

# ADSP pavojaus vertinimas

---

Valstybinės duomenų apsaugos  
inspekcijos Informacinių technologijų  
skyriaus vedėja Lina Lelešienė



VALSTYBINĖ  
DUOMENŲ  
APSAUGOS  
INSPEKCIJA

# ADSP pavojaus vertinimas

Kada incidentas tampa pavojumi asmenų teisėms ir laisvėms?

**Vertinimo ašis: galimo poveikio sunkumas + poveikio atsiradimo tikimybė**

## 01 Faktai

Kas įvyko?  
Kokie duomenys?  
Kiek asmenų?

## 02 ADSP pobūdis

Konfidencialumas  
Vientisumas  
Prieinamumas

## 03 Duomenys

Jautrumas  
Kiekis  
Duomenų  
deriniai

## 04 Identifikavimas

Ar galima susieti?  
Ar taikytas  
šifravimas ar  
pseudonimizacija?

## 05 Sprendimas

Pranešti VDAI?  
Pranešti  
asmeniui?  
Dokumentuoti  
vertinimą

**Pavojaus vertinimas nėra formalumas – tai atskaitomybės ir tinkamo reagavimo įrodymas.**

# ADSP pobūdis

Koks pažeidimas įvyko ir kokį pavojų jis dažniausiai kelia?

## 01 Konfidencialumo pažeidimas

Neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos suteikimas

Vertinama pagal  
**PAVOJAUS LYGIS PRIKLAUSO  
NUO KONTEKSTO**

## 02 Vientisumo pažeidimas

Neleistinas arba netyčinis asmens duomenų pakeitimas

Vertinama pagal  
**PAVOJAUS LYGIS PRIKLAUSO  
NUO KONTEKSTO**

## 03 Prieinamumo pažeidimas

Prieigos praradimas, duomenų sunaikinimas ar laikinas neprieinamumas

Vertinama pagal  
**PAVOJAUS LYGIS PRIKLAUSO  
NUO KONTEKSTO**

**Vien ADSP pobūdis pats savaime nenulemia pavojaus lygio.**

**Tos pačios rūšies pažeidimas skirtingomis aplinkybėmis gali kelti skirtingo lygio pavojų.**

# Duomenų pobūdis ir jautrumas

Kokie duomenys paveikti ir kiek žalos jie gali sukelti?

**Kuo jautresni duomenys ir kuo platesnis jų derinys, tuo didesnis galimos žalos pavojus.**

**01 Specialių kategorijų ir teistumo duomenys**  
Sveikatos, biometriniai, genetiniai duomenys, politinės pažiūros, religija, teistumas

**GALI DIDINTI  
PAVOJŲ**

**02 Finansiniai ir mokėjimų duomenys**  
Mokėjimai, kreditinės kortelės, sąskaitos, kiti finansiniai duomenys

**VERTINTI  
PAGAL  
KONTEKSTĄ**

**03 Prisijungimo duomenys ir raktai**  
Slaptažodžiai, prisijungimai, šifravimo raktai ar kiti autentifikavimo duomenys

**GALI LEMTI  
DIDELĮ  
PAVOJŲ**

**04 Tinkamai apsaugoti duomenys**  
Tik pseudonimizuoti ar užšifruoti duomenys, kai raktai nepažeisti

**PAVOJAUS  
NĖRA,  
JEI  
APSAUGA  
VEIKSMINGA**

**Net nedidelis labai jautrių duomenų kiekis gali turėti didelį poveikį vienam asmeniui.**

**Pavojaus lygį lemia ne vien duomenų kategorija, bet ir visas ADSP kontekstas.**

# Asmenų identifikavimo lengvumas

Ar pažeisti duomenys leidžia tiesiogiai ar netiesiogiai nustatyti asmenį?

**Du pagrindiniai klausimai: ar galima susieti duomenis su asmeniu + ar taikytos apsaugos priemonės?**

## 01 Tiesioginis identifikavimas

Duomenys savaime leidžia atpažinti konkretų asmenį.

**Pvz.: asmens kodas, IBAN**

## 02 Netiesioginis identifikavimas

Asmuo gali būti nustatomas susiejant kelis duomenis.

**Pvz.: IP, geolokacija, deriniai**

## 03 Apsaugos priemonės

Svarbu, ar duomenys buvo šifruoti ar pseudonimizuoti.

**Pavojus mažėja, kai šifravimas tinkamas, o raktai nepažeisti**

**Kuo lengviau susieti duomenis su asmeniu, tuo didesnė galimų pasekmių tikimybė.**

**Vien pseudonimizacijos nepakanka, jeigu yra papildoma informacija tapatybei atkurti.**

**Vertinkite ne tik duomenų pavadinimą, bet ir realią galimybę juos susieti su konkrečiu žmogumi.**

# Pavojaus lygis ir pareigos

Ką daryti įvertinus, kokį pavojų ADSP kelia asmenų teisėms ir laisvėms?

**Sprendimas priklauso nuo nustatyto pavojaus lygio:  
dokumentuoti • pranešti VDAI • informuoti asmenis**

## 01 PAVOJAUS NĖRA

|                    |      |
|--------------------|------|
| Dokumentuoti       | TAIP |
| Pranešti VDAI      | NE   |
| Informuoti asmenis | NE   |

## 02 KYLA PAVOJUS

|                    |      |
|--------------------|------|
| Dokumentuoti       | TAIP |
| Pranešti VDAI      | TAIP |
| Informuoti asmenis | NE   |

## 03 KYLA / GALI KILTI DIDELIS PAVOJUS

|                    |       |
|--------------------|-------|
| Dokumentuoti       | TAIP  |
| Pranešti VDAI      | TAIP  |
| Informuoti asmenis | TAIP* |

**\* Informuoti asmenų gali nereikėti, jeigu įvykdyta BDAR 34 str. 3 d. sąlyga, pvz., pažangus šifravimas.**

**Atsiradus naujoms aplinkybėms,  
pavojaus vertinimas turi būti peržiūrimas.**

**Operatyvios poveikio mažinimo priemonės  
gali sumažinti pavojaus lygį.**

**Pavojaus lygis turi lemti konkretų veiksmų planą, o ne likti vien formaliu vertinimu.**

# Pažeidžiamos asmenų grupės

Kam asmens duomenų saugumo pažeidimas gali turėti didesnį poveikį?

## 01 Vaikai ir paaugliai

Didesnis pažeidžiamumas dėl amžiaus ir priklausomumo nuo kitų

## 02 Sunkiai sergantys asmenys

Sveikatos būklė gali sustiprinti neigiamų pasekmių poveikį

## 03 Socialiai jautrios grupės

Asmenų padėtis gali didinti pažeidimo pasekmių sunkumą

## 04 Asmenys su intelekto ar kognityviniais sutrikimais

Gali būti sunkiau atpažinti grėsmes ar apsisaugoti nuo pasekmių

**Paveikus pažeidžiamas grupes, pavojus vertinamas kaip didesnis.**

**Vertinkite ne tik duomenis, bet ir konkrečių paveiktų asmenų situaciją.**

# ADSP pavojaus vertinimo matrica

Pavojaus lygis nustatomas pagal galimo poveikio sunkumą ir tikimybę

|          |                   |                      |                        |                        |
|----------|-------------------|----------------------|------------------------|------------------------|
| TIKIMYBĖ | Didelė tikimybė   | <b>Pavojaus nėra</b> | <b>Didelis pavojus</b> | <b>Didelis pavojus</b> |
|          | Vidutinė tikimybė | <b>Pavojaus nėra</b> | <b>Kyla pavojus</b>    | <b>Didelis pavojus</b> |
|          | Maža tikimybė     | <b>Pavojaus nėra</b> | <b>Pavojaus nėra</b>   | <b>Kyla pavojus</b>    |
|          |                   | Žemas sunkumas       | Vidutinis sunkumas     | Didelis sunkumas       |
|          |                   | SUNKUMAS             |                        |                        |

## Kaip naudoti matricą?

1. Įvertinkite galimo poveikio sunkumą.
2. Įvertinkite žalos atsiradimo tikimybę.
3. Raskite susikirtimo tašką.

Matrica padeda pagrįsti sprendimą, bet galutinį pavojaus lygį lemia konkretus ADSP kontekstas.

**Vertinimas turi būti pagrįstas objektyviais faktais; netipinėmis aplinkybėmis lygis gali būti padidintas arba sumažintas.**

# Pavojaus vertinimas nėra vienkartinis

ADSP poveikis gali paaiškėti ne iš karto – vertinimą reikia peržiūrėti, jei atsiranda naujų faktų

## 01 Pirminis vertinimas

Kai sužinoma apie ADSP, įvertinamos faktinės aplinkybės ir pradinis pavojaus lygis.



## 02 Trumpalaikis scenarijus

Kas gali nutikti per pirmąsias savaites?  
Ar žala jau pasireiškia?



## 03 Vėlesnės pasekmės

Per kelis mėnesius ar metus duomenys gali būti sujungiami su kitais rinkiniais ir panaudoti.



## 04 Vertinimo peržiūra

Jei paaiškėja naujų aplinkybių, pavojaus vertinimas turi būti atnaujinamas.

**Rekomenduotina analizuoti bent tris perspektyvas: tiesioginę, vidutinės trukmės ir ilgalaikę.**

**Nutekinti duomenys gali būti panaudoti vėliau, todėl pirminis vertinimas nėra galutinis.**

# AČIŲ!

## Dėkoju už dėmesį

---

Valstybinės duomenų apsaugos  
inspekcijos Informacinių technologijų  
skyriaus vedėja Lina Lelešienė



VALSTYBINĖ  
DUOMENŲ  
APSAUGOS  
INSPEKCIJA