



ISO 9001  
ISO 45001  
ISO 14001

## UŽDAROJI AKCINĖ BENDROVĖ „SDG“

Draugystės g. 8E, 51264 Kaunas, tel. (8 37) 46 00 66, faks. (8 37) 46 00 67, el. p. [info@sdg.lt](mailto:info@sdg.lt), [www.sdg.lt](http://www.sdg.lt)  
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 135899565, PVM mokėtojo kodas LT358995610

# ASMENS DUOMENŲ APSAUGA

2024-01-11

## Kaip elgtis asmens duomenų saugumo pažeidimo atveju?

### Žemiau esanti informacija aktuali įmonės / įstaigos darbuotojui, atsakingam už asmens duomenų apsaugos klausimų įgyvendinimą.

**Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (BDAR<sup>1</sup> 4 str. 12 p.).

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

1. „Konfidencialumo Pažeidimas“ – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų (tyčinis ar netyčinis informacijos atskleidimas pašaliniams asmenims);
2. „Prieinamumo Pažeidimas“ – kai netyčia arba neteisėtai prarandama prieiga prie informacinių sistemų arba sunaikinami asmens duomenys (tai pilnas arba dalinis informacinės sistemos darbingumo pažeidimas, dėl kurio informacija ir sistemos resursai tampa nepasiekiami visiems arba daliai jos naudotojų);
3. „Vientisumo Pažeidimas“ – kai asmens duomenys pakeičiami be leidimo ar netyčia (tai dažniausiai nesankcionuoti prisijungimai prie informacinių sistemų ir joje atlikti pakeitimai, dalinis arba visiškas informacijos praradimas. Prie vientisumo pažeidimų taip pat priskiriami nesklaidumai tarp sistemų perduodant duomenis arba kai įsivelia klaida darbuotojams juos įvedinėjant. Šie pažeidimai gali būti tyčiniai arba netyčiniai).

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

Taigi, darbuotojas, sužinojęs ar pats nustatęs galimą Pažeidimą (pavyzdžiui, kai informacija apie galimą Pažeidimą gaunama iš kliento, partnerio, žiniasklaidos ar kito šaltinio), privalo nedelsdamas apie tai **informuoti** atsakingą asmenį, t. y. įmonės / įstaigos vadovą, asmens duomenų apsaugos pareigūną arba bet kurį kitą įgaliotą asmenį, atsakingą už asmens duomenų apsaugos klausimų įgyvendinimą apie pastebėtą Pažeidimą. Pranešimas gali būti pateikiamas žodžiu, raštu ar elektroninėmis priemonėmis.

Aukščiau minėtieji asmenys, gavę informaciją apie Pažeidimą, turi kaip įmanoma greičiau imtis atitinkamų techninių priemonių bei atlikti pirminį tyrimą, išsiaiškinti ir nustatyti, ar Pažeidimas iš tikrųjų įvyko, bei kokios galimos pasekmės asmenims, t. y. įvertinti riziką. Rizika vertinama atsižvelgiant į šiuos kriterijus: pažeidimo tipą; asmens duomenų pobūdį, apimtį; kaip lengvai identifikuojamas fizinis asmuo; pasekmių rimtumą fiziniams asmenims; specialias fizinio asmens savybes (pavyzdžiui, duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis); nukentėjusių asmenų skaičių; specialias duomenų valdytojo savybes (pavyzdžiui, veiklos pobūdį). Pirminio tyrimo metu turi būti fiksuojama informacija apie Pažeidimą. Pildomas Pranešimas apie duomenų saugumo pažeidimą.

<sup>1</sup> Bendrasis duomenų apsaugos reglamentas (ES) 2016/679.

Įvertinus riziką, įmonės / įstaigos vadovas ar jo įgaliotas asmuo, pasitarę su duomenų apsaugos pareigūnu, turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimo sustabdymu bei pašalinimu. Negalima delsti, nes apie Pažeidimą privaloma **pranešti** Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ne vėliau kaip per 72 val. nuo sužinojimo apie Pažeidimą, pateikiant pranešimą apie asmens duomenų saugumo pažeidimą, išskyrus, kai tikėtina, kad toks Pažeidimas nekels pavojaus asmenų teisėms ir laisvėms. Kai dėl Pažeidimo pobūdžio ir rizikos rimtumo kyla didelė grėsmė fizinių asmenų teisėms ir laisvėms, įmonė / įstaiga apie Pažeidimą privalo pranešti ir duomenų subjektui. Taip pat, esant poreikiui yra informuojamos ir kitos valstybinės įstaigos, kaip pavyzdžiui: **policija**, kuri tiria atvejus, kai padaromas nusikalstamos veikos, susijusios su asmens duomenimis, pvz., tapatybės vagystė; **Nacionalinis kibernetinio saugumo centras** (toliau – NKSC), kurį reikia informuoti apie kibernetinius incidentus užpildant specialią formą NKSC tinklapyje, kurią rasite adresu: <https://www.nksc.lt/pranesti.html>, taip pat galima siųsti elektroninį laišką ar skambinti telefonu.

Be to, visi Pažeidimai, nepriklausomai ar apie juos buvo pranešta VDAI, ar ne, turi būti registruojami.

**Žemiau esanti informacija aktuali įmonės / įstaigos darbuotojams.** Priminkite visiems darbuotojams (pavyzdžiui, susirinkimo metu, elektroniniu būdu, skelbimų lentoje ir pan.), kad

- 1. privaloma saugoti asmens duomenų konfidencialumą ir negalima atskleisti šių duomenų tretiesiems asmenims** (išskyrus tuos, kurie teisės aktų nustatyta tvarka turi tokią teisę), įskaitant kitus įmonės / įstaigos darbuotojus, kurie neturi teisės susipažinti su asmens duomenimis, nepriklausomai nuo to, kokių būdu jie šiuos duomenis gavo. Konfidencialumo taisyklė taikoma tiek tais atvejais, kuomet darbuotojui prieigą prie asmens duomenų suteikė įmonė / įstaiga, tiek tais atvejais, kuomet darbuotojas pats sužinojo asmens duomenis.
- 2. Jeigu kyla abejonių, ar konkretus asmuo turi teisę gauti asmens duomenis, privaloma konsultuotis su tiesioginiu vadovu ir / ar duomenų apsaugos pareigūnu** ir tik gavus teigiamą atsakymą galima pateikti asmens duomenis.
- 3. privaloma rūpestingai elgtis su informacija, kurioje yra asmens duomenys** (nepriklausomai nuo jos laikymo formos) ir dėti visas pastangas, kad šios informacijos nesužinotų tretieji asmenys (išskyrus tuos, kurie teisės aktų nustatyta tvarka turi tokią teisę), įskaitant kitus įmonės / įstaigos darbuotojus, kurie neturi teisės susipažinti su asmens duomenimis.
- 4. privaloma informuoti įmonę / įstaigą apie bet kokius pastebėtus neteisėto asmens duomenų tvarkymo atvejus.** Apie įtariamą duomenų saugumo pažeidimą<sup>2</sup> (toliau – Pažeidimas) privaloma informuoti tą pačią dieną, nedelsiant įmonės / įstaigos vadovą, asmens duomenų apsaugos pareigūną arba bet kurį kitą įgaliotą asmenį, atsakingą už asmens duomenų apsaugos klausimų įgyvendinimą. Pranešimas galėtų būti pateikiamas žodžiu, raštu ar elektroninėmis priemonėmis. Negalima delsti, nes apie Pažeidimą gali būti priimtas sprendimas **pranešti** Valstybinei duomenų apsaugos inspekcijai ne vėliau kaip per 72 val. nuo sužinojimo apie Pažeidimą.
- 5. neprivaloma būti visiškai įsitikinusiam, ar tai Pažeidimas, ar ne. Geriau pranešti nesant visiškai įsitikinus dėl galimo Pažeidimo, negu nepranešti visai.**

Teisės departamento vadovė / Duomenų apsaugos pareigūnė

Birutė Pėstininkė

UAB „SDG“

Draugystės g. 8E, 51264 Kaunas

Mob. 8 686 18867

El. paštas: [b.pestininke@sdg.lt](mailto:b.pestininke@sdg.lt)

***Būkite su mumis ir būsite geriausi***

<sup>2</sup> **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.