SIEKIO ID

Informacinė valanda NVO

DUOMENŲ APSAUGA

Ona Valainienė
Teisininkė, sertifikuota duomenų apsaugos pareigūnė

Iceland Liechtenstein Norway
Active citizens fund

PRIMINIMUI IR APTARIMUI

1. Asmens duomenų samprata
2. Asmens duomenų tvarkymas
    - 2.1. Tikslai ir pagrindai
        - 2.1.1. Asmens sutikimas kaip duomenų tvarkymo pagrindas.
        - 2.1.2. Teisėtas interesas kaip duomenų tvarkymo pagrindas. Interesų balanso testas
    - 2.2. Asmens duomenų tvarkymo principai
3. Asmens duomenų apsaugos reikalavimai
4. Duomenų valdytojo ir tvarkytojo statusai
5. Duomenų tvarkymo veiklos įrašai ir atsakingų asmenų paskyrimas
6. Organizacijos vidiniai dokumentai
7. Organizacijos privatumo pranešimas
8. Poveikio duomenų apsaugai vertinimas
9. Asmens duomenų saugumo pažeidimas

SIEKIO ID

ASMENS DUOMENYS

Asmens duomenys – bet kokia informacija susijusi su gyvu žmogumi, kurio tapatybė mums jau žinoma, arba, kurio tapatybę galime tiesiogiai ar netiesiogiai nustatyti pagal tą informaciją.

„Nustatyti tiesiogiai“ – pvz., pagal vardą ir pavardę, asmens kodą ir pan.

„Nustatyti netiesiogiai“ – pvz., automobilio valstybinis numeris, vaizdo duomenys, telefono numeris, t. y. kai turimų duomenų nepakanka konkrečiam asmeniui nustatyti, tačiau **asmens tapatybę galima nustatyti panaudojant kitus duomenis, nepriklausomai ar juos turi** ta pati įmonė (organizacija).

ASMENS DUOMENŲ PAVYZDŽIAI (NEBAIGTINIS SĄRAŠAS):

- vardas, pavardė, asmens kodas, gimimo data;
- telefono numeris (taip pat ir atsitiktinai sugeneruotas), el. paštas (taip pat ir darbinis vardas.pavarde@darbas.lt), gyvenamasis adresas;
- pilietybė, socialinio draudimo numeris, banko kortelės Nr., sąskaita;
- išsilavinimo informacija, darbovietė, pajamos, duomenys apie turimą turtą;
- duomenys apie sveikatą;
- vaizdo duomenys (nuotraukose, filmuotoje medžiagoje);
- buvimo vietos duomenys (pvz., mobiliajame telefone);
- biometriniai duomenys;
- asmens pomėgiai, šeimyninė padėtis, vaikų (ne)turėjimas;
- naršymo internete istorija, interneto protokolo (IP) adresas ir t. t.

SIEKIO ID

JAUTRŪS (YPATINGI) ASMENS DUOMENYS

Duomenys, kurių tvarkymo pagrindimui taikomos griežtesnės arba papildomos sąlygos:

SPECIALIŲ KATEGORIJŲ ASMENS DUOMENYS

- Rasinė, etninė kilmė;
- Politiniai, religiniai, filosofiniai įsitikinimai
- Narystė profsąjungoje;
- Genetiniai, biometriniai duomenys, tvarkomi siekiant nustatyti asmens tapatybę;
- Sveikata, lytinis gyvenimas.

DUOMENYS SUSIJĘ SU NUSIKALSTMA VEIKA

SIEKIO ID

ASMENS DUOMENŲ TVARKYMAS

Asmens duomenų tvarkymas – bet kokia automatizuotomis (skaitmenine forma) arba neautomatizuotomis priemonėmis (susistemintame rinkinyje popierine forma) **su asmens duomenimis** ar asmens duomenų rinkiniais **atliekama operacija** ar operacijų seka.

- Rinkimas
- Įrašymas
- Rūšiavimas
- Sisteminimas
- Saugojimas
- Adaptavimas ar keitimas
- Išgavimas
- Susipažinimas
- Naudojimas
- Atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis
- Sugretinimas ar sujungimas su kitais duomenimis
- Apribojimas
- Ištrynimas arba sunaikinimas.

SIEKIO ID

ASMENS DUOMENŲ TVARKYMAS

Asmens duomenų tvarkymui, kurį atlieka fizinis asmuo, įmonė ar organizacija yra taikomas **Bendrasis duomenų apsaugos reglamentas** (BDAR). Pradėtas taikyti 2018 m. gegužės 25 d.

BDAR NETAIKOMAS:

- mirusių asmenų asmens duomenų tvarkymui;
- juridinių asmenų duomenų (pvz., pavadinimas, teisinė forma, kontaktiniai duomenys) tvarkymui [! vykdant tiesioginę rinkodarą taikomas Elektroninių ryšių įstatymas];
- anoniminės informacijos tvarkymui;
- duomenims, kuriuos asmuo tvarko tik asmeniniais tikslais arba savo namuose vykdomos veiklos tikslais, su sąlyga, kad nėra jokio ryšio su profesine ar komercine veikla.

BDAR taikymas priklauso ne nuo organizacijos dydžio, bet nuo atliekamo asmens duomenų tvarkymo pobūdžio. Kita vertus, ne visos BDAR prievolės taikomos mažoms ir vidutinėms įmonėms, pvz., jei dirba mažiau kaip 250 darbuotojų, nereikia tvarkyti duomenų tvarkymo veiklos įrašų.

Duomenų apsaugos pareigūną privaloma paskirti tuomet, jeigu pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus, kai dideliu mastu tvarkomi specialių kategorijų duomenys ar duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas ir t. t.

SIEKIO ID

ASMENS DUOMENŲ TVARKYMAS

TIKSLAS

Asmens duomenys gali būti renkami ir tvarkomi tik konkrečiu tikslu ir tik tiek, kiek reikalinga šiam apsibrėžtam tikslui pasiekti.

Nusistatę tikslą, turime įvertinti, ar yra ir, jei yra, koks teisinis pagrindas asmens duomenų tvarkymui.

TEISINIS PAGRINDAS

- Sutikimas
- Sutarties sudarymas, vykdymas
- Teisinė prievolė (nustatoma teisės aktuose)
- Gyvybinių interesų apsauga
- Viešasis interesas, valdžios funkcijų vykdymas (nustatoma teisės aktuose)
- Teisėtas interesas (negali būti pagrindas valdžios institucijoms)

SIEKIO ID

SPECIALIŲ KATEGORIJŲ DUOMENŲ TVARKYMAS

Bendra taisyklė – draudžiama tvarkyti specialių kategorijų asmens duomenis.

Sąlygos išimtims, kai specialių kategorijų duomenis galima tvarkyti:

- Sutikimas
- Prievolių ar teisių įgyvendinimas darbo ir socialinės apsaugos teisės srityje (nustatyta teisės aktuose)
- Gyvybinių interesų apsauga
- NVO narių asmens duomenų tvarkymas politinių, filosofinių, religinių ar profesinių sąjungų tikslais
- Duomenų subjekto viešas asmens duomenų paskelbimas
- Teisinių reikalavimų gynimas
- Profilaktinės, darbo medicinos tikslai, sveikatos priežiūros arba socialinės rūpybos paslaugos ir jų sistemų valdymas
- Viešasis interesas visuomenės sveikatos apsaugos tikslu, taip pat archyvavimo, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais

SIEKIO ID

SUTIKIMAS KAIP TEISINIS PAGRINDAS

! Tyla, iš anksto pažymėti langeliai arba neveikimas nelaikomi sutikimu.

Reikalavimai:

- suteiktas laisva valia (nėra statuso disbalanso tarp sutikimo davėjo ir gavėjo, yra galimybė nesutikti);
- Konkretus, vienareikšmis, nedviprasmiškas (aiškiai įvardinant duomenų tvarkymo veiklą ir tikslus, negali būti nesąžiningų sąlygų);
- informacija pagrįstas (duomenų valdytojo tapatybė, tikslai ir t.t.);
- aiškiai atskirtas nuo kitų klausimų;
- suprantama ir lengvai prieinama forma, aiški ir paprasta kalba.

! Atšaukti sutikimą turi būti taip pat lengva kaip jį duoti.

VAIKŲ SUTIKIMAS

Už nepilnametį iki 14 metų sutikimą turi duoti vaiko tėvai ar globėjai. Organizacija (įmonė) yra atsakinga už amžiaus patikrinimo priemones. Vaikui tapus suaugusiu, jis turi teisę sutikimą atšaukti ir reikalauti duomenis ištrinti.

! Tėvų sutikimo nereikalaujama tiesiogiai vaikui teikiant prevencijos ar konsultavimo paslaugas, jei jomis siekiama apsaugoti vaiko interesus.

SIEKIO ID

TEISĖTAS INTERESAS KAIP TEISINIS PAGRINDAS

Remtis savo teisėtu interesu galime, kai:

- duomenų subjekto interesai arba teisės nėra viršesni už organizacijos teisėtą interesą;
- renkant asmens duomenis duomenų subjektas gali tikėtis, kad duomenys gali būti tvarkomi tuo tikslu;
- Duomenų subjektas turi teisę prieštarauti, kad jo asmens duomenys butų tvarkomi teisėto intereso pagrindu.

INTERESŲ BALANSO TESTAS

- Teisėto intereso nustatymas. Aiškiai apibrėžiame duomenų tvarkymo tikslus ir informuojame apie tai duomenų subjektus (pvz., Privatumo politikoje);
- Būtinumo testas. Turime pagrįsti, kad toks asmens duomenų tvarkymas (būdas ir apimtis) tikrai yra būtinas nustatytiems tikslams pasiekti, ar nėra kito varianto, palankesnio duomenų subjektams, tikslams pasiekti (proporcingumas);
- Pusiausvyros testas. Vertiname teisėto intereso pobūdį ir duomenų tvarkymo poveikį. Ar kuriame kokią nors vertę, ar tai gali atitikti pagrįstus duomenų subjekto lūkesčius, ar dėl duomenų tvarkymo gali kilti pavojus asmenų teisėms.

Pvz: Vaizdo stebėjimas saugumo tikslu, kontaktinių duomenų naudojimas tiesioginės rinkodaros tikslu (laikantis Elektroninių ryšių įstatymo nuostatų).

! Specialių kategorijų asmens duomenys negali būti tvarkomi teisėto intereso pagrindu.

SIEKIO ID

DUOMENŲ TVARKYMO PRINCIPAI

Asmens duomenys turi būti:

- Tvarkomi teisėtu, sąžiningu ir skaidriu būdu;
- Renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu;
- Adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų;
- Tikslūs ir prireikus atnaujinami;
- Laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina;
- Tvarkomi užtikrinant tinkamą saugumą (įdiegiamos tinkamos techninės ir organizacinės priemonės).

! Organizacija (įmonė) yra atsakinga už tai, kad šių principų būtų laikomasi, ir turi sugebėti įrodyti, kad jų yra laikomasi praktikoje.

SIEKIO
ID

TVARKYTOJO IR VALDYTOJO STATUSAS

Duomenų valdytojas – duomenų „savininkas“, tas, kuris nustato duomenų tvarkymo tikslus ir priemones.

Duomenų tvarkytojas – tas, kuris duomenų valdytojo vardu tvarko asmens duomenis (duomenų valdytojo naudai ir pagal duomenų valdytojo nurodymus).

Duomenų valdytojas, patikėdamas duomenų tvarkytojui tvarkymo veiklą, turi įsitikinti, kad duomenų tvarkytojas yra patikimas, pajėgus ir kompetentingas įgyvendinti technines ir organizacinės priemones duomenų saugumui ir duomenų subjektų teisėms užtikrinti.

DUOMENŲ TVARKYTOJŲ PAVYZDŽIAI :

- Debesijos paslaugų teikėjai;
- IT sistemų priežiūros paslaugų teikėjai;
- Programavimo paslaugų teikėjai;
- Personalo, buhalterinės apskaitos paslaugas teikiantys asmenys;
- Archyvavimo paslaugų teikėjai ir t. t.

SIEKIO ID

TVARKYTOJO IR VALDYTOJO STATUSAS

Duomenų valdytojas ir duomenų tvarkytojas turi pasirašyti sutartį (ar susitarimą), kurioje nustatomi:

- duomenų tvarkymo dalykas bei trukmė (pasibaigus tvarkymui duomenų ištrynimas ir (arba) grąžinimas);
- duomenų tvarkymo pobūdis ir tikslai;
- asmens duomenų rūšys ir duomenų subjektų kategorijos;
- duomenų tvarkytojo įsipareigojimai duomenų valdytojui (užtikrinti duomenų saugumą, veikti tik pagal duomenų valdytojo rašytinius nurodymus, užtikrinti, kad asmenys tvarkantys duomenis laikytųsi konfidencialumo, teikti būtiną informaciją ir bendradarbiauti sprendžiant klausimus su duomenų subjektais ar priežiūros institucija, informuoti apie duomenų saugumo pažeidimus ir pan.);
- techninės ir organizacinės priemonės duomenų saugumui užtikrinti;
- subtvarkytojų pasitelkimas, duomenų perdavimas;
- asmens duomenų saugumo pažeidimų valdymas (duomenų tvarkytojas valdytojui praneša ne ilgiau kaip per 24 val.);
- duomenų valdytojo prievolės ir teisės (instruktuoti, teikti paklausimus, galimybė tikrinti ir audituoti).

SIEKIO ID

ASMENS DUOMENŲ APSAUGOS REIKALAVIMAI

Saugumo priemonės turi būti parenkamos atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei **duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus pavojus fizinių asmenų teisėms ir laisvėms**. Organizacijos **privalo atlikti duomenų saugumo priemonių ir rizikos įvertinimą** (pagal Valstybinės duomenų inspekcijos 2019 m. gruodžio 18 d. parengtas gaires).

SAUGUMO PRIEMONIŲ PAVYZDŽIAI

- **Techninės priemonės** (antivirusinių programų diegimas; sertifikuotos programinės įrangos naudojimas, el. paštu siunčiamų duomenų šifravimas, prieigų kontrolė ir autentifikavimas, *logų* kiekvienos sistemos ar aplikacijos, naudojamos asmens duomenų tvarkymui fiksavimas, duomenų bazių, serverių, tinklų ir ryšio, patalpų saugumas, atsarginių kopijų darymas, atkūrimo procedūros, mobiliųjų įrenginių autorizavimas, duomenų trynimas, laikmenų utilizavimas ir t. t.)
- **Organizacinės priemonės** (asmens duomenų tvarkymo taisyklių ir procedūrų parengimas ir laikymosi kontrolė, atsakingų asmenų paskyrimas, apibrėžiant jų vaidmenis ir atsakomybę, IT išteklių registras, saugumo incidentų valdymo ir tęstinumo planas, mokymai darbuotojams ir t. t.).

DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

BDAR numato pareigą duomenų valdytojams ir duomenų tvarkytojams turėti duomenų tvarkymo veiklos įrašus, kuriuose būtų detaliai aprašytas atliekamas asmens duomenų tvarkymas.

Duomenų tvarkymo veiklos įrašai privalomi:

- Įmonėms, įstaigoms ar organizacijoms, kuriose dirba **daugiau kaip 250 darbuotojų**;
- **Valdžios institucijoms ir įstaigoms** (nepriklausomai nuo to, kiek dirba darbuotojų);
- Įmonėms, įstaigoms ar organizacijoms, kurių atliekamas asmens duomenis tvarkymas apima **bent vieną iš šių atvejų:**
- **kai dėl vykdomo duomenų tvarkymo gali kilti pavojus duomenų subjektų teisėms ir laisvėms** (pvz., kai siekiant sukurti arba naudoti asmens profilį vertinami asmeniniai aspektai, pvz., duomenys susiję su darbo rezultatais, ekonomine situacija, asmeniniais pomėgiais ar interesais ir t. t.; kai tvarkomi pažeidžiamų fizinių asmenų, visų pirma vaikų, asmens duomenys; arba kai duomenų tvarkymas apima didelį kiekį asmens duomenų);
- **duomenų tvarkymas yra reguliarus;**
- **duomenų tvarkymas apima specialių kategorijų asmens duomenis;**
- **tvarkomi asmens duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas.**

SIEKIO ID

DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

Duomenų tvarkymo veiklos įrašai turi būti tvarkomi raštu, įskaitant elektronine forma, reguliariai (rekomenduojama kartą per metus) atnaujinami.

BDAR nenumato prievolės duomenų valdytojui ir (ar) duomenų tvarkytojui duomenų tvarkymo veiklos įrašų skelbti viešai.

Duomenų valdytojas ar duomenų tvarkytojas turi pateikti įrašus Valstybinei duomenų apsaugos inspekcijai, gavę jos prašymą.

! Plačiau apie tai, kas turėtų būti pildoma duomenų tvarkymo veiklos įrašuose galima rasti Valstybinės duomenų apsaugos inspekcijos 2018 m. birželio 20 d. rekomendacijoje „Dėl duomenų tvarkymo veiklos įrašų“.

Už duomenų veiklos įrašų nuolatinį pildymą prasminga paskirti atsakingą asmenį – „duomenų šeimininką“. Tai gali būtu asmuo dirbantis su konkrečia kategorija asmens duomenų (pvz., atsakingas už tam tikrą procesą organizacijoje). Organizacijoje gali būti keli duomenų šeimininkai priklausomai, kiek ir kokiuose procesuose yra tvarkoma asmens duomenų (pvz., personalo, klientų, partnerių, vaizdo stebėjimo, IT sistemų ir t.t.).

SIEKIO ID

ORGANIZACIJOS PRIVATUMO PRANEŠIMAS

Tai informacinis dokumentas, pateikiamas duomenų subjektams duomenų rinkimo metu, apie tai, kas, kaip, kodėl ir kiek ilgai tvarko jų asmens duomenis. Duomenų subjektus privaloma informuoti apie:

- duomenų valdytojo ir, jeigu aktualu, duomenų valdytojo atstovo tapatybę ir kontaktinius duomenis;
- duomenų apsaugos pareigūno, jeigu yra, kontaktinius duomenis;
- duomenų tvarkymo tikslus, dėl kurių ketinama tvarkyti asmens duomenis, taip pat duomenų tvarkymo teisinį pagrindą;
- teisėtą interesą, jei duomenys tvarkomi teisėto intereso pagrindu;
- asmens duomenų gavėjus ar jų kategorijas;
- ketinimą asmens duomenis perduoti į trečiąją valstybę arba tarptautinei organizacijai, jeigu aktualu;
- asmens duomenų saugojimo laikotarpį;
- duomenų subjektų teises, įskaitant jo teisę bet kuriuo metu atšaukti savo sutikimą, jeigu asmens duomenys tvarkomi sutikimo pagrindu ir teisę pateikti skundą priežiūros institucijai;
- tai, ar asmens duomenų pateikimas yra teisės aktais arba sutartyje numatytas reikalavimas, ar reikalavimas, kurį būtina įvykdyti norint sudaryti sutartį, taip pat tai, ar duomenų subjektas privalo pateikti asmens duomenis, ir informaciją apie galimas tokių duomenų nepateikimo pasekmes;
- apie tai, kad esama automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasmingą informaciją apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui;

SIEKIO ID

ORGANIZACIJOS PRIVATUMO PRANEŠIMAS

Jei asmens duomenys gaunami ne iš paties duomenų subjekto, jis, be prieš tai įvardintų dalykų, turi būti papildomai informuojamas apie:

- asmens duomenų gavimo šaltinį;
- asmens duomenų kategorijas.
- Šiuo atveju nurodyta informacija duomenų subjektams pateikiama:
- ne vėliau kaip per mėnesį;
- pirmą kartą susisiekiant su duomenų subjektu (jeigu naudojama ryšiams palaikyti);
- prieš atskleidžiant duomenis kitam duomenų gavėjui.

Jeigu tokios informacijos pateikimas yra neįmanomas arba tam reikėtų neproporcingų pastangų, visų pirma kai duomenys tvarkomi archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais arba jeigu dėl informavimo pareigos gali tapti neįmanoma arba ji gali labai sukliudyti pasiekti tvarkymo tikslus, duomenų valdytojas imasi tinkamų priemonių duomenų subjekto teisėms ir laisvėms ir teisėtiems interesams apsaugoti, įskaitant viešą informacijos paskelbimą.

! Duomenų subjekto informuoti nereikia, jeigu:

- jis jau turi tokią informaciją;
- duomenų gavimas ar atskleidimas yra aiškiai apibrėžtas teisės aktuose;
- yra prievolė saugoti konfidencialumą ar paslaptį.

SIEKIO ID

ORGANIZACIJOS VIDINIAI DOKUMENTAI

PAVYZDINIS NEBAIGTINIS SĄRAŠAS:

- Asmens duomenų tvarkymo veiklos įrašai;
- Asmens duomenų tvarkymo tvarka (skirta darbuotojams, „duomenų šeimininkams“ dirbantiems su asmens duomenimis);
- Darbuotojų asmens duomenų tvarkymo politika (skirta darbuotojams susipažindinti, kaip tvarkomi jų asmens duomenys);
- IT saugumo politika;
- Prieigų valdymo politika;
- Duomenų saugojimo politika;
- Pažeidimų valdymo tvarka;
- Poveikio vertinimo tvarka;
- Teisėto intereso balanso vertinimo tvarka
- Duomenų subjektų teisių įgyvendinimo tvarka ir t.t.

SIEKIO ID

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

Poveikio duomenų apsaugai vertinimas – procedūra, kuri turi būti atliekama tais atvejais, kai dėl duomenų tvarkymo pobūdžio, tikslų, aprėpties, ypač kai naudojamos inovatyvios technologijos gali kilti didelis pavojus. Tai būdas apsibrėžti duomenų tvarkymo reikalingumą ir proporcingumą, visapusiškai įvertinti rizikas ir nustatyti jų pašalinimo priemones.

Poveikio duomenų apsaugai vertinimas turi būti atliekamas prieš pradedant asmens duomenų tvarkymą. Jei poveikio vertinimo rezultatai parodytų, kad gali kilti didelis pavojus fizinių asmenų teisėms bei laisvėms, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti, turi būti **konsultuojamasi su Valstybine duomenų inspekcija** (BDAR 36 straipsnis).

DIDELIS PAVOJUS FIZINIŲ ASMENŲ TEISĖMS BEI LAISVĖMS

Tai situacija, kai dėl duomenų tvarkymo arba dėl galimo duomenų saugumo pažeidimo pažeidžiama ne tik asmens teisė į privatumą bet ir kitos pagrindinės teisės (žodžio, minties, judėjimo laisvės, diskriminacijos draudimas, teisė į laisvę, sąžinės ir tikėjimo laisvės ir pan.) ir duomenų subjektas dėl to, pvz., gali patirti atskirtį arba diskriminaciją, finansinius nuostolius, gali būti pakenkta jo reputacijai arba atsirasti kitokie rimti padariniai kasdieniam fizinio asmens gyvenimui.

! **Valstybinė duomenų inspekcija yra patvirtinusi pavyzdinę poveikio duomenų apsaugai vertinimo formą.**

SIEKIO ID

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

Atlikti poveikio duomenų apsaugai vertinimą būtina šiais atvejais:

- Asmens duomenų tvarkymas **mokslinių ar istorinių tyrimų** tikslais, (1) kai be asmens sutikimo tvarkomi **specialių kategorijų** asmens duomenys arba asmens duomenų tvarkymas vykdomas susiejant ar derinant **duomenų rinkinius**; (2) kai tvarkomi **nepilnamečių asmenų** duomenys; (3) kai tvarkomas **asmens kodas**.
- Asmens duomenų tvarkymas vykdomas **dideliu mastu**, kai asmens duomenys **gauti ne iš asmens** bei informacijos pateikimas yra neįmanomas arba pareikalautų neproporcingų pastangų.
- Asmens duomenų tvarkymas, kai duomenų gavėjų, kuriems buvo atskleisti asmens duomenys, **informavimas apie asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą nėra įmanomas** arba pareikalautų neproporcingų pastangų.
- **Biometrinių** duomenų tvarkymas.
- **Vaizdo** stebėjimas vykdomas (1) patalpose ar teritorijose, kurios nepriklauso nuosavybės teise duomenų valdytojui; (2) sveikatos priežiūros, socialinės globos, įkalinimo ar kitose įstaigose, kuriose paslaugos teikiamos pažeidžiamiems asmenims; (3) įrašant garsą.
- **Pokalbių telefonu** įrašymas.
- **Inovatyvių technologijų** panaudojimas, tvarkant pažeidžiamų asmenų duomenis.
- **Vaikų asmens duomenų tvarkymas tiesioginės rinkodaros** tikslais, naudojant automatizuotą duomenų tvarkymą, įskaitant profiliavimą.
- **Darbuotojų vaizdo, garso** duomenų tvarkymas, **komunikacijos, elgesio, vietos ar judėjimo** stebėsena, tvarkymas.

SIEKIO ID

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai **sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami asmens duomenys** arba prie jų be leidimo gaunama **prieiga**.

- **Konfidencialumo** pažeidimas – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;
- **Prieinamumo** pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba sunaikinami asmens duomenys;
- **Vientisumo** pažeidimas“– kai asmens duomenys pakeičiami be leidimo ar netyčia.

Priklausomai nuo aplinkybių, pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

SIEKIO
ID

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

PAVYZDINIS NEBAIGTINIS SĄRAŠAS:

- Dokumentų dingimas, vagystė;
- Ne tam adresatui el. paštu išsiunčiamas laiškas su asmens duomenimis;
- Pašalinis asmuo prisijungia prie el. pašto, kompiuterio ar kitų įrenginių;
- Prarandamas kompiuteris/USB laikmena/telefonas;
- Paviešinami asmens duomenys, kurių atžvilgiu privalome užtikrinti konfidencialumą (pvz., darbuotojų darbo užmokestis ir pan.);
- Darbuotojui per klaidą, kai tai nėra būtina jo darbinėms funkcijoms atlikti, suteikiama prieiga prie organizacijos tvarkomų asmens duomenų;
- Užfiksuojamas kompiuterinių įsilaužėlių prisijungimas prie bendrovės IT sistemų ir konfidencialių asmens duomenų;
- Ant darbo stalo paliekami dokumentai, kuriuose yra asmens duomenų;
- Palikus darbo vietą, neužrakinamas kompiuteris;
- Pametami administracinių patalpų raktai, magnetinės durų kortelės;
- Liūtis užpila serverio patalpą;
- Organizacijoje įvyksta vagystė ir t.t.

SIEKIO ID

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

Organizacijai rekomenduojama turėti patvirtintą dokumentą, kuriame būtų aprašyta pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie juos tvarka:

- Pranešimas apie galimą pažeidimą (bet kuris darbuotojas, vos pastebėjęs galimą pažeidimą, praneša apie jį numatyta forma – visais įmanomais būdais įgaliotiems imtis priemonių asmenims);
- Pranešimų tyrimų eiga (nurodoma, koks saugumo incidentas gali būti tiriamas, rizikos vertinimo būdai, atvejai, kada pranešama Valstybinei duomenų apsaugos inspekcijai ir (ar) duomenų subjektui ir pan.);
- Pažeidimų dokumentavimas (kas registruoja pažeidimus, kokia informacija įrašoma Asmens duomenų saugumo pažeidimų žurnale, kur ir kokia forma jis pildomas ir kiek laiko saugomas);
- Tyrimo rezultatų įforminimas, pažeidimų analizė ir prevencijos priemonių įgyvendinimo kontrolė.

SIEKIO ID

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

Vertinant riziką, kuri gali atsirasti dėl duomenų apsaugos pažeidimo, turėtų būti laikoma, kad pažeidimas keliantis pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, turtinę ar neturtinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, pakenkta reputacijai, atskleista profesinė paslaptis ar pan.

Įvertinus riziką rekomenduotina nustatyti, kad yra:

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

Atsakingas asmuo išvadą dėl rizikos įvertinimo teikia vadovui ar įgaliotam asmeniui, kuris turi priimti sprendimą dėl tolimesnių veiksmų. Atsakingas asmuo, be kita ko, turėtų imtis tinkamų techninių organizacinių priemonių, kad pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų.

SIEKIO ID

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

- **Pranešimas Valstybinei duomenų apsaugos inspekcijai**

Turi būti pranešama nedelsiant, **per 72 val.** nuo sužinojimo apie pažeidimą (nurodomas pažeidimo pobūdis, esamos ir tikėtinos pasekmės, priemonės, kurių buvo ar bus imtasi joms išvengti).

Galima nepranešti, jei pažeidimas **nekelia pavojaus** fizinių asmenų teisėms ir laisvėms.

! Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie pažeidimą, rekomenduojama pranešti.

- **Pranešimas duomenų subjektui**

Pranešama nedelsiant, kai dėl asmens duomenų saugumo pažeidimo gali kilti **didelis pavojus** jų teisėms ir laisvėms.

! Rekomenduojama periodiškai peržiūrėti Asmens duomenų saugumo pažeidimų žurnale esančius įrašus ir numatyti, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip bus kontroliuojamas šių prevencinių priemonių įdiegimas, kad ateityje analogiški pažeidimai nepasikartotų.

SIEKIO ID