PATVIRTINTA
UAB „Panevėžio autobusų parkas“
generalinio direktoriaus
2026 m. lapkričio 12 d. įsakymu Nr. 41

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO UAB „PANEVĖŽIO AUTOBUSŲ PARKAS“ TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo UAB „Panevėžio autobusų parkas“ (toliau – PAP) tvarkos aprašas (toliau – Tvarkos aprašas) nustato asmens duomenų saugumo pažeidimų nustatymo, registravimo, tyrimo, valdymo, pašalinimo, dokumentavimo bei pranešimų Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams teikimo tvarką.

2. Tvarkos apraše vartojamos sąvokos:

2.1. **Asmens duomenų saugumo pažeidimas** (toliau – pažeidimas) – duomenų tvarkymo saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami gauti, saugomi arba kitaip tvarkomi duomenys arba prie jų be leidimo gaunama prieiga.

2.2. **Duomenų apsaugos pareigūnas** – Bendrojo duomenų apsaugos reglamento nustatytas ir PAP paskirtas arba pasitelktas asmuo, atliekantis duomenų apsaugos pareigūno funkcijas.

2.3. **Sužinojimo apie pažeidimą momentas** – laikas, kai PAP gauna pakankamai informacijos pagrįstai manyti, kad įvyko saugumo pažeidimas.

2.4. **Atsakingas asmuo** – bendrovės pasitelktas teisininkas, atsakingas už pažeidimų tyrimą ir pranešimą.

3. Galimi šie asmens duomenų saugumo pažeidimai:

3.1. konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas;

3.2. vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas;

3.3. prieinamumo pažeidimas – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

4. Atsižvelgiant į aplinkybes, asmens duomenų saugumo pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu, taip pat su bet kokiu jų deriniu.

5. Asmens duomenų saugumo pažeidimas gali įvykti dėl šių priežasčių:

5.1. žmogiškoji klaida (pvz., prarandama autobuso vaizdo įrašymo įrenginio laikmena, asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti nešiojami/mobilieji įrenginiai (telefonas, nešiojamasis kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.);

5.2. vagystė (pvz., pavogti nešiojami/mobilieji įrenginiai, kuriuose saugomi asmens duomenys; pavogtos bylos, kuriose yra asmens duomenų ir kt.);

5.3. kibernetinė ataka (pvz., įsilaužiama į vaizdo įrašymo įrenginį (DVR/NVR), duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

5.4. neleistina (neautorizuota) prieiga prie asmens duomenų (pvz., asmuo neturėdamas įgaliojimų peržiūri, eksportuoja arba nukopijuoja vaizdo įrašus, įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis; įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

5.5. įrenginių ar programinės įrangos gedimas, saugos sistemos spragos (pvz., sugedus vaizdo įrašymo įrenginiui prarandami įrašai, kuriuose yra asmens duomenų, energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

5.6. nenugalimos jėgos (*force majeure*) aplinkybės ir kitos priežastys (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).

6. Tvarkos aprašo nuostatų privalo laikytis visi PAP darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino bei juridiniai asmenys, tvarkantys PAP duomenis sutartiniais pagrindais, kuriems pagal Reglamento 33 straipsnio 2 dalį nustatyta pareiga nedelsiant informuoti PAP apie kiekvieną asmens duomenų saugumo pažeidimą.

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

7. Informacija apie galimą asmens duomenų saugumo pažeidimą gali būti gaunama:

7.1. iš darbuotojų;

7.2. iš duomenų tvarkytojų;

7.3. iš duomenų subjektų;

7.4. iš žiniasklaidos ar viešosios erdvės;

7.5. atliekant vidaus auditą ar patikrinimą;

7.6. iš informacinių sistemų stebėsenos priemonių;

7.7. iš kitų šaltinių.

8. PAP darbuotojas, nustatęs galimą asmens duomenų saugumo pažeidimą, arba gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą:

8.1. nedelsdamas, bet ne vėliau kaip per 2 valandas nuo sužinojimo momento, nepriklausomai nuo darbo laiko, poilsio ar švenčių dienų, apie tai praneša. Bendrovės administracijos darbo metu informuojamas tiesioginis vadovas, teisininkas ir duomenų apsaugos pareigūnas, o administracijos ne darbo metu pranešama telefonu budinčiam dispečeriui. Pranešimas budinčiam dispečeriui laikomas tinkamu darbuotojo pranešimo pareigos įvykdymu. Pranešama apie tuo metu žinomas aplinkybes, nelaukiant rašytinio pranešimo įforminimo ar generalinio direktoriaus rezoliucijos;

8.2. Pateikęs pirminį pranešimą šio Tvarkos aprašo 8.1 papunktyje nustatyta tvarka, darbuotojas užpildo Pranešimą apie asmens duomenų saugumo pažeidimą (Tvarkos aprašo 1 priedas) ir pateikia jį teisininkui. Jeigu dėl objektyvių aplinkybių darbuotojas negali nedelsdamas

užpildyti ar pasirašyti pranešimo, jis įforminamas, kai tik atsiranda galimybė. Rašytinio pranešimo nepateikimas nestabdo galimo pažeidimo vertinimo ir tyrimo pradžios.

8.3. Jei įmanoma, pagal savo kompetenciją ir galiojančias instrukcijas imasi neatidėliotinų priemonių pažeidimo pasekmėms sumažinti, neatlikdamas savavališkų techninių veiksmų, galinčių sunaikinti ar pakeisti tyrimui reikšmingus duomenis;

8.4. Budintis dispečeris, gavęs pranešimą apie galimą asmens duomenų saugumo pažeidimą ne Bendrovės administracijos darbo metu, nedelsdamas užfiksuoja pranešimo gavimo datą, laiką, pranešėjo kontaktinius duomenis ir jam žinomas įvykio aplinkybes bei telefonu perduoda informaciją teisininkui. Jeigu su teisininku susisiekti nepavyksta, dispečeris nedelsdamas susisiekia su generaliniu direktoriumi, o jeigu nepavyksta susisiekti ir su juo – su Pervežimų skyriaus vadovu. Informacija taip pat perduodama teisininkui ir duomenų apsaugos pareigūnui elektroniniu paštu. Dispečeris užfiksuoja, kam ir kada informacija buvo perduota;

8.5. Teisininkas, o jeigu su juo susisiekti nepavyksta – generalinis direktorius arba Pervežimų skyriaus vadovas, gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą, organizuoja pirminį įvykio aplinkybių įvertinimą ir prireikus neatidėliotinų priemonių taikymą. Pirminis įvertinimas atliekamas nedelsiant, bet ne vėliau kaip per 24 valandas nuo pirmosios informacijos gavimo Bendrovėje, nepriklausomai nuo darbo laiko. Vertinant aplinkybes prireikus konsultuojamasi su duomenų apsaugos pareigūnu ir pasitelkiami kompetentingi techniniai specialistai. Gavus informaciją apie galimą pažeidimą, turintį skubos požymių, su duomenų apsaugos pareigūnu susisiekiama nedelsiant.

8.6. Asmenų, kuriems perduodama informacija apie galimus asmens duomenų saugumo pažeidimus, kontaktiniai duomenys nurodomi generalinio direktoriaus įsakymu patvirtintame kontaktų sąraše. Sąrašas atnaujinamas pasikeitus atsakingiems asmenims ar jų kontaktiniams duomenims;

8.7. galimo asmens duomenų saugumo pažeidimo skubos požymiais laikomos aplinkybės, rodančios, kad pažeidimas tebevyksta arba nedelsiant nesiėmus veiksmų gali padidėti jo neigiamos pasekmės, įskaitant kibernetinę ataką, įsilaužimą į informacinę ar vaizdo stebėjimo sistemą, prisijungimo duomenų perėmimą, įrenginio ar laikmenos su asmens duomenimis praradimą arba vagystę, neteisėtą didelio kiekio asmens duomenų atskleidimą ar pažeidimą, susijusį su specialių kategorijų asmens duomenimis.

9. Duomenų tvarkytojai, sužinoję apie galimą asmens duomenų saugumo pažeidimą:

9.1. Nedelsdami, sutartyje nustatytu terminu, o jeigu toks terminas nenustatytas – ne vėliau kaip per 24 valandas nuo sužinojimo apie galimą asmens duomenų saugumo pažeidimą, informuoja PAP ir teisininką elektroninio pašto adresu teisininkas@panevezioautobusai.lt, pateikdami visą tuo metu turimą informaciją. Jeigu vėliau paaiškėja papildomų aplinkybių, ši informacija pateikiama nedelsiant. Pavėluoto pranešimo atveju nurodomos vėlavimo priežastys;

9.2. nedelsdami imasi priemonių asmens duomenų saugumo pažeidimui pašalinti ir (ar) jo pasekmėms sumažinti ar pašalinti, siekdami atkurti padėtį, kuri buvo prieš asmens duomenų saugumo pažeidimą.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

10. Asmens duomenų saugumo pažeidimai (toliau – pažeidimai), atsižvelgiant į pagal šio Tvarkos aprašo 15 ir 16 punktus įvertintą pavojų fizinių asmenų teisėms ir laisvėms, klasifikuojami:

10.1. Didelės rizikos pažeidimas – pažeidimas, dėl kurio tikėtinas didelis pavojus fizinių asmenų teisėms ir laisvėms;

10.2. Vidutinės rizikos pažeidimas – pažeidimas, dėl kurio tikėtinas pavojus fizinių asmenų teisėms ir laisvėms, tačiau nenustatytas didelis pavojus;

10.3. Žemos rizikos pažeidimas – pažeidimas, dėl kurio mažai tikėtinas pavojus fizinių asmenų teisėms ir laisvėms.

10.4. pažeidimo rizikos lygis nustatomas pagal šio Tvarkos aprašo 15 ir 16 punktuose numatytą rizikos vertinimą ir peržiūrimas paaiškėjus naujoms aplinkybėms. Apie didelės rizikos pažeidimus pranešama VDAI ir duomenų subjektams, išskyrus šio Tvarkos aprašo 34 punkte numatytus atvejus; apie vidutinės rizikos pažeidimus – VDAI; žemos rizikos pažeidimai registruojami žurnale. Kilus pagrįstų abejonių dėl rizikos lygio, vadovaujamasi šio Tvarkos aprašo 26 punktu.

11. Teisininkas, gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą šio Tvarkos aprašo 7 punkte nurodytais būdais, įskaitant darbuotojų pranešimus pagal 8 punktą ir duomenų tvarkytojų pranešimus pagal 9.1 papunktį, privalo:

11.1. Nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pirmosios informacijos apie galimą asmens duomenų saugumo pažeidimą gavimo Bendrovėje, atlikti pirminį aplinkybių įvertinimą, nustatyti, ar yra skubos požymių ir ar būtini neatidėliotini veiksmai. Kai teisininkas nepasiekiamas, pirminis įvertinimas organizuojamas šio Tvarkos aprašo 8.5 papunktyje nustatyta tvarka. Išsamus pažeidimo tyrimas pradedamas ne vėliau kaip artimiausią darbo dieną, o nustačius skubos požymių – nedelsiant.

11.2. įvertinti, ar padarytas pažeidimas;

11.3. konsultuotis su duomenų apsaugos pareigūnu;

11.4. jei pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkti IT specialistus. Užtikrinti su galimu asmens duomenų saugumo pažeidimu susijusių įrodymų išsaugojimą. Iki IT specialisto ar kito kompetentingo asmens įvertinimo organizuojamas paveiktų įrenginių ir juose esančių duomenų išsaugojimas, įskaitant sistemų žurnalus. Darbuotojai savo iniciatyva neperkrauna paveiktų įrenginių, netrina jų duomenų ir nekeičia nustatymų, išskyrus pagal galiojančias instrukcijas atliekamus būtinus saugos veiksmus;

11.5. jei pažeidimas padarytas, nustatyti, kokio pobūdžio (tipo) pažeidimas padarytas, asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis, pažeidimo priežastis, pažeidimo apimtis (duomenų subjektų kategorijos ir jų skaičius), esamas ir (ar) galimas pasekmes ir žalą, padarytą duomenų subjektui (-ams), įvertinti pavojų duomenų subjekto teisėms ir laisvėms (toliau – rizika), kuris gali atsirasti dėl galimo pažeidimo, pateikti užpildytą Asmens duomenų saugumo pažeidimo tyrimo ataskaitą duomenų apsaugos pareigūnui išvadai gauti;

11.6. teikti rekomendacijas PAP darbuotojams, atsakingiems už pažeidimo ir (ar) jo pasekmių pašalinimą ir (ar) sumažinimą, ir (ar) duomenų tvarkytojui dėl tinkamų techninių ir

organizacinių priemonių, kad pažeidimas būtų išsamiai ištirtas ir jis ir (ar) jo pasekmės būtų pašalintos ir (ar) sumažintos ir pažeidimas ateityje nepasikartotų, taikymo ir (arba) pats imtis šių veiksmų;

11.7. įvertinti, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas pažeidimas;

11.8. nustatyti, ar apie pažeidimą būtina pranešti VDAI;

11.9. nustatyti, ar apie pažeidimą būtina pranešti duomenų subjektams.

12. Duomenų apsaugos pareigūnas, gavęs pranešimą, privalo:

12.1. teisininkui patarti dėl pažeidimo tyrimo ir teikti išvadas dėl pranešimo teikimo VDAI ir (ar) duomenų subjektui;

12.2. bendradarbiauti su VDAI dėl pažeidimų;

12.3. stebėti, kaip vykdomos BDAR ir Apraše nustatytos PAP pareigos, susijusios su Pažeidimų valdymu.

13. Atliekant pažeidimo tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas. Tyrimo rezultatai įforminami Asmens duomenų saugumo pažeidimo tyrimo ataskaita (tyrimo išvada) (Tvarkos aprašo 2 priedas), kurioje turi būti nurodytas pažeidimo faktas, rizikos įvertinimas, sprendimas dėl pranešimo VDAI ir (ar) duomenų subjektams bei siūlomos pažeidimo šalinimo ir prevencinės priemonės.

14. Pažeidimo tyrimo metu darbuotojai ir duomenų tvarkytojas privalo operatyviai teikti teisininkui visą jo paprašytą su pažeidimu susijusią informaciją ir dokumentus.

15. Vertinant rizikos lygį, atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

15.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis: nuo padaryto pažeidimo pobūdžio gali priklausyti pavojaus duomenų subjektams dydis;

15.2. asmens duomenų pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

15.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

15.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

15.5. nukentėjusių duomenų subjektų skaičius – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus;

15.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

16. Įvertinus šio Tvarkos aprašo 15 punkte nurodytas aplinkybes, nustatomas pažeidimo keliamo pavojaus fizinių asmenų teisėms ir laisvėms lygis – žemas, vidutinis arba didelis. Rizikos lygis nustatomas atsižvelgiant tiek į neigiamų pasekmių atsiradimo tikimybę, tiek į galimų pasekmių rimtumą. Rizikos vertinimo rezultatai ir juos pagrindžiančios aplinkybės dokumentuojami Asmens duomenų saugumo pažeidimo tyrimo ataskaitoje (Tvarkos aprašo 2 priedas).

17. Vertinant pažeidimą taip pat nustatoma, ar tai yra pakartotinis tokio pobūdžio pažeidimas.

18. Ataskaita yra pateikiama generaliniam direktoriui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

19. Jeigu įvertinus gautą informaciją nustatoma, kad nėra pažeidimo požymių arba trūksta duomenų pagrįstai manyti, jog pažeidimas įvyko, tyrimas gali būti nepradedamas. Tokį sprendimą priima teisininkas, gavęs privalomą duomenų apsaugos pareigūno išvadą. Sprendimas nepradėti tyrimo turi būti motyvuotas, įformintas tarnybiniu pranešimu ir užregistruotas žurnale, nurodant sprendimo pagrindimą. Pirminis įvertinimas ir būtini saugumo veiksmai atliekami nelaukiant DAP nuomonės.

20. Nustačius pažeidimą, teisininkas gali pateikti generaliniam direktoriui siūlymą patvirtinti priemonių planą, kuriame numatomos techninės, organizacinės ir administracinės priemonės, skirtos pažeidimo pasekmėms pašalinti ir užkirsti kelią analogiškų pažeidimų pasikartojimui. Priemonių plane numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl pažeidimo pašalinimo, paskirti atsakingi vykdytojai ir nustatyti priemonių įgyvendinimo terminus. Priemonių planas rengiamas pagal Tvarkos aprašo 4 priede nustatytą formą.

21. Sprendžiant pažeidimo pašalinimo klausimą, bei tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą. Priklausomai nuo konkrečių pažeidimo aplinkybių, turėtų būti atlikti tokie veiksmai, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo / mobilaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius, jeigu jie tapo žinomi tretiesiems asmenims; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

Jeigu pažeidimas susijęs su vaizdo stebėjimo sistema, atsižvelgiant į konkrečias aplinkybes, gali būti imamasi šių priemonių: apribojama neteisėta prieiga prie vaizdo stebėjimo sistemos, sustabdomas neteisėtas vaizdo įrašų eksportavimas ar kopijavimas, imamasi veiksmų prarastai laikmenai surasti ir galimai neteisėtai prieigai užkirsti, išsaugomi sistemos žurnalai ir kiti su pažeidimu susiję įrodymai, įvertinamos prarastų vaizdo įrašų atkūrimo galimybės. Techniniai veiksmai atliekami pasitelkiant kompetentingus specialistus, užtikrinant, kad nebūtų sunaikinti pažeidimo tyrimui reikšmingi duomenys.

22. Siekiant apriboti ar sustabdyti pažeidimą, papildomai surenkami ir dokumentuojami duomenys bei įrodymai apie įvykusį incidentą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.).

23. Rengiant priemonių planą turi būti įvertintos pažeidimą lėmusios priežastys bei nustatyti konkretūs veiksmai šioms priežastims pašalinti.

IV SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

24. Kai PAP sužino apie įvykusį asmens duomenų saugumo pažeidimą, dėl kurio gali kilti pavojus fizinių asmenų teisėms ir laisvėms, apie pažeidimą VDAI pranešama nedelsiant ir, jei įmanoma, ne vėliau kaip per 72 valandas nuo sužinojimo apie pažeidimą momento. Galutinio pažeidimo tyrimo užbaigimas nėra būtina pranešimo VDAI sąlyga. Jeigu per šį terminą neįmanoma surinkti visos reikalingos informacijos, ji teikiama etapais šio Tvarkos aprašo 28 punkte nustatyta tvarka. Pranešimo pateikimą organizuoja teisininkas.

25. VDAI informuojama Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto VDAI direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“ (su visais aktualiais pakeitimais), nustatyta tvarka ir sąlygomis.

26. Jeigu atlikus šio Tvarkos aprašo 15 ir 16 punktuose numatytą rizikos vertinimą išlieka pagrįstų abejonių, ar pažeidimas gali sukelti pavojų fizinių asmenų teisėms ir laisvėms, ir nėra pagrindo daryti išvados, kad toks pavojus mažai tikėtinas, apie pažeidimą pranešama VDAI šio Tvarkos aprašo 24 punkte nustatytu terminu ir 25 nurodyta tvarka. Jeigu pranešimo teikimo metu nėra visos reikalingos informacijos, papildoma informacija teikiama VDAI šio Tvarkos aprašo 28 punkte nustatyta tvarka.

27. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie pažeidimą VDAI pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., pamesta USB atmintinė, kurioje saugomi asmens duomenys, užšifruoti taikant pažangų algoritmą – jeigu yra atsarginės duomenų kopijos ir nėra pavojaus šifro saugumui, apie tokį saugumo pažeidimą pranešti VDAI nereikia, tačiau jei vėliau paaiškėja, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus bus vertinamas iš naujo ir apie tokį pažeidimą reikės pranešti VDAI).

28. Tuo atveju, kai priklausomai nuo pažeidimo pobūdžio būtina atlikti išsamesnį tyrimą, nustatyti visus svarbius faktus, susijusius su pažeidimu, ir per 72 valandas dėl objektyvių priežasčių nėra įmanoma ištirti padarytą pažeidimą, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.

29. Jeigu po pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai pažeidimo nebuvo, apie tai nedelsiant informuojama VDAI.

30. Tuo atveju, kai yra įtariama, kad pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, teisės aktų, reguliuojančių tokios informacijos teikimą, nustatyta tvarka.

V SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

31. Nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, PAP nepagrįstai nedelsdama apie pažeidimą praneša duomenų subjektams, kurių teisėms ir laisvėms gali kilti toks pavojus, išskyrus šio Tvarkos aprašo 34 punkte nustatytus atvejus. Pranešimo pateikimą organizuoja teisininkas.

32. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu arba elektroniniu paštu arba trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui teikiamas atskirai nuo kitos komunikacijos (pvz., naujienlaiškių ar bendrinių informacinių pranešimų).

33. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

33.1. asmens duomenų saugumo pažeidimo pobūdžio ir tikėtinų pažeidimo pasekmių aprašymas;

33.2. priemonių, kurių ėmėsi PAP, kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas;

33.3. teisininko, duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

33.4. kita reikšminga informacija, susijusi su pažeidimu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

34. Pranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektams teikti nereikia, jeigu:

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

34.2. iš karto po pažeidimo PAP ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

34.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi. Tokiu atveju gali būti taikomos viešo informavimo priemonės (pvz., paskelbimas interneto svetainėje, keli informavimo kanalai), užtikrinant, kad duomenų subjektai būtų informuoti efektyviai.

35. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą duomenų subjektui pranešti nereikia, tačiau po kurio laiko situacija pasikeitė, pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą, – duomenų bazėje esantys asmens duomenys užšifruojami. Jei atlikus tyrimą paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik VDAI, tačiau jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, saugumo pažeidimo keliamas pavojus bus

vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas saugumo pažeidimo pasekmes reikia apie jį pranešti duomenų subjektams).

36. Informavimas duomenų subjektams gali būti atidėtas, jei tai būtina tam, kad nebūtų pakenkta teisėsaugos institucijų veiksmams.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

37. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų žurnale (toliau – Asmens duomenų saugumo pažeidimų registravimo žurnalas) (Tvarkos aprašo 3 priedas).

38. Informacija apie pažeidimą registruojama nedelsiant, kai tik nustatomas pažeidimo faktas ir įvertinama rizika, bet ne vėliau kaip per 5 darbo dienas.

39. Registruojami ir dokumentuojami ne tik įvykę pažeidimai, bet ir potencialūs pažeidimai („beveik pažeidimai“), kurie galėjo sukelti asmens duomenų saugumo incidentą.

40. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

40.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

40.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

40.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

40.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

40.5. informacija apie pranešimą ar nepranešimą VDAI:

40.5.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

40.5.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;

40.6. informacija apie pranešimą ar nepranešimą duomenų subjektui (subjektams):

40.6.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

40.6.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

40.7. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

41. Už Asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą, tvarkymą ir saugojimą atsakingas teisininkas. Žurnalo įrašai ir su konkrečiu įvykiu susiję dokumentai saugomi 2 metus nuo pažeidimo tyrimo pabaigos, o kai tyrimas neatliekamas – nuo sprendimo užbaigti įvykio vertinimą įforminimo dienos. Pasibaigus šiam terminui, dokumentai sunaikinami, išskyrus atvejus, kai jų saugojimo terminas pratęsiamas Asmens duomenų tvarkymo taisyklių 16 ir 17 punktuose

nustatytais pagrindais. Pratęsus saugojimo terminą, dokumentai saugomi tik tol, kol išlieka jų saugojimo būtinybę pagrindžiančios aplinkybės.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. PAP darbuotojai, pažeidę šio Tvarkos aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka. Jei pažeidimas susijęs su darbuotojo veiksmais ar neveikimu, gali būti inicijuojamas vidinis tyrimas dėl darbo pareigų pažeidimo.

43. PAP užtikrina, kad darbuotojai būtų reguliariai mokomi atpažinti ir tinkamai valdyti asmens duomenų saugumo pažeidimus.

44. Aprašas peržiūrimas periodiškai, ne rečiau kaip kartą per metus, arba įvykus organizaciniams, sisteminiams ar kitiems pokyčiams arba pasikeitus teisės aktų reikalavimams. Už peržiūrą atsakingas teisininkas.

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
1 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO PRANEŠIMAS

Pranešimo data ir laikas: _____
Pranešimo registracijos Nr. _____
Pranešėjas: _____
Vardas, pavardė _____
Pareigos _____
Kontaktinis telefono numeris _____

INFORMACIJA APIE PIRMINĮ PRANEŠIMĄ

Duomenys	**Pildoma informacija**
Kam apie galimą pažeidimą pranešta žodžiu (pareigos, vardas ir pavardė, jei žinoma)	
Pranešimo data	
Pranešimo laikas	val. min.
Pranešimo būdas	Telefonu / tiesiogiai

1. **Kada pastebėjote galimą pažeidimą?**

   _____

2. **Kaip sužinojote apie pažeidimą?**

   ☐ Pats pastebėjau
   ☐ Pranešė kolega
   ☐ Pranešė klientas / keleivis
   ☐ Iš sistemos (pvz., pranešimas, klaida)
   ☐ Kita _____

3. **Kur įvyko arba buvo pastebėtas pažeidimas?**

_____

4. **Aprašykite, kas įvyko.**

_____

_____

_____

5. **Ar pažeidimas vis dar vyksta**?
   ☐ Taip
   ☐ Ne
   ☐ Nežinau

6. **Apytikslis paveiktų duomenų subjektų skaičius:**
   ☐ 1–5

☐ 6–50
☐ 51–500
☐ >500
☐ Nežinau

7. **Kokie asmens duomenys, Jūsų nuomone, galėjo būti paveikti?**
   ☐ Darbuotojų duomenys
   ☐ Keleivių duomenys
   ☐ Kandidatų į darbo vietą duomenys
   ☐ Vaizdo stebėjimo duomenys
   ☐ GPS duomenys
   ☐ Prisijungimo / IT duomenys (slaptažodžiai ir pan.)
   ☐ Nežinau
   ☐ Kita _____
8. **Ar buvo imtasi veiksmų situacijai suvaldyti (pvz., laiško atšaukimas, slaptažodžio keitimas) ?**

   ☐ Taip
   ☐ Ne
   Jei taip, kokių?

_____

_____

9. **Papildoma informacija**

_____

_____

Pranešėjo parašas _____

Pastaba. Pirminis pranešimas apie galimą asmens duomenų saugumo pažeidimą pateikiamas Tvarkos aprašo 8.1 papunktyje nustatyta tvarka. Šios formos užpildymas ar pasirašymas nėra būtina pirminio pranešimo pateikimo sąlyga ir negali būti pagrindas atidėti informacijos perdavimą ar pažeidimo tyrimo pradžią. Rašytinė forma užpildoma ir pateikiama vėliau Tvarkos aprašo 8.2 papunktyje nustatyta tvarka.

_____

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
2 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA

_____ Nr. _____
(data)

1. Asmens duomenų saugumo pažeidimo aprašymas

1.1. Pažeidimo data ir laikas _____
1.2. Pažeidimo nustatymo data ir laikas _____
1.3. Pažeidimo vieta _____
1.4. Pažeidimo pobūdis (konfidencialumo / vientisumo / prieinamumo)
1.5. Nustatytos pažeidimo priežastys

_____
1.6. Pažeistų duomenų kategorijos

_____
1.7. Duomenų subjektų kategorijos (darbuotojai, kandidatai, keleiviai, pareiškėjai, vaizdo stebėjimo sistemoje užfiksuoti asmenys, kita)

_____
1.8. Apytikslis paveiktų duomenų subjektų skaičius

_____
1.9. Pranešėjas

_____
1.10. Duomenų tvarkytojas (jei taikoma)

_____
1.11. Pažeidimo klasifikacija:
☐ Žemos rizikos pažeidimas
☐ Vidutinės rizikos pažeidimas
☐ Didelės rizikos pažeidimas

1.12. Momentas, kai Bendrovė sužinojo apie įvykusį asmens duomenų saugumo pažeidimą (data ir laikas): _____
1.13. Ar pažeidimas buvo sustabdytas?
☐ Taip
☐ Ne
☐ Nežinoma
1.14. Pirmosios informacijos apie galimą asmens duomenų saugumo pažeidimą gavimo Bendrovėje data ir laikas: _____
1.15. Asmens duomenų saugumo pažeidimo tyrimo pradžios data ir laikas: _____

2. Asmens duomenų saugumo pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms įvertinimas

2.1. Specifiniai fizinių asmenų, kurių asmens duomenų saugumas buvo pažeistas, ypatumai (vaikai, asmenys su negalia ir kt.):

2.2. Galimybė identifikuoti fizinį asmenį (pvz., iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užšifruoti, anonimizuoti, arba iki saugumo pažeidimo asmens duomenims šifravimas nebuvo taikomas ir kt.):

2.3. Ar pažeisti asmens duomenys buvo apsaugoti (pvz., šifravimas, pseudonimizavimas)?

2.4. Kas galėjo gauti prieigą prie asmens duomenų, kurių saugumas pažeistas?

2.5. Ar buvo kokių kitų įvykių ar aplinkybių, turėjusių poveikį asmens duomenų saugumo pažeidimo padarymui?

2.6. Kokia žala padaryta fiziniams asmenims (duomenų subjektams)?

2.7. Galimos asmens duomenų saugumo pažeidimo pasekmės:

2.8. Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis:

☐ Žemas rizikos lygis

☐ Vidutinis rizikos lygis

☐ Didelis rizikos lygis

2.9. Ar nustatyta, kad tai pakartotinis tokio pobūdžio pažeidimas?

☐ Taip

☐ Ne

Jei taip, nurodyti ankstesnio pažeidimo datą ir numerį.

2.10. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?

2.11. Kokios taikytos priemonės, siekiant sumažinti neigiamą poveikį duomenų subjektams?

2.12. Duomenų apsaugos pareigūno konsultacijos data ir laikas: _____

Konsultacijos būdas ir pateiktos rekomendacijos (arba nuoroda į atskirai pateiktą DAP išvadą):

3. Pranešimų apie asmens duomenų saugumo pažeidimą pateikimas

3.1. **Pranešimas Valstybinei duomenų apsaugos inspekcijai (VDAI)**

Momentas, kai Bendrovė sužinojo apie įvykusį asmens duomenų saugumo pažeidimą (pagal šios ataskaitos 1.12 papunktį):

Data _____ Laikas _____ val. _____ min.
BDAR 33 straipsnio 1 dalyje nustatyto 72 valandų termino pabaiga:
Data _____ Laikas _____ val. _____ min.
Ar apie asmens duomenų saugumo pažeidimą pranešta VDAI?
☐ Taip
- Pranešimo pateikimo data ir laikas: _____
- Pranešimo registracijos numeris (jeigu suteiktas): _____

☐ Ne
Nepranešimo VDAI priežastys (nurodomi rizikos vertinimu pagrįsti motyvai):
_____
Ar pranešimas VDAI pateiktas etapais?
☐ Taip
☐ Ne
Jeigu taip, nurodoma papildomos informacijos pateikimo data ir numeris (jeigu suteiktas):
_____
Ar pirminis pranešimas VDAI pateiktas vėliau nei per 72 valandas nuo sužinojimo apie pažeidimą momento?
☐ Taip
☐ Ne
☐ Netaikoma (apie pažeidimą pranešti VDAI neprivaloma)
Jeigu taip, nurodomos vėlavimo priežastys:
_____
3.2. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą?
☐ Taip
Pranešimo duomenų subjektui data ____ numeris (jeigu pranešimas užregistruotas)
Pranešimo duomenų subjektui būdas (pažymėti tinkamą (-us):
☐ paštu
☐ elektroniniu paštu
☐ trumpąja žinute (SMS)
☐ kitais būdais
Informuotų duomenų subjektų skaičius
Pranešimo duomenų subjektui turinys:

_____
☐ Ne (nurodomos nepranešimo duomenų subjektui priežastys):
_____
☐ Apie asmens duomenų saugumo pažeidimą duomenų subjektams pranešta nepagrįstai uždelsus (nurodomos pranešimo pateikimo uždelsimo priežastys):
_____
☐ Apie saugumo pažeidimą pranešta viešai (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta):

3.3. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jeigu taip, nurodoma rašto data ir numeris):

4. Taikytos ir planuojamos priemonės

Priemonė	Esama / įgyvendinta	Planuojama	Terminas

5. Tyrimo išvada

Sprendimas priimamas remiantis šios ataskaitos 1–3 punktuose pateikta informacija. Sprendimą priima atsakingas asmuo, įvertinęs šios ataskaitos duomenis.

☐ Pažeidimas nepasitvirtino

☐ Nustatytas pažeidimas

Rizikos lygis nustatytas pagal šios ataskaitos 2.8 punktą.

☐ Pranešti VDAI
☐ Nepranešti VDAI
☐ Pranešti duomenų subjektams
☐ Nepranešti duomenų subjektams

Sprendimo motyvai _____
☐ Rengti priemonių planą (4 priedas)

☐ Priemonių planas nereikalingas

Apie priimtą sprendimą informuotas generalinis direktorius.

Atsakingas asmuo:

_____ _____ _____
(pareigos) (parašas) (vardas ir pavardė)

Duomenų apsaugos pareigūno išvada pateikta _____
(data)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

UAB „Panevėžio autobusų parkas“ | Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo 3 priedas

Vienas įvykis – viena eilutė. Datą ir laiką įrašykite į nurodytus laukus. „Beveik pažeidimas“ žymimas atskirai; išsamūs įrodymai saugomi tyrimo dokumentuose.

REGISTRAVIMAS IR ĮVYKIO APLINKYBĖS								PAŽEIDIMO KLASIFIKAVIMAS IR RIZIKA			PRIEMONĖS IR TYRIMAS		
Eil. Nr.	Registravimo data	Sužinojimo apie pažeidimą momentas (data ir laikas)	Pažeidimo nustatymo data, laikas ir vieta	Pranešęs darbuotojas ar duomenų tvarkytojas (vardas, pavardė, pareigos / pavadinimas)	Pažeidimo padarymo data ir vieta	Pažeidimo pobūdis, priežastys ir kitos aplinkybės	Žyma „beveik pažeidimas“	Pažeidimo klasė / rizikos lygis	Duomenų subjektų kategorijos ir apytikslis skaičius	Asmens duomenų kategorijos ir apytikslis skaičius	Tikėtinos pasekmės ir pavojus fizinių asmenų teisėms ir laisvėms	Priemonės pažeidimui pašalinti ir (ar) padariniams sumažinti	Tyrimo ataskaitos Nr.

PRANEŠIMAS VDAI				DUOMENŲ SUBJEKTAI IR KITA			
Ar pranešta VDAI?	Pranešimo VDAI data	Pranešimo VDAI Nr.	Pranešimo VDAI arba nepranešimo motyvai; etapinis teikimas; vėlavimo priežastys	Ar informuoti duomenų subjektai?	Duomenų subjektų informavimo data, būdas, sprendimo motyvai ir vėlavimo priežastys	Pakartotinis pažeidimas?	Kita reikšminga informacija / nuoroda į įrodymus

Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo
4 priedas

PRIEMONIŲ PLANAS

Asmens duomenų saugumo pažeidimo tyrimo ataskaitos Nr.
Pažeidimo nustatymo data: _____
Priemonių plano parengimo data: _____

Eil. Nr.	Nustatytas trūkumas / pažeidimo priežastis	Priemonė	Atsakingas asmuo	Įvykdymo terminas	Įvykdymo data	Pastabos

Priemonių plano vykdymo kontrolė
Priemonių plano įgyvendinimą kontroliuoja:

_____
(pareigos, vardas, pavardė)

Išvada dėl priemonių plano įvykdymo
☐ Visos priemonės įvykdytos.
☐ Priemonės įvykdytos iš dalies.
☐ Priemonės neįvykdytos.
Komentarai:

_____
_____
_____

Atsakingas asmuo

_____
(pareigos) (parašas) (vardas, pavardė)

Duomenų apsaugos pareigūno išvada pateikta: _____
(data, išvados numeris arba nuoroda į išvadą, jei taikoma)