieniuose ar nedideliuose odontologų kabinetuose).

Kas tvirtina elgesio kodeksą?

Parengto elgesio kodekso projektas turi būti pateikiamas VDAI, kuri pateikia nuomonę, ar kodekso projektas, pakeitimas ar išplėtimas atitinka BDAR, bei patvirtina tokį kodekso projektą, jei nustato, kad jame numatytos tinkamos apsaugos priemonės.

Jeigu elgesio kodekso projektas ar pakeitimas arba išplėtimas yra patvirtinamas, ir jis nėra susijęs su keliose valstybėse narėse vykdoma duomenų tvarkymo veikla, VDAI užregistruoja ir paskelbia kodeksą.

Jeigu elgesio kodekso projektas yra susijęs su keliose valstybėse narėse vykdoma duomenų tvarkymo veikla, VDAI šį projektą pateikia EDAV, kuri savo nuomonę dėl elgesio kodo pateikia Europos Komisijai. Komisija gali nuspręsti, kad elgesio kodeksas galioja visose ES šalyse. Tokiu atveju ji užtikrina, kad patvirtinti elgesio kodeksai būtų tinkamai skelbiami viešai.

EDAV įtraukia į registrą visus patvirtintus elgesio kodeksus, pakeitimus ir išplėtimus bei padaro juos viešai prieinamus.

Kas turi laikytis elgesio kodekso?

Įsipareigojimas laikytis elgesio kodekso yra savanoriškas, tačiau, jei yra patvirtintas elgesio kodeksas, atitinkantis įmonės atliekamą asmens duomenų tvarkymą, vertėtų apsvarstyti galimybę prisiimti įsipareigojimą jo laikytis, ir taip parodyti, kad tvarkant asmens duomenis yra laikomasi BDAR nuostatų. BDAR aiškiai pripažįstami ir skatinami elgesio kodeksai, nes jie papildo ir (ar) patikslina teisės aktus, reglamentuojančius asmens duomenų tvarkymą. Taip kuriamos gairės ir suteikiama aiškumo paslaugų teikėjams ir gavėjams.

VDAI patvirtintų ir visuotinai galiojančių elgesio kodeksų gali laikytis ne tik duomenų valdytojai arba duomenų tvarkytojai, kuriems taikomas BDAR, bet ir duomenų valdytojai (duomenų tvarkytojai), kuriems šis reglamentas netaikomas, kad užtikrintų asmens duomenų perdavimo į trečiąsias valstybes arba tarptautinėms organizacijoms tinkamas apsaugos priemones. Tokie duomenų valdytojai arba duomenų tvarkytojai gali prisiimti privalomus ir vykdytinus įsipareigojimus taikyti šias tinkamas apsaugos priemones, ypač duomenų subjektų teisių atžvilgiu naudodamiesi sutartinėmis arba kitomis teisiškai privalomomis priemonėmis.

Pavyzdys

Draudimo bendrovėms atstovaujanti asociacija parengė elgesio kodeksą, kurį patvirtino VDAI. Šio kodekso laikosi įvairios konkuruojančios draudimo įmonės. Nors jos tą daro savanoriškai, šio kodekso laikymasis padeda įrodyti, kad jos, tvarkydamos asmens duomenis, laikosi BDAR.

Kas prižiūri elgesio kodekso laikymąsi?

Nedarant poveikio VDAI užduotims ir įgaliojimams, elgesio kodekso laikymosi stebėseną gali atlikti įstaiga, turinti tinkamo lygio ekspertinių žinių kodekso dalyko srityje ir tuo tikslu akredituota atitinkamos kompetentingos priežiūros institucijos. Tai netaikoma valdžios institucijų ir įstaigų atliekamam duomenų tvarkymui.

Elgesio kodekse turi būti numatomi mechanizmai, leidžiantys minėtai atliekančiai įstaigai vykdyti privalomą duomenų valdytojų ar duomenų tvarkytojų (kurie įsipareigojo taikyti kodeksą) šio kodekso nuostatų laikymosi stebėseną.

Elgesio kodekso laikymosi stebėseną atliekanti įstaiga gali imtis atitinkamų veiksmų, kai duomenų valdytojas arba duomenų tvarkytojas pažeidžia elgesio kodeksą (pvz., sustabdyti atitinkamo duomenų valdytojo arba duomenų tvarkytojo teisę užsiimti su kodeksu susijusia veikla ar nušalinti jį nuo su kodeksu susijusių pareigų). Apie tokius veiksmus ir jų vykdymo priežastis ji informuoja VDAI.

Kodėl elgesio kodeksai yra svarbūs ir kokia yra jų praktinė reikšmė?

- Įsipareigojimas laikytis elgesio kodekso parodo ne tik tai, kad įmonė asmens duomenis tvarko laikydamasi BDAR nuostatų, tačiau tai yra ir „ženklas“ visiems suinteresuotiems subjektams, kad įmonė supranta, ką ji turi daryti, kad asmens duomenų tvarkymas būtų teisėtas, kad nebūtų pažeistos duomenų subjektų teisės, laisvės ir pan.
- Tuo, kad laikomasi patvirtinto elgesio kodekso, gali būti remiamasi kaip vienu iš elementų, kuriuo siekiama įrodyti, kad duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones (siekiant užtikrinti pavojų atitinkančio lygio saugumą), atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas ir duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms.
- Kai įmonė prisiima įsipareigojimą laikytis elgesio kodekso, jos atliekamo asmens duomenų tvarkymo atitiktis elgesio kodeksui bus reguliariai stebima. Ši stebėsena užtikrina, kad asmens duomenys tvarkomi teisėtai ir tinkamai. Jeigu atliekamas asmens duomenų tvarkymas nebeatitiks elgesio kodekso reikalavimų, į tai bus iškart reaguojama (pvz., bus sustabdoma teisė užsiimti su kodeksu susijusia veikla ar kt.).
- Elgesio kodeksai yra viešai skelbiami, todėl tiek duomenų subjektai, tiek kiti suinteresuoti asmenys, gali susipažinti su elgesio kodekse reglamentuojamo asmens duomenų tvarkymo nuostatomis.
- BDAR įpareigoja duomenų valdytoją pasitelkti tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga. Duomenų tvarkytojo įsipareigojimas laikytis elgesio kodekso patvirtina, kad duomenų tvarkytojo veikla bei atliekami asmens duomenų tvarkymo veiksmai atitinka BDAR reikalavimus. Tokiu būdu duomenų valdytojams yra palengvinama našta pasirinkti tinkamą duomenų tvarkytoją, o duomenų tvarkytojams – įrodyti, kad jie yra atsakingi ir laikosi visų jiems keliamų reikalavimų bei yra pranašesni už kitus, tas pačias paslaugas siūlančius duomenų tvarkytojus.
- Įsipareigojimas laikytis elgesio kodekso gali parodyti, kad duomenų valdytojas (duomenų tvarkytojas) yra įsidiegęs tinkamas duomenų saugumo priemones asmens duomenims teikti į šalis, esančias už ES ribų. BDAR numatyta, kad duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai (jeigu nėra priimtas sprendimas pagal šio reglamento 45 straipsnio 3 dalį) tik tuo atveju, jeigu jis yra nustatęs tinkamas apsaugos priemones, su sąlyga, kad suteikiama galimybė naudotis vykdytinomis duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis. Šios priemonės nereikalaujant specialaus VDAI leidimo gali būti nustatomos patvirtintu elgesio kodeksu kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo trečiojoje valstybėje įsipareigojimais taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis.
- Įsipareigojimas laikytis elgesio kodekso gali padėti sumažinti administracinės baudos riziką. Taip yra todėl, kad sprendžiant dėl to, ar skirti administracinę baudą, ir sprendžiant dėl administracinės baudos dydžio kiekvienu konkrečiu atveju, turi būti atsižvelgiama ir į tai, ar duomenų valdytojas (duomenų tvarkytojas) laikosi patvirtintų elgesio kodeksų.