

PATVIRTINTA

Klaipėdos sutrikusio vystymosi

kūdikių namų direktorės Aušros Nikolajevienės

2022 m. balandžio 14 d. įsakymu Nr. V- 36/1

**KLAIPĖDOS SUTRIKUSIO VYSTYMO SI KŪDIKIŲ NAMŲ  
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ INCIDENTŲ  
VALDYMO TVARKOS APRAŠAS**

## I. BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja duomenų saugumo pažeidimų aptikimo, sustabdymo (pašalinimo) ir pranešimo apie juos įgyvendinimo tvarką Klaipėdos sutrikusio vystymosi kūdikių namuose (toliau – Kūdikių namai).
2. Pagrindinės Apraše vartojamos sąvokos:
  - 2.1. **asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti;
  - 2.2. **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;
  - 2.3. **duomenų subjektas** – fizinis 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;
  - 2.4. **duomenų tvarkytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis;
  - 2.5. **duomenų valdytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones;
  - 2.6. **VDAI** – Valstybinė duomenų apsaugos inspekcija;
3. Asmens duomenų saugumo pažeidimai yra skirstomi į 3 tipus:
  - 3.1. *konfidencialumo pažeidimas* – be Kūdikių namų leidimo ar neteisėtai tretiesiems asmenims atskleidžiami asmens duomenys arba suteikiama prieiga prie šių duomenų;
  - 3.2. *prieinamumo pažeidimas* – dėl neatsargumo arba neteisėtai prarandama prieiga prie Kūdikių namų ar jos duomenų tvarkytojų tvarkomų asmens duomenų arba pastarieji asmens duomenys dėl neatsargumo arba neteisėtai yra sunaikinami;
  - 3.3. *vientisumo pažeidimas* – Kūdikių namų ar jos duomenų tvarkytojų tvarkomi asmens duomenys neteisėtai ar dėl neatsargumo yra pakeičiami be Kūdikių namų leidimo.
4. Vienas asmens duomenų saugumo pažeidimas gali atitikti kelis tipus.
5. Reagavimo į galimą asmens duomenų saugumo pažeidimą, nustatyto asmens duomenų saugumo pažeidimo valdymo ir šalinimo procese dalyvauja Kūdikių namų duomenų apsaugos pareigūnas.
6. Aprašas parengtas vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Reglamentas) bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ), o Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente, ADTAĮ ir kituose Lietuvos Respublikos teisės aktuose.

## II. DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

7. Asmens duomenų saugumo pažeidimu yra laikoma 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.
8. Kūdikių namų darbuotojas, sužinojęs ar pats nustatęs galimą pažeidimą arba kai informacija apie galimą pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio, privalo nedelsdamas visais įmanomais būdais (įskaitant, tačiau neapsiribojant, žodžiu, raštu, telefonu, elektroniniu paštu) apie tai informuoti Kūdikių namų atsakingą darbuotoją už asmens duomenų apsaugą (jeigu pažeidimas susijęs su elektroninės formos asmens duomenų tvarkymu bei Kūdikių namų naudojamomis informacinėmis programomis, jeigu pažeidimas susijęs su rašytinės formos asmens duomenų tvarkymu). Siekdamas nustatyti, ar iš tikrųjų įvyko asmens duomenų saugumo pažeidimas bei kokios galimos pasekmės duomenų subjektams, atsakingas darbuotojas privalo imtis atitinkamų ir adekvačių priemonių galimo duomenų saugumo pažeidimo tyrimui ir apie įvykusį asmens duomenų

saugumo pažeidimą bei jo tyrimo rezultatus nedelsiant visais įmanomais būdais informuoti Kūdikių namų direktorių bei duomenų apsaugos pareigūną (toliau – Pareigūnas).

9. Galimi asmens duomenų saugumo pažeidimo tipai: konfidencialumo pažeidimas (kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų), prieinamumo pažeidimas (kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba sunaikinami asmens duomenys) ir vientisumo pažeidimas (kai asmens duomenys pakeičiami be leidimo ar netyčia). Priklausomai nuo aplinkybių asmens duomenų saugumo pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

10. Priklausomai nuo asmens duomenų saugumo pažeidimo pobūdžio (tipo), atliekant pirminį tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, turi būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamoms visoms tinkamos techninės ir organizacinės priemonės (pavyzdžiui, duomenų srauto ir prisijungimų analizės įrankiai bei kita).

11. Vertinant riziką, kuri gali atsirasti dėl asmens duomenų saugumo pažeidimo, turi būti atsižvelgiama į konkrečias asmens duomenų saugumo pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turi būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus: asmens duomenų saugumo pažeidimo tipą bei pobūdį (pavyzdžiui, ypatingi asmens duomenys), apimtis, kaip lengvai identifikuojamas duomenų subjektas, pasekmių rimtumą duomenų subjektams, specialias duomenų subjekto savybes (pavyzdžiui, duomenys, susiję su vaikais ar kitais pažeidžiamais asmenimis), nukentėjusiųjų duomenų subjektų skaičių, Kūdikių namų veiklos pobūdį.

12. Vertinant riziką, turi būti laikoma, kad asmens duomenų saugumo pažeidimas, galintis kelti pavojų duomenų subjektų teisėms ir laisvėms, yra toks, dėl kurio laiku nesiėmus tinkamų priemonių, duomenų subjektai gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie laikomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam duomenų subjektui).

13. Įvertinus riziką, nustatoma: *žema rizikos tikimybė, vidutinė rizikos tikimybė arba didelė (aukšta) rizikos tikimybė.*

14. Už duomenų saugumo pažeidimų valdymą Kūdikių namuose atsakingi asmenys, visų pirma, turi imtis visų tinkamų techninių ir organizacinių priemonių, kad su Pareigūno pagalba asmens duomenų saugumo pažeidimas būtų išsamiai iširtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų.

15. Išvadą dėl asmens duomenų saugumo pažeidimo buvimo ir rizikos duomenų subjektų teisėms bei laisvėms įvertinimo atsakingas asmuo turi nedelsiant pateikti Kūdikių namų direktoriui bei Pareigūnui, kurie turi priimti sprendimą dėl tolimesnių veiksmų, susijusių su asmens duomenų saugumo pažeidimu.

16. Nustačius asmens duomenų saugumo pažeidimą, Kūdikių namai imasi neatidėliotinų adekvačių priemonių užkertant kelią neteisėtam asmens duomenų tvarkymui. Įvertinus riziką, Kūdikių namų direktorius, asmens duomenų saugumo pažeidimo atveju nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai sužino apie asmens duomenų saugumo pažeidimą, apie tai praneša Pareigūnui bei Valstybinei duomenų apsaugos inspekcijai (toliau – Priežiūros institucija) ir / ar duomenų subjektams, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu Priežiūros institucijai apie asmens duomenų saugumo pažeidimą nepranešama per 72 valandas, pranešime nurodomos vėlavimo priežastys ir, jei įmanoma, pridedami nurodytas aplinkybes pagrindžiantys dokumentai. Pranešti apie asmens duomenų saugumo pažeidimą Priežiūros institucijai reikia net ir tuo atveju, jeigu įvertinus riziką yra abejojama, ar rizika yra ir ar reikia apie tai pranešti Priežiūros institucijai.

17. Pareigūnui sužinojus apie įvykusį asmens duomenų saugumo pažeidimą ar kitą incidentą, Pareigūnas nedelsiant įvertina su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, apimtį, kontekstą ir tikslus, bendradarbiaudamas kartu su Kūdikių namų

direktoriumi bei komisija, pasiūlo įstaigai sprendimus dėl priemonių, reikiamų asmens duomenų apsaugos pažeidimui ir jo padariniams pašalinti.

18. Kūdikių namai fiksuoja bei dokumentuoja visus asmens duomenų saugumo pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi taip, kad remdamasi tais dokumentais, Priežiūros institucija galėtų patikrinti, ar laikomasi šio reikalavimo.

19. Įvykusius duomenų saugumo pažeidimus Kūdikių namų direktoriaus patvirtintos formos asmens duomenų saugumo pažeidimų registravimo žurnale registruoja atsakingas darbuotojas už asmens duomenų apsaugą įstaigoje. Kūdikių namų asmens duomenų saugumo pažeidimų registravimo žurnalas (Priedas Nr. 1) yra pildomas elektronine forma, o jame esantys duomenų saugumo pažeidimų įrašai elektronine forma Kūdikių namuose yra saugomi 3 (trejus) metus po duomenų saugumo pažeidimo tyrimo pabaigos.

20. Asmens duomenų saugumo pažeidimų registravimo žurnale turi būti registruojami visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Priežiūros institucijai ar ne. Informacija apie asmens duomenų saugumo pažeidimą į asmens duomenų saugumo pažeidimų registravimo žurnalą turi būti įvedama nedelsiant, bet ne vėliau kaip per 5 (penkias) darbo dienas, kai tik nustatomas asmens duomenų saugumo pažeidimo faktas ir įvertinama rizika. Esant būtinybei, asmens duomenų saugumo pažeidimų registravimo žurnale esanti informacija turi būti papildoma ir / arba koreguojama.

21. Asmens duomenų saugumo pažeidimų registravimo žurnale turi būti nurodomi visi su asmens duomenų saugumo pažeidimu susiję faktai – pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti, pažeidimo poveikis ir pasekmės, taisomieji veiksmai (techninės priemonės), kurių buvo imtasi, priežastys dėl su asmens duomenų saugumo pažeidimu susijusių sprendimų priėmimo (pavyzdžiui, kodėl Kūdikių nami nusprendė nepranešti apie asmens duomenų saugumo pažeidimą Priežiūros institucijai ir / ar duomenų subjektui), pranešimo Priežiūros institucijai pateikimo vėlavimo priežastys (jeigu pranešimą vėluojama pateikti arba pranešimas yra teikiamas etapais), informacija, susijusi su pranešimu duomenų subjektui (pavyzdžiui, ar buvo pranešta, kodėl nepranešta ir pan.), kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

22. Kūdikių namų direktoriaus įsakymų paskirta komisija, privalo periodiškai, bet ne rečiau kaip kartą per 1 (vienerius) metus, peržiūrėti asmens duomenų saugumo pažeidimų registravimo žurnale esančius įrašus ir numatyti, kokios prevencinės priemonės turi būti įgyvendinamos, kad ateityje analogiški asmens duomenų saugumo pažeidimai nesikartotų.

23. Pranešime Priežiūros institucijai apie asmens duomenų saugumo pažeidimą turi būti bent:

23.1. aprašytas asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;

23.2. nurodyta Pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;

23.3. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

23.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Kūdikių namai, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant tinkamas priemones, galimoms neigiamoms jo pasekmėms sumažinti (pavyzdžiui, nurodyti, kad apie asmens duomenų saugumo pažeidimą yra informuota Priežiūros institucija ir kad yra gautas patarimas dėl asmens duomenų saugumo pažeidimo tvarkymo ir jo poveikio sumažinimo, duomenų subjektui buvo pasiūlyta pasikeisti slaptažodį ir pan.).

24. Jeigu informacijos neįmanoma pateikti Priežiūros institucijai tuo pačiu metu arba, priklausomai nuo asmens duomenų saugumo pažeidimo pobūdžio, Kūdikių namams yra būtina atlikti išsamesnį tyrimą ir nustatyti visas svarbias asmens duomenų saugumo pažeidimo aplinkybes ir per 72 valandas nuo sužinojimo apie asmens duomenų saugumo pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, pranešimui reikalinga informacija toliau nepagrįstai nedelsiant gali būti teikiama etapais. Esant galimybei, Kūdikių namai privalo pateikti Priežiūros institucijai pirminį pranešimą bei informuoti apie tai, kad informacija apie asmens duomenų saugumo pažeidimą bus teikiama etapais.

25. Jeigu po pranešimo Priežiūros institucijai pateikimo, atlikus išsamesnį tyrimą yra nustatoma, kad asmens duomenų saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio asmens duomenų saugumo pažeidimo, apie tai nedelsiant turi būti informuojama Priežiūros institucija ir tai pažymėta asmens duomenų saugumo pažeidimų registravimo žurnale.

26. Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, Kūdikių namai nedelsiant turi pranešti apie tai ir duomenų subjektui. Pranešime duomenų subjektui aiškia ir paprasta kalba aprašomas asmens duomenų saugumo pažeidimo pobūdis ir pateikiama bent Aprašo 20 punkte nurodyta informacija ir priemonės bei kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu, kuri, Kūdikių namų manymu, turėtų būti pateikta duomenų subjektui. Priežiūros institucijos informavimas apie asmens duomenų saugumo pažeidimą, neatleidžia Kūdikių namų nuo pareigos informuoti duomenų subjektą.

27. Duomenų subjektai apie asmens duomenų saugumo pažeidimą turi būti informuoti tiesiogiai (pavyzdžiui, siunčiant jiems pranešimą elektroniniu paštu, trumpąją žinutę, paštu ar pan.). Šis pranešimas turi būti atskirtas nuo kitos siunčiamos informacijos (pavyzdžiui, naujienlaiškiai ar standartiniai pranešimai).

28. Pranešimas duomenų subjektui gali būti neteikiamas, jeigu įvykdomos bet kurios toliau nurodytos sąlygos:

28.1. Kūdikių namai įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (pavyzdžiui, šifravimo priemonės);

28.2. Kūdikių namai ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

28.3. jei pareikalautų neproporcingai daug pastangų, tokiu atveju vietoj to apie tai viešai paskelbiama arba taikoma panaši priemonė, kuria Duomenų subjektai būtų informuojami taip pat efektyviai.

29. Jeigu tiriant duomenų saugumo pažeidimą pradžioje nustatoma, kad nėra pavojaus duomenų subjektų teisėms ir laisvėms, tačiau detalesnio duomenų saugumo pažeidimo tyrimo metu nustatoma, kad toks pavojus gali kilti, Kūdikių namai privalo riziką vertinti iš naujo.

### **III. BAIGIAMOSIOS NUOSTATOS**

30. Už duomenų saugumo pažeidimų valdymą (įskaitant, tačiau neapsiribojant pirminį duomenų saugumo pažeidimo tyrimą (kada ir koks pažeidimas įvyko, kokie duomenys buvo pažeisti, kokie galimi neigiami padariniai, siūlomos priemonės pažeidimo padariniams sumažinti ir kt.) bei Pareigūno informavimą, Kūdikių namuose atsakingas atsakingas darbuotojas, paskirtas įstaigos direktoriaus įsakymu.

31. Už asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą Kūdikių namuose atsakingas įsakymu paskirtas darbuotojas.

32. Už duomenų saugumo pažeidimų valdymą bei asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą Kūdikių namuose atsakingi asmenys su Aprašu yra supažindinami pasirašytinai ir privalo laikytis jo nuostatų bei atlikdami savo darbo funkcijas vadovautis Apraše nustatyta duomenų saugumo pažeidimų valdymo tvarka.

33. Kūdikių namai turi teisę iš dalies arba visiškai pakeisti Aprašą. Su Aprašo nuostatų pakeitimais už duomenų saugumo pažeidimų valdymą bei asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą Kūdikių namuose atsakingi asmenys yra supažindinami pasirašytinai .



