UAB „LINĖJA transport“

POVEIKIO DUOMENŲ APSAUGAI VERTINIMO IŠVADA

(VAIZDO STEBĖJIMAS)

Kėdainiai

DUOMENŲ VALDYTOJO INFORMACIJA

Pavadinimas	UAB „LINĖJA transport“
Įmonės kodas	302626917
Buveinės adresas	Didžioji g. 38, Kėdainiai, Lietuva
El. paštas	info@lineja.com
Telefonas	+37065505536

Šioje poveikio duomenų apsaugai vertinimo išvadoje (toliau atitinkamai – **PDAV** ir **Išvada**) vartojamos sąvokos turi būti aiškinamos taip, kaip apibrėžtos UAB „LINĖJA transport“ (toliau – **Įmonė**) Asmens duomenų tvarkymo taisyklėse, Bendrajame duomenų apsaugos reglamente (ES) 2016/679 (toliau – **BDAR**), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (toliau – **ADTAĮ**). Šiuose teisės aktuose iš šioje Išvadoje neapibrėžti žodžiai ir jų junginiai aiškinami pagal jų bendrinę reikšmę, nebent iš konteksto matyti, kad žodis ar žodžių junginys vartojamas specialiąja – teisine, technine ar kitokia reikšme.

1. Priežastys, dėl kurių būtina atlikti poveikio duomenų apsaugai vertinimą

Planuojamos vykdyti veiklos aprašymas, jos tikslai ir planuojamos atlikti asmens duomenų tvarkymo operacijos. Paaiškinimas, kodėl būtina atlikti poveikio duomenų apsaugai vertinimą. Jei reikia, prie išvados pridedami susiję dokumentai.
1.1. Ši Išvada, susijusi su Įmonės teritorijoje ir patalpose vykdoma vaizdo stebėsena, yra rengiama atsižvelgiant į BDAR 35 straipsnio, 75 ir 90 konstatuojamųjų dalių nuostatas, Valstybinės duomenų apsaugos inspekcijos (toliau – **VDAI**) reikalavimus, išaiškinimus ir konsultacijas bei kitų priežiūros institucijų išaiškinimus.
1.2. BDAR 75 konstatuojamoji dalis numato konkrečius pavojus, kurie gali kilti dėl asmens duomenų tvarkymo ir sukelti tam tikras pasekmes duomenų subjektui, kurio duomenys yra tvarkomi. PDAV, visų pirma, yra skirtas įsitikinti, kokios grėsmės gali kilti dėl atliekamo asmens duomenų tvarkymo.
1.3. BDAR 90 konstatuojamoji dalis numato, jog duomenų valdytojas turi įvertinti tikimybę ir rimtumą konkrečiam pavojui atsirasti. Tam, kad tai padarytų, duomenų valdytojas privalo atsižvelgti į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus bei pavojaus šaltinius. Tai galima įgyvendinti atlikus PDAV. PDAV pirmiausia turėtų būti nurodytos numatomos apsaugos priemonės ir mechanizmai, kuriais tas pavojus būtų valdomas (sumažinamas, perkeliamas ar išvengiamas), užtikrinama asmens duomenų apsauga ir įrodoma atitiktis BDAR.
1.4. BDAR 35 straipsnio 1 dalyje nustatyta, kad PDAV turi būti atliktas, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus.
1.5. Įmonė vaizdo stebėseną vykdo tik Įmonės patalpų, esančių registruotos buveinės adresu, prieigose, pačios Įmonės patalpos nėra stebimos. Į vaizdo stebėjimo lauką patenka Įmonės darbuotojai tiek, kiek turi praeiti pro vaizdo stebėjimo lauką, siekiant patekti į Įmonės patalpas, kuriose atlieka savo darbo funkcijas. Dėl tarp darbdavio ir darbuotojų esančio galios disbalanso, darbuotojai pagal BDAR paprastai yra laikomi pažeidžiamais asmenimis. Pažeidžiamų asmenų asmens duomenų tvarkymas didina duomenų tvarkymo pavojingumą.

1.6. BDAR 35 straipsnio 4 dalis numato, jog priežiūros institucija, šiuo atveju – VDAI, sudaro ir viešai paskelbia sąrašą duomenų tvarkymo operacijų, kurioms pagal BDAR 35 straipsnio 1 dalį taikomas reikalavimas atlikti PDAV. Remiantis VDAI direktoriaus 2019 m. kovo 14 d. įsakymo Nr. 1T-35 (1.12.E) Dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašo patvirtinimo (toliau – **Įsakymas**) 10 punktu, šiuo atveju PDAV atlikti būtina (vaizdo duomenų tvarkymas darbo vietoje ir (ar) duomenų valdytojo patalpose ar teritorijose, kuriose dirba jo darbuotojai).

1.7. PDAV atliekamas dėl vaizdo stebėjimo, vykdomo Įmonės turto ir asmenų (tiek darbuotojų, tiek kitų asmenų, kurie lankosi Įmonė) saugumo, įrodymų apie pažeidimus rinkimo ir Įmonės teisių gynimo tikslais.

2. Asmens duomenų tvarkymo aprašymas

Aprašomi asmens duomenų rinkimo, naudojimo, saugojimo ir naikinimo veiksmai, nurodoma, iš kokių šaltinių bus renkami asmens duomenys, kam bus teikiami (esant poreikiui pateikiama asmens duomenų tvarkymo veiksmų schemą). Aprašoma, kokie asmens duomenų tvarkymo veiksmai gali kelti pavojų fizinių asmenų teisėms ir laisvėms.

2.1. **Įmonės Asmens duomenų tvarkymo operacijų teisinis pagrindas.** Asmens duomenys PDAV 1.5 punkte nurodytu tikslu yra tvarkomi teisėto intereso (BDAR 6 straipsnio 1 dalies f punktas) pagrindu. Teisėto intereso pagrindimas yra pateiktas Išvados 4 dalyje.

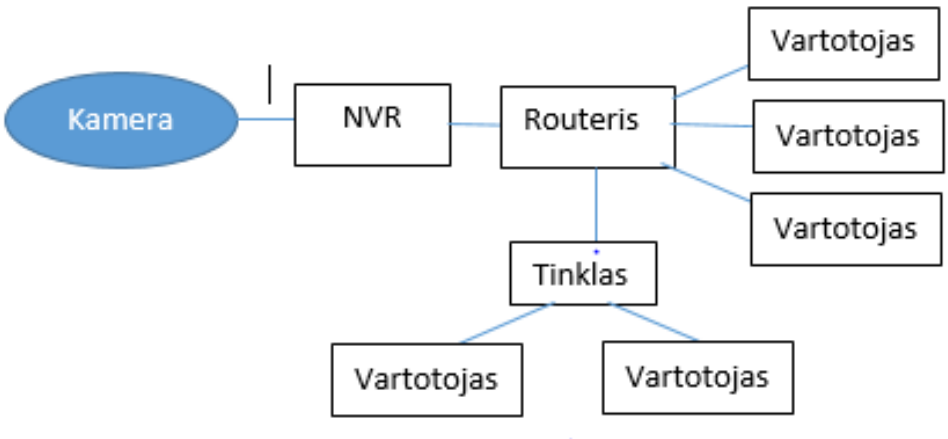
2.2. **Asmens duomenų rinkimo, naudojimo, saugojimo ir naikinimo veiksmai:**

2.2.1. Asmens duomenys yra surenkami naudojant Įmonės patalpų prieigose įrengtas vaizdo kameras.

2.2.2. Vaizdas įrašomas naudojant gamintojo Hik-vision IP kameras. Vaizdo kameros fiksuoja šiuos asmens duomenis: atvaizdas, atliekami veiksmai, turimi daiktai. Garsas nėra įrašomas. Nenaudojamos jokios kitos išmaniosios technologijos (biometrinio atpažinimo ir pan.).

2.2.3. Vaizdo duomenys saugomi vaizdo įrašymo įrenginyje (NVR). NVR įrenginys yra saugomas rakinamoje spintoje. Iš vaizdo stebėjimo įrenginių vaizdo duomenys lokaliu tinklu (LAN) perduodami vaizdo įrašymo įrenginius NVR, todėl išorinio tinklo (WAN) nepasiekia.

2.2.4. Žemiau pateikiama schema kaip vaizdo įrašai yra išsaugomi, sąveikauja tinkle:



2.2.5. Prieiga prie vaizdo duomenų nėra galima per mobiliuosius telefonus, vaizdo duomenis gali peržiūrėti tik Įmonės vadovas, prisijungęs prie NVR įrenginio.

2.2.6. Atsarginės vaizdo duomenų kopijos nėra daromos, vaizdo įrašai yra saugomi tik NVR įrenginiuose.

2.2.7. Vaizdo duomenys saugomi 7 dienas ir pasibaigus saugojimo terminai automatiniu būdu sunaikinami. Kai tam tikri vaizdo duomenys yra išsaugomi atskirai (tiriant pažeidimus ir pan.), jie pasibaigus jų saugojimo terminui yra sunaikinami rankiniu būdu.

2.2.8. Siekdama užtikrinti vaizdo duomenų apsaugą, Įmonė įgyvendina organizacines (darbuotojų supažindinimas su dokumentais, reglamentuojančiais duomenų saugą, dokumentų, reglamentuojančių duomenų saugą, periodinis peržiūrėjimas, prireikus atnaujinimas, kontroliuojamas jų vykdymas; atsakingų darbuotojų apmokymas tvarkyti duomenis ir pan.); techninės ir programinės įrangos apsaugos (vaizdo stebėjimo sistemos ir įrenginių, darbo vietų, Įmonės patalpų priežiūra, operacinių sistemų apsauga, apsauga nuo kompiuterinių virusų, slaptažodžiai ir kt.) priemones ir kitas asmens duomenų saugumo priemones, nurodytas Įmonės Duomenų saugumo politikoje.

2.3. **Duomenų gavėjai:** Vaizdo duomenys gali būti perduodami teisėsaugos institucijoms, teismams, advokatams (kaip atskiram duomenų valdytojui).

2.4. **Pavojai, galintys kilti**: nenumatoma, kad pats asmens duomenų tvarkymas (jei atliekamas tinkamai) keltų pavojus fizinių asmenų teisėms ir laisvėms, pavojus gali kilti nebent įvykus asmens duomenų saugumo pažeidimui, jei prieigą prie asmens duomenų gautų tokios teisės neturintys asmenys, asmens duomenys būtų paviešinti ir pan. Pavojų vertinimas ir priemonės jiems suvaldyti nurodytos Išvados 5 ir 6 dalyse.

Aprašomas tvarkymo mastas: kokių kategorijų Asmens duomenys bus tvarkomi; ar bus tvarkomi Specialių kategorijų Asmens duomenys arba duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas; kiek duomenų, kaip dažnai bus renkama ir naudojama; kaip ilgai bus saugomi Asmens duomenys; nurodomas apytikslis duomenų subjektų skaičius bei geografinė duomenų tvarkymo aprėptis.

2.5. **Specialių kategorijų asmens duomenys arba duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas.** Įmonė PDAV 1.5 p. nurodytu tikslu specialių kategorijų asmens duomenų arba duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas nerenka ir tokių duomenų netvarko.

2.6. **Duomenų subjektų asmens duomenų tvarkymo metodas.**

Vaizdo stebėjimo kameros yra sumontuotos tik Įmonės patalpų prieigose, iš išorės, lauke. Įmonės vidaus patalpos, taip pat konkrečių darbuotojų darbo vietos nėra stebimos. Vaizdo stebėjimo kameros nėra sumontuotos patalpose, kurios asmenys tikėtųsi absoliutaus privatumo, pavyzdžiui, persirengimo vietose, tualetuose, poilsio patalpose.

Įmonės teritorijos, patalpų nuolatinė stebėsena realiu laiku paprastai nėra vykdoma, vaizdo duomenys yra peržiūrimi tuo atveju, kai tai yra reikalinga dėl tikslų, dėl kurių vaizdo stebėjimas Įmonėje yra vykdomas.

Konkretūs peržiūros atvejai nėra fiksuojami. Reikalavimas prisijungiant prie sistemos ar prieš peržiūrint konkretų vaizdo įrašą nurodyti tos konkrečios peržiūros tikslą nėra taikomas.

2.7. **Asmens duomenų saugojimo terminai:**

Vaizdo duomenys saugomi 7 dienas. Vaizdo duomenys Įmonės vadovo sprendimu gali būti saugomi ilgesnį laiko tarpą, jei yra pagrindo manyti, kad vaizdo duomenų gali prireikti tiriant Įmonės patalpų prieigose ar patalpose įvykdytą nusikalstamą veiką ar kitokį incidentą, ar Įmonei žalos sukėlusį kitokį įvykį. Tokiu atveju vaizdo duomenys saugomi iki bus priimtas atitinkamas galutinis teisėsaugos institucijų ar teismo sprendimas, susijęs su nusikalstama veika, ar kitoks asmenų, tiriančių/nagrinėjančių incidentą, ar kitų asmenų, tiriančių/nagrinėjančių Įmonei žalos sukėlusį įvykį, sprendimas ar išvada.

Aprašomas asmens duomenų tvarkymo pobūdis: kokio pobūdžio santykiai sieja Įmonę su duomenų subjektais; ar duomenų subjektai turės galimybę kontroliuoti duomenų tvarkymą; ar duomenų subjektai gali numatyti, kad jų asmens duomenys bus tvarkomi šiuo būdu; ar bus tvarkomi vaikų ir kitų pažeidžiamų asmenų duomenys; įvertinama, ar toks duomenų tvarkymas yra saugus; ar duomenų tvarkymo technologijos yra naujos, ar egzistuojančios technologijos bus panaudotos kitokiu būdu; koks yra technologijų išsivystymo lygis šioje srityje; ar yra kokių nors visuomeninių ar pan. problemų ar klausimų, į kuriuos būtina atsižvelgti; nurodoma, ar yra įsipareigojimas laikytis patvirtinto elgesio kodekso ar patvirtinto sertifikavimo mechanizmo.

2.8. **Įmonę ir duomenų subjektą siejantis santykis:**

Į vaizdo stebėjimo lauką patenka Įmonės darbuotojai, taip pat bet kurie kiti asmenys, kai lankosi Įmonės patalpose ar jų prieigose (Įmonės klientai, tiekėjų darbuotojai, kiti Įmonės patalpose ar jų prieigose apsilankę fiziniai asmenys). Tarp Įmonės (duomenų valdytojo) ir darbuotojų egzistuoja galios disbalansas, todėl darbuotojai laikytini labiau pažeidžiamais duomenų subjektais.

2.9. **Duomenų subjektai turi galimybę kontroliuoti jų asmens duomenų tvarkymą, tačiau ši galimybė yra / gali būti apribota dėl netinkamo informavimo apie atliekamą vaizdo stebėseną:**

1) Vadovaujantis ADTAĮ 5 straipsnio 3 dalimi, darbuotojai apie vykdomą vaizdo stebėseną turi būti informuojami pasirašytinai ar kitu informavimo faktą įrodančiu būdu. Įmonės darbuotojai yra supažindinami su vaizdo stebėjimo vykdymu Įmonėje, juos pasirašytinai supažindinant su Asmens duomenų tvarkymo taisyklėmis ir jų priedais, įskaitant Vaizdo duomenų tvarkymo taisyklėmis.

2) Išorės duomenų subjektai (Įmonės klientai, tiekėjų darbuotojai, kiti Įmonės patalpose ar jų prieigose apsilankę fiziniai asmenys) apie vaizdo stebėjimą informuojami informacine lentele. Įmonės Vaizdo duomenų tvarkymo taisyklėse nustatyta, kad prieš patenkant į vaizdo stebėjimo lauką, pakabina specialius ženklus (lenteles), informuojančius apie vykdomą vaizdo stebėjimą. Specialiame ženkle (lentelėje) yra nurodoma ši informacija: (i) kokiais tikslais ir teisiniu pagrindu vykdomas vaizdo stebėjimas; (ii) nurodomas vaizdo stebėjimo simbolis (vaizdo kamera); (iii) nurodomas vaizdo duomenų valdytojo (Įmonės) pilnas pavadinimas, juridinio asmens kodas, adresas, el. pašto adresas; (iv) nuoroda, kad informaciją apie duomenų tvarkymą teikiama nurodytais kontaktais.

3) Duomenų subjektai, pateikę prašymą, turi teisę susipažinti su tvarkomais asmens duomenimis, kiek tai leidžia Įmonės naudojama techninė ir programinė įranga ir kiek tai nepažeidžia trečiųjų asmenų teisių ir laisvių. Įmonės Vaizdo duomenų tvarkymo taisyklėse ir Duomenų subjektų teisių įgyvendinimo tvarkoje yra reglamentuota duomenų subjektų teisių įgyvendinimo tvarka.

4) „Teisė būti užmirštam“ gali būti įgyvendinama pagal atskirus prašymus. Ši teisė įgyvendinama, kai vaizdo duomenys buvo tvarkomi nesilaikant teisės aktų ir, jie nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami, arba vaizdo duomenys turi būti ištrinti laikantis teisės aktais nustatytos prievolės. Konkrečiu duomenų subjekto prašymu visi jo vaizdo duomenys gali būti pašalinti iš Įmonės turimų laikmenų, tačiau tik su sąlyga, kad toks vaizdo duomenų pašalinimas nepakenks Įmonės, Įmonės darbuotojų ar kitų duomenų subjektų teisėms ar interesams, kai vaizdo duomenys yra reikalingi apsaugoti išvardintų asmenų teises ir interesus. Taip pat Įmonė neprivalo ištrinti asmens duomenų, kai duomenys reikalingi siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus. Duomenų subjektas informuojamas apie vaizdo duomenų ištrynimą.

5) Duomenų subjektai gali pasinaudoti savo teise į savo asmens duomenų kopijos gavimą, jei pateikiamas rašytinis prašymas, o pateikusiojo duomenų subjekto asmenybė patvirtinama, šio duomenų subjekto asmens duomenys gali būti pateikti duomenų subjektui, nepateikiant trečiųjų asmenų duomenų.

6) Teisė ištaisyti duomenis gali būti įgyvendinama BDAR nustatyta tvarka, jeigu tai techniškai įmanoma. Įprastai, atsižvelgiant į asmens duomenų tvarkymo pobūdį, neturėtų pasitaikyti netikslių duomenų, kuriuos reikėtų taisyti, tačiau gali pasitaikyti, kai įrenginiuose bus nustatyta netinkamas laikas, ko pasėkoje, gali būti tvarkomi klaidingi duomenys apie tai,

kada asmuo lankėsi ar atliko kokius nors veiksmus užfiksuotame vaizdo įraše, tai labiau būtų siejama su vaizdo duomenų metaduomenimis.

7) Teisė nesutikti įgyvendinama BDAR, Įmonės Vaizdo duomenų tvarkymo taisyklėse ir Duomenų subjektų teisių įgyvendinimo tvarkoje nustatyta tvarka. Asmeniui išreiškus prieštaravimą asmens duomenų tvarkymui, Įmonė nebetvarkys duomenų subjekto vaizdo duomenų, išskyrus atvejus, kai įrodys, kad duomenys tvarkomi dėl įtikinamų teisėtų priežasčių, kurios yra viršesnės už duomenų subjekto interesus, teises ir laisves, arba siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus.

8) Duomenų subjektams yra suteikiama galimybė apriboti savo duomenų tvarkymą BDAR, Įmonės Vaizdo duomenų tvarkymo taisyklėse ir Duomenų subjektų teisių įgyvendinimo tvarkoje nustatyta tvarka. Įmonė minėtuose dokumentuose yra numačiusi, kad apribojus duomenų subjekto vaizdo tvarkymo veiksmus, vaizdo duomenys, kurių tvarkymo veiksmai apriboti, turi būti saugomi tol, kol bus ištaisyti ar sunaikinti (duomenų subjekto prašymu arba pasibaigus vaizdo duomenų saugojimo terminui). Kiti tvarkymo veiksmai su tokiais asmens duomenimis gali būti atliekami tik:
   (i) turint tikslą pareikšti, vykdyti arba apginti teisinius reikalavimus;
   (ii) jei duomenų subjektas duoda sutikimą toliau tvarkyti savo vaizdo duomenis;
   (iii) jei reikia apsaugoti trečiųjų asmenų teises ar teisėtus interesus.

2.10. **Duomenų subjektai iš esmės gali numatyti, kad jų asmens duomenys bus tvarkomi.** Prieš patenkant į Įmonės vykdomo vaizdo stebėjimo lauką yra informacinės lentelės, informuojančios apie atliekamą vaizdo stebėseną, darbuotojai yra supažindinti su vaizdo stebėjimu pasirašytinai, todėl vaizdo stebėjimo vykdymas nėra duomenų subjektams netikėtas.

2.11. Vaizdo stebėjimo kameros yra pastebimoje, matomoje vietoje. Įmonės patalpų prieigose yra įrengtos standartinės vaizdo stebėjimo kameros, nėra naudojamos technologijos, kurios duomenų subjektams būtų netikėtos (pavyzdžiui, biometrinio atpažinimo ir pan.).

2.12. Vaizdo stebėsena nėra nukreipta į kokios nors konkrečios asmenų grupės (vaikų ar kitų pažeidžiamų asmenų) stebėjimą. Nors vaizdo stebėjimo laukas apima ir Įmonės darbuotojus, tačiau vaizdo stebėjimu nėra tikslingai siekiama stebėti Įmonių darbuotojų elgseną, vertinti jų darbo efektyvumą ir pan.

2.13. Tvarkant vaizdo duomenis yra taikomos Įmonės Duomenų saugumo politikoje ir Vaizdo duomenų tvarkymo taisyklėse nustatytos saugumo priemonės.

2.14. Šioje srityje šiuo metu nėra patvirtintų etikos kodeksų ar sertifikavimo mechanizmų.

Aprašomi Asmens duomenų tvarkymo tikslai: kokį rezultatą siekiama gauti; kokį poveikį tai turės fiziniams asmenims; kokia yra tokio duomenų tvarkymo nauda Įmonei bei kitiems asmenims.

2.15. **Siekiamas rezultatas:** išvengta žalos Įmonei, jos darbuotojams ir Įmonės klientams (prevencinė priemonė siekiant atgrasyti galimus pažeidėjus), padidintos galimybės esant teisės pažeidimams, nusikaltimams nustatyti kaltininką, vaizdo stebėjimo įrašą pateikiant teisėsaugos ar kitoms institucijoms, užtikrinta saugi aplinka Įmonės darbuotojams (saugumo jausmas).

2.16. **Poveikis fiziniams asmenims:** fiziniai asmenys (tiek darbuotojai, tiek kiti asmenys, patenkantys į Įmonės vaizdo stebėjimo lauką), žinodami, kad Įmonės patalpų prieigos yra stebimos vaizdo kameromis, turėtų jaustis saugiau (užtikrinamas didesnis saugumas). Kita vertus, dėl vaizdo stebėjimo galimas ir tam tikras neigiamas poveikis darbuotojų išgyvenimams, žinant, kad kiekvienas įėjimas ir išėjimas iš darbo patalpų (Įmonės patalpų) yra stebimas.

2.17. **Nauda Įmonei bei kitiems asmenims:** užtikrintas teritorijoje ir patalpose esančio Įmonės turto, jos darbuotojų saugumas, surinkti įrodymai apie pažeidimus, vaizdo įrašų duomenys taip pat gali padėti išaiškinti galimai padarytas nusikalstamas veikas, kitus teisės pažeidimus, padarytus stebimose Įmonės patalpų prieigose. Taip pat akivaizdus faktas, jog vaizdo

stebėjimas yra vykdomas, atlieka ir prevencinę funkciją, sulaiko asmens nuo sąmoningai ir tyčia atliekamų pažeidimų, turto vagysčių ir pan.

3. Konsultacijos

Aprašoma, kaip planuojama sužinoti suinteresuotų asmenų nuomonę arba pagrindžiama, kodėl to daryti nebūtina: kokių asmenų nuomonę planuojama gauti; kokie asmenys bus pasitelkti Įmonėje, ar bus pasitelkti duomenų tvarkytojai; ar planuojama konsultuotis su duomenų saugos ekspertais ar kitokių sričių ekspertais.
3.1. Su duomenų subjektais nėra konsultuojamasi, nes vaizdo stebėsena nėra nauja ar netikėta duomenų tvarkymo operacija. Vaizdo stebėjimas yra vykdomas nuo 2018 m. rugpjūčio 13 d. Duomenų subjektai yra informuoti apie vaizdo stebėseną (žino, kad Įmonės patalpų prieigose yra stebimas vaizdas). Per visą vaizdo stebėjimo laikotarpį Įmonė negavo nei vieno duomenų subjekto (nei darbuotojo, nei kito asmens, patekusio į Įmonės vykdomo vaizdo stebėjimo lauką) skundo dėl vaizdo stebėjimo, todėl daro išvadą, kad vaizdo stebėsena duomenų subjektams yra priimtina, nepatogumų nesukelia ir šiuo metu nėra poreikio vykdyti konsultacijas su duomenų subjektais. 3.2. Įmonė vaizdo stebėjimą vykdo pati, nėra pasitelkusi duomenų tvarkytojo, kuris atliktų bent vieną iš šių asmens duomenų tvarkymo veiksmų: rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas. 3.3. Išankstinės konsultacijos (BDAR 36 straipsnis) su Priežiūros institucija nebuvo atliekamos, nes nenustatyta, kad dėl duomenų tvarkymo gali kilti didelis pavojus.

4. Būtinumo ir proporcingumo įvertinimas

Aprašomas Asmens duomenų tvarkymo teisėtumas ir tvarkymo proporcingumas: nurodomas teisėto tvarkymo pagrindas; įvertinama, ar tvarkant Asmens duomenis bus pasiektas tikslas; ar tą patį rezultatą įmanoma pasiekti kitokiu būdu; kokiu būdu bus išvengta veiklos sutrikimų; kaip bus užtikrinta duomenų kokybė ir įgyvendintas duomenų kiekio mažinimo principas; kokia informacija bus pateikta Duomenų subjektams; kaip Įmonė planuoja įgyvendinti Duomenų subjektų teises; kokiu būdu bus užtikrinta, kad duomenų tvarkytojas laikytųsi reikalavimų; kokiu būdu bus užtikrintas į užsienio valstybes teikiamų Asmens duomenų saugumas (jei taikoma).
4.1. **Teisėto tvarkymo pagrindas.** BDAR 35 straipsnio 7 dalies b punktas numato, jog PDAV privalo būti pateiktas asmens duomenų tvarkymo operacijų reikalingumo ir proporcingumo, palyginti su tikslais, vertinimas. Asmens duomenys yra tvarkomi teisėto intereso (BDAR 6 straipsnio 1 dalies f punkto) pagrindu tikslu užtikrinti Įmonės turto ir asmenų (tiek darbuotojų, tiek kitų asmenų, kurie lankosi Įmonė) saugumą, surinkti įrodymus apie pažeidimus ir Įmonės teisių gynimo tikslais. 4.2. **Teisėto intereso balanso testas.** Įmonei tvarkant asmens duomenis teisėto intereso pagrindu Asmens duomenų tvarkymo tikslas turi būti teisėtas, o asmens duomenų tvarkymo metodas ar technologija turi būti reikalinga ir būtina Įmonės interesams užtikrinti. Asmens duomenų tvarkymas taip pat turi būti proporcingas verslo poreikiams. Konkrečiu atveju siekiant nustatyti, ar Įmonė turi teisėtą interesą tvarkyti duomenų subjektų asmens duomenis, ir patvirtinti, kad teisėtas interesas yra tinkamas pagrindas asmens duomenų tvarkymui, vertinami žemiau nurodyti kriterijai: (a) **tikslo**, kurio siekiama tvarkant asmens duomenis teisėto intereso pagrindu, pobūdis; (b) **būtinybė** tvarkyti asmens duomenis teisėto intereso

pagrindu; (c) **pusiausvyra** tarp Įmonės lūkesčio tvarkyti asmens duomenis teisėto intereso pagrindu ir duomenų subjekto interesų, teisių ir laisvių ir, ar šie nėra svarbesni už Įmonės interesus.

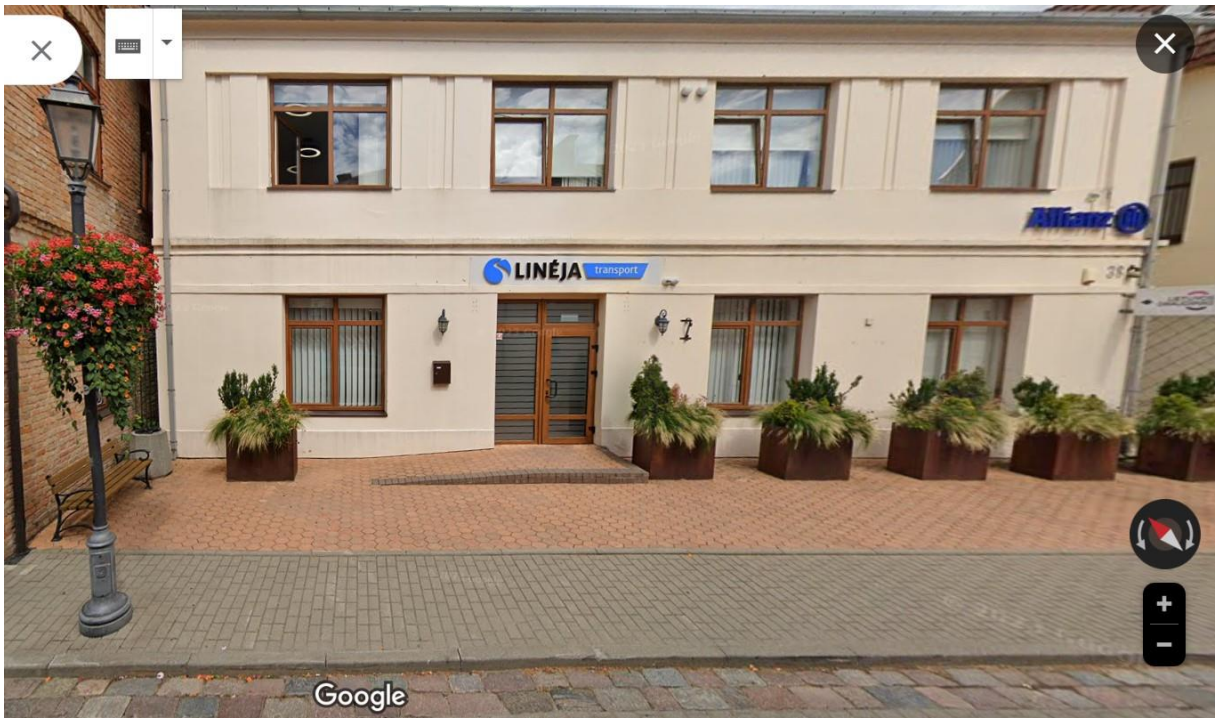
4.2.1. **Tikslas**. Asmens duomenų tvarkymo tikslai yra Įmonės turto ir asmenų (tiek darbuotojų, tiek kitų asmenų, kurie lankosi Įmonė) saugumo užtikrinimas, įrodymų apie pažeidimus surinkimas ir Įmonės teisių gynimas. Jie atitinka verslo poreikius, interesus ir yra aiškiai suprantamas.

4.2.2. **Būtinybė**. Vaizdo stebėjimas nėra vykdomas pačiose Įmonės patalpose, vaizdo stebėjimo laukas yra minimalus, stebimos tik Įmonės patalpos, esančios Įmonės buveinės registracijos adresu. Vis dėl to, nustatant vaizdo stebėjimo vykdymo aplinkybes, prieš Įmonės asmens duomenų apsaugą reglamentuojančių dokumentų atnaujinimą, buvo pateikta informacija, kad į vaizdo stebėjimo lauką patenka ne Įmonei priklausanti teritorija. Atitinkamai, siekiant įgyvendinti būtinybės principą, vaizdo stebėjimo laukas privalo būti pakoreguotas, kad į Įmonės vaizdo stebėjimo lauką nepatektų: kitų įmonių, įstaigų, fizinių asmenų patalpos, teritorijos, eismo kelias, šaligatviai ir pan.

4.2.3. Vaizdo stebėjimas Įmonėje pradėtas vykdyti 2018 m. Įmonė nėra išsaugojusi jokių įrodymų, kad stebimose Įmonės patalpų prieigose būtų įvykę kokie nors rimti incidentai, nusikaltimai ir pan. Europos duomenų apsaugos valdyba Gairėse 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus[1] yra pasisakiusi, kad atsižvelgiant į realią ir pavojingą padėtį, tikslas apsaugoti turtą nuo plėšimo įsilaužiant, vagystės arba vandalizmo gali reikšti teisėtą interesą, kuriam apsaugoti reikalingas stebėjimas vaizdo kameromis. Teisėtas interesas turi būti realus ir aktualus (t. y. tai negali būti fiktyvus arba hipotetinis interesas). Stebėjimo galima imtis tuomet, kai iš tikrųjų įvyksta nelaimė, pavyzdžiui, anksčiau buvo padaryta žala arba įvyko rimti incidentai. Atsižvelgiant į atskaitomybės principą, duomenų valdytojams būtų patartina dokumentuose aprašyti atitinkamus incidentus (data, pobūdis, finansiniai nuostoliai) ir susijusius baudžiamuosius kaltinimus. Šie dokumentais patvirtinti interesai gali būti patikimas teisėto intereso buvimo įrodymas. Reikėtų periodiškai iš naujo įvertinti teisėto intereso buvimą, taip pat būtinybę vykdyti stebėseną (pvz., kartą per metus, priklausomai nuo aplinkybių). Prieš sumontuodamas stebėjimo vaizdo kameromis sistemą duomenų valdytojas visada turėtų kritiškai įvertinti, ar ši priemonė, pirma, yra tinkama norint pasiekti norimą tikslą, ir, antra, ar ji yra būtina nustatytiems tikslams pasiekti. Stebėjimo vaizdo kameromis priemonės turėtų būti pasirenkamos tik tuo atveju, jeigu duomenų tvarkymo tikslo pagrįstai nebūtų galima pasiekti kitomis priemonėmis, kuriomis mažiau apribojamos duomenų subjekto pagrindinės teisės ir laisvės. Atsižvelgiant į tai, kad duomenų valdytojas nori užkirsti kelią nusikaltimams nuosavybei, užuot sumontavęs stebėjimo vaizdo kameromis sistemą, jis taip pat galėtų imtis alternatyvių saugumo priemonių, pavyzdžiui, aptverti turtą tvora, pasirūpinti reguliariu apsaugos darbuotojų patruliavimu, naudotis sargo paslaugomis, įrengti geresnį apšvietimą, uždėti apsaugines spynas, įdėti smūgiams atsparius langus ir duris arba naudoti grafičiams atsparią dangą arba foliją. Šios priemonės gali būti lygiai taip pat veiksmingos kaip ir stebėjimo vaizdo kameromis sistemos ir padėti apsisaugoti nuo plėšimo įsilaužiant, vagystės ir vandalizmo. Duomenų valdytojas kiekvienu konkrečiu atveju turi įvertinti, ar tokios priemonės gali būti pagrįstas sprendimo būdas. Apskritai būtinybė naudoti stebėjimą vaizdo kameromis, siekiant apsaugoti duomenų valdytojo patalpas, nebėra aktuali už nuosavybės ribų. Tačiau pasitaiko atvejų, kai turto stebėjimo nepakanka veiksmingai apsaugai užtikrinti. Tam tikrais pavieniais atvejais stebėjimą vaizdo kameromis gali prireikti vykdyti arčiausiai patalpų esančioje aplinkoje. Šiomis aplinkybėmis duomenų valdytojas turėtų apsvarstyti fizines ir technines priemones, pavyzdžiui, blokuoti arba pikseliuoti nesvarbias vietas.

4.2.4. Įmonės buveinė yra Kėdainių miesto senamiestyje, kur Įmonė negali imtis tokių papildomų apsaugos priemonių kaip tvoros užtvėrimas, ar papildomo švietimo įrengimas. Žr. Įmonės prieigų vaizdo užfiksuotą Google Maps:

[1] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_lt.pdf



4.2.5. Iš esmės vaizdo stebėjimo alternatyva lieka vienintelė - paskirti žmogų, kurie nuolatos (24/7) budėtų Įmonės patalpų prieigose, tačiau tokios alternatyvos taikymas, nepašalintų panašaus lygio pavojaus Įmonės turto saugumui, priešingai iškiltų papildoma grėsmė tokiam budinčiam asmeniui, būti užpultam, sužalotam, o susidorojus su tokiu asmeniu, pažeidėjui, nusikaltėliui liktų mažiau kliūčių padaryti pažeidimą, nusikaltimą, o jį padarius didesnė tikimybė išvengti atsakomybės, o Įmonei apginti savo interesus, nes nebūtų jokių užfiksuotų įrodymų. Tad tokia alternatyva nėra vertintina kaip tinkama ir efektyvi.

4.2.6. Kita vertus, nors Įmonė ir neturi įrodymų, kad stebimose Įmonės patalpų prieigose yra įvykę rimtų incidentų, pažeidimų nusikaltimų, tačiau Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos viešai skelbiamais duomenimis, Kėdainiuose nėra mažiausias, o vidutinis nusikalstamumo lygis[2]. Miestų senamiesčiai yra patraukli vieta vandalams, įvairiems susibūrimams, todėl tai yra to vietos, kurios kelia didesnį pavojingumo lygį. Todėl atsižvelgiant į Įmonės buveinės specifiškumą, ribojantį taikyti kitas priemones, siekiant tikslų, dėl kurių vykdomas vaizdo stebėjimas, taip pat į labai ribotą vaizdo stebėjimo lauką (tik Įmonės patalpų prieigos iš išorės), laikytina, kad vertinamas Įmonės vaizdo stebėjimas, jį pakoregavus, kad į lauką patektų ne daugiau kaip 1- 1,5 m. atstumas nuo Įmonės patalpų sienų (ne toliau nei iki šaligatvio), užtikrinant, kad į jį nepatektų prieigos į kitiems asmenims (tiek fiziniams, tiek juridiniams asmenims) priklausančios patalpas, patalpų langai šalia esantis šaligatvis, važiuojamoji eismo dalis ir pan., atitiktų būtinybės kriterijų.

4.2.7. **Intereso viršenybė**. Laikytina, kad šiuo atveju duomenų subjektų interesai nėra viršesni už Įmonės interesą apsaugoti jos turtą, užtikrinti Įmonės, darbuotojų ir kitų asmenų saugumą, surinkti įrodymus apie pažeidimus, apginti teises.

4.2.8. Vaizdo stebėseną Įmonė vykdo tik Įmonės patalpų prieigose, iš išorės. Duomenų subjektai iš anksto yra įspėti apie tai, kad vykdomas vaizdo stebėjimas, nėra stebimos tos vietos, kur asmuo pagrįstai tikisi visiško privatumo.

[2] https://www.ird.lt/lt/paslaugos/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos/nvzr-nusikalstamumas-pagal-savivaldybes?municipality=18

4.2.9. Išdėstyti argumentai patvirtina, kad duomenų subjektų interesai atitinkamai pakoregavus vaizdo stebėjimo lauką, kaip nurodyta šios Išvados 4.2.6 punkte, nebūtų nepagrįstai suvaržomi, nes jie būtų stebimi tik tais atvejais ir tose vietose, kuriose negali pagrįstai tikėtis privatumo.

4.3. **Proporcingumas**. Vertinant proporcingumą, atsižvelgiama į tai, ar tam tikros priemonės yra proporcingos siekiamam tikslui esant pagrįstai būtinybei. Tinkamai kontroliuojama stebėsena yra laikoma proporcinga tikslui, dėl kurio ji vykdoma.

4.4. Vaizdo stebėsena, visų pirma, siekiama išvengti žalos Įmonei ir jos turtui, užtikrinti jų saugumą, išaiškinti įvairius incidentus, siekiam užtikrinti Įmonės darbuotojų kitų asmenų saugumą. Siekis užtikrinti asmens ir turto saugumą pateisina tam tikrą fizinių asmenų privatumo suvaržymą (vaizdo kamerų įrengimą).

4.5. Siekiant, kad fizinių asmenų privatumas būtų varžomas kuo mažiau, vaizdas Įmonės patalpų prieigose vaizdas yra įrašomas be garso. Vaizdo kameros nestebi vietų, kuriose asmenys pagrįstai gali tikėtis privatumo.

4.6. Realiu laiku vaizdo stebėjimas galimas, tačiau nėra vykdomas.

4.7. **Duomenų rinkimo adekvatumo ir tinkamumo, siekiant numatytų tikslų, vertinimas (BDAR 5 straipsnio 1 dalies c punktas).** Stebimos tik Įmonės patalpų prieigos. Vaizdo stebėsena, visų pirma, siekiama žalos Įmonei ir jos turtui, užtikrinti jų saugumą, išaiškinti įvairius incidentus, siekiama užtikrinti darbuotojų, kitų asmenų saugumą. Siekis užtikrinti asmens ir turto saugumą pateisina tam tikrą fizinių asmenų privatumo suvaržymą (vaizdo kamerų įrengimą).

4.8. Pasirinkta priemonė tikslui pasiekti (vaizdo stebėsena) yra įprastai taikoma Įmonėse. Alternatyvių priemonių, kurios būtų tokios pačios efektyvios ir nesudėtingai įgyvendinamos, nėra (budinčio asmens samdymas būtų mažiau efektyvus, o ir keliantis grėsmę pačiam tokias pareigas atliekančiam asmeniui, dėl darbo pobūdžio, tikėtina net ir vieno asmens samdymas nebūtų pakankamas, kas, matyt, nebūtų efektyvu ir neleistų pasiekti to paties rezultato, ypač prevencinio).

4.9. **Ribotos duomenų saugojimo trukmės vertinimas (BDAR 5 straipsnio 1 dalies e punktas).** Stebėsenos metu surinkti asmens duomenys yra saugomi PDAV 2.7 p. nurodytus laikotarpius, kurie iš esmės priklauso nuo įrenginio įrašymo galimybės. Europos duomenų apsaugos valdyba 2020 m. sausio 29 d. Gairėse 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus yra pasisakiusi, kad „Atsižvelgiant į BDAR 5 straipsnio 1 dalies c ir e punktuose nustatytus principus, būtent duomenų kiekio mažinimo ir saugojimo trukmės apribojimo principus, asmens duomenis dažniausiai (pvz., siekiant nustatyti vandalizmo atvejį) ir idealiausiu atveju reikėtų ištrinti po kelių dienų. Kuo ilgesnis saugojimo laikotarpis nustatomas (ypač kai jis ilgesnis negu 72 valandos), tuo daugiau reikia pateikti argumentų, susijusių su tikslo teisėtumu ir saugojimo būtinumu.” Įmonės poreikį saugoti vaizdo įrašus ilgiau nei 72 val., t. y. 7 dienas, pagrindžia, tai, kad kartais dėl šventinių laikotarpių, Įmonės atsakingus asmenis dėl šventinių laikotarpių, kurių kalendorinių metų eigoje gali būti ne vienas, informacija apie incidentus gali pasiekti vėliau nei per 72 val., todėl 7 dienų terminas būtų pakankamas ir būtinas.

4.10. **Su nacionaliniu ir tarptautiniu perdavimu susijusių apsaugos priemonių vertinimas (BDAR V skyrius. ir 28 straipsnis).** Nurodytu tikslu tvarkomi asmens duomenys į trečiąsias valstybes ir tarptautines organizacijas neperduodami, todėl šio aspekto vertinimas neatliekamas.

5. **Pavojų nustatymas ir įvertinimas**

Aprašomas pavojaus ir poveikio fiziniam asmeniui pobūdis. Jei būtina, aprašomos susijusios rizikos.	**Žalos tikimybė**	**Žalos sunkumas**	**Bendras pavojaus lygis**
Duomenų subjektų teisių suvaržymas (nepakankamas informavimas apie vaizdo stebėseną). Duomenų subjektų informavimas apie vaizdo stebėjimą yra reglamentuotas Įmonės asmens duomenų apsaugą reglamentuojančiuose dokumentuose, taip pat ir Vaizdo duomenų tvarkymo taisyklėse, įskaitant ir naujų darbuotojų supažindinimą su šiais dokumentais. Todėl tokio pavojaus rizika yra maža. Rizika galia pasireikšti tik tais atvejais, kai dėl žmogiškosios klaidos nebus laiku ir tinkamai informuoti nauji darbuotojai. Dėl per mažo šrifto informacinėje lentelėje asmuo prieš patenkant į vaizdo stebėjimo lauką negalės jo įskaityti, ar kai dėl vandalizmo veiksmų, lentelė bus pašalinta ar tekstas joje, pvz., uždažytas dažais. Atsižvelgiant į tai, kad tokių atvejų iki šiol nepasitaikė, tokia tokių atvejų pasireiškimo tikimybė vertintina kaip maža.	Maža	Minimali	Mažas
Vaizdo duomenų tvarkymo neatitiktis būtinumo reikalavimui. Ši rizika apima tuos atvejus, kai į Įmonės vaizdo stebėjimo lauką patenka prieigos į kitiems asmenims (tiek fiziniams, tiek juridiniams asmenims) priklausančias patalpas, patalpų langai, šalia esantis šaligatvis, važiuojamoji eismo dalis. Tikimybė vertinama kaip didelė, atsižvelgiant į informaciją, pateiktą šio vertinimo atlikimo metu.	Didelė	Vidutinė	Didelis
Trečiųjų asmenų neteisėta prieiga prie asmens duomenų. Asmens duomenų nutekėjimas galimai turėtų lengvų neigiamų pasekmių duomenų subjektams, jie galimai patirtų neigiamus dvasinius išgyvenimus. Atskirais atvejais, jei po duomenų nutekėjimo būtų paviešintas duomenų subjektą pašiepiantis (pavyzdžiui, kai duomenų subjektas juokingai paslysta ir nukrenta) ar kompromituojantis vaizdo įrašas, duomenų subjektas gali patirti ir didesnį neigiamą poveikį – dėl streso gali būti padaryta minimali žala duomenų subjekto sveikatai, galimas neigiamas poveikis asmeniniams santykiams ir pan.	Mažai tikėtina	Vidutinė	Vidutinis

Nacionalinio kibernetinio saugumo centro duomenimis[3] Hikvision kamerose naudojami programinės įrangos paketai turi gana daug žinomų kibernetinio saugumo spragų, pažymėtų viešai prieinamose pažeidžiamumų duomenų bazėse (angl. Common Vulnerabilities and Exposures, CVE). Pasinaudojus šiomis spragomis iškyla reali kibernetinių atakų rizika, tokių kaip atkirtimo nuo paslaugos (DoS) ar kenkėjiško kodo įterpimas. Kamerose nėra automatinio atnaujinimo funkcijos, o naujinimo infrastruktūra išdėstyta Kinijos ir Rusijos serveriuose. Gaminiuose panaudoti prasti slaptažodžių apsaugos mechanizmai, kai vartotojų autentifikavimas kamerose vykdomas nešifruotu ryšiu, naudojant HTTP protokolą, kartu su pasenusiu MD5 algoritmu. Dėl to, vartotojui jungiantis prie kameros, jo slaptažodžio reikšmė gali būti perimta, slaptažodis dekoduotas ir panaudotas neteisėtam prisijungimui. Tai galėtų leisti pašaliniams perimti kameros turinio transliaciją, realiuoju laiku aktyvuoti ar deaktyvuoti kameros funkcijas (vaizdo atpažinimo, garso įrašymo ir kt.), stabdyti kameros veikimą. Be to, nustatyta, kad gamintojo „Hikvision“ parengta kamerų valdymo mobili aplikacija „Hik-Connect“ vykdo sujungimus su Kinija, Tailandu, Singapūru, Airija ir registruoja SIM kortelės IMSI ir ICCID identifikacinius numerius bei mobilaus įrenginio IMEI identifikacinį numerį.			
Asmens duomenų atskleidimas asmenims, neturintiems teisės su jais susipažinti. Tokie atvejai galimi, jei reaguojant į duomenų subjektų prašymus duomenų subjektams būtų atskleista per daug asmens duomenų. Paprastai dėl to duomenų subjektai galėtų patirti tik lengvus dvasinius išgyvenimus, atskirais atvejais – ir didesnį stresą, neigiamą poveikį sveikatai ar asmeniniams santykiams.	Mažai tikėtina	Vidutinė	Vidutinis
Prašymų dėl Duomenų subjektų teisių įgyvendinimo vykdymo termino praleidimas. Tokiu atveju asmuo gali patirti lengvų dvasinių išgyvenimų.	Mažai tikėtina	Minimali	Žemas
Pavėluotas Asmens duomenų sunaikinimas. Tai reikštų vėlesnį nei nustatyta Įmonės vidaus dokumentuose asmens duomenų sunaikinimą. Tokiu atveju asmuo gali patirti lengvų dvasinių išgyvenimų.	Mažai tikėtina	Minimali	Žemas

[3] https://www.nksc.lt/naujienos/hikvision_ir_dahua_gamintoju_kameru_tyrimas_nustat.html

6. **Priemonių pavojui sumažinti nustatymas**

Nurodomos papildomos priemonės, kurių galima imtis siekiant sumažinti ar panaikinti aukšto ar vidutinio lygio pavojus.				
Pavojus	**Priemonės sumažinti ar pašalinti pavojų**	**Priemonės pritaikymo rezultatas**	**Likęs pavojus**	**Priemonė patvirtinta**
Vaizdo duomenų tvarkymo neatitiktis būtinumo reikalavimui	Techninėmis priemonėmis (pavyzdžiui, pikseliuojant) užtikrinti, kad į Įmonės vaizdo stebėjimo lauką patektų ne daugiau kaip 1- 1,5 m. atstumas nuo Įmonės patalpų sienų (ne toliau nei iki šaligatvio), užtikrinant, kad į jį nepatektų prieigos į kitiems asmenims (tiek fiziniams, tiek juridiniams asmenims) priklausančios patalpas, patalpų langai, šalia esantis šaligatvis, važiuojamoji eismo dalis ir pan.	Pritaikius nustatytas priemones, būtinumo reikalavimo pažeidimas dėl vaizdo stebėsenos yra mažai tikėtinas. Vis dėl to, išlieka galimybė, kad priežiūros institucija, vertindama, kad vaizdo stebėjimo apimtyje nėra buvę rimtų incidentų ir nusikaltimų, nėra objektyvaus pagrindo konstatuoti Įmonės vykdomo vaizdo stebėjimo atitiktį būtinumo reikalavimui.	Žemas	Taip
Trečiųjų asmenų neteisėta prieiga prie asmens duomenų	Siekiant sumažinti rizikas dėl Hikvision vaizdo kamerų naudojimo, turėtų būti įgyvendintos šios saugumo priemonės, rekomenduojamos Nacionalinio kibernetinio saugumo centro: 1. Izoliuoti atskirame fiziniame arba specifiškai parametrizuotame loginiame tinkle, neturinčiame prieigos prie tarnybinių, vietinių ar viešųjų interneto tinklų. 2. Neatskleisti savo tapatybės ir nesisiųsti atnaujinimų iš nutolusių serverių, nepriklausančių NATO ar Europos Sąjungos šalims. 3. Nuolatos vykdyti realaus laiko kamerų prievadų aktyvumo ir formuojamų kreipinių auditą, blokuoti perteklines užklausas ar srautus, naudoti ugniasienes su konkrečiam kameros modeliui verifikuotomis prieigos instrukcijomis (angl. White-list).	Pritaikius nustatytas priemones, neteisėta trečiųjų asmenų prieiga prie asmens duomenų (vaizdo duomenų) yra mažai tikėtina.	Žemas	Taip

Asmens duomenų atskleidimas asmenims, neturintiems teisės su jais susipažinti	Asmenys, turintys teisę ir įgaliojimus įgyvendinti duomenų subjektų teises, turi būti reguliariai, kartą per metus apmokomi duomenų apsaugos klausimais, įskaitant ir duomenų subjektų teisių įgyvendinimo tema.	Pritaikius minėtą priemonę, asmens duomenų atskleidimas būtų mažai tikėtinas.	Žemas	Taip

7. Papildoma informacija

BDAR 35 straipsnio 8 dalis numato, jog vertinant duomenų valdytojų ir duomenų tvarkytojų vykdomų duomenų tvarkymo operacijų poveikį, visų pirma, atliekant PDAV, deramai atsižvelgiama į tai, ar atitinkami duomenų valdytojai ir duomenų tvarkytojai laikosi BDAR 40 straipsnyje nurodytų patvirtintų elgesio kodeksų. Atsižvelgiant į tai, kad atitinkami elgesio kodeksai nėra patvirtinti, jų nuostatos nebuvo vertinamos ir nebuvo jomis nebuvo remiamasi atliekant PDAV.

8. Išvados ir sprendimai

Nurodomos priemonės ir įvardijamas likęs pavojus	Vardas, pavardė, data, parašas	Pastabos
Priemonės patvirtintos	Direktorius Gediminas Norkus _____ _____	Įtraukti numatytas priemones į veiklos planą, nustatant atlikimo terminą ir atsakingus asmenis.
Likęs pavojus pripažintas priimtina rizika. Išvadoje nurodytos likutinės vertės yra minimalios, todėl nėra pagrindo konsultuotis su Priežiūros institucija dėl praėjimo kontrolei reikalingų Asmens duomenų tvarkymo (BDAR 36 str. 1 d.).		Jei priimtina rizika pripažintas aukšto lygio pavojus, privaloma kreiptis dėl išankstinės konsultacijos į priežiūros instituciją (VDAI).

9. **Pridedami dokumentai**

Nr.	Pavadinimas
1.	Klausimynas dėl vaizdo stebėjimo.

10. **Už duomenų apsaugą atsakingo asmens nuomonė**

Nuomonė turi būti pateikta dėl asmens duomenų tvarkymo teisėtumo, planuojamų priemonių pavojams mažinti ar pašalinti bei dėl galimybės toliau tvarkyti asmens duomenis.

Siekiant užtikrinti asmens duomenų tvarkymo teisėtumą, būtina kuo greičiau pašalinti nustatytus duomenų subjektų informavimo trūkumus ir įgyvendinti rekomenduojamas Hikvision kamerų saugumo užtikrinimo priemones, kiek jos nėra įgyvendintos, pakoreguotas vaizdo stebėjimo laukas ir organizuoti asmens duomenų apsaugos mokymai su asmens duomenimis dirbantiems Įmonės darbuotojams. Kitų nei nustatyta šioje Išvadoje duomenų tvarkymo rizikų neįžvelgiu. Pasiūlytas priemones pavojams suvaldyti laikau tinkamomis, pasiūlymų dėl papildomų priemonių taikymo neturiu.
Gabija Ruseckaitė, 2024-05-08

11. **Nurodoma, ar atsižvelgta į duomenų apsaugos pareigūno nuomonę.**

Jeigu atmesta, pagrindžiama, kodėl.

Daiva Tamulionienė, 2024-05-08

12. **Gautos kitų asmenų nuomonės**

Trumpai aprašomos kitų asmenų nuomonės ir nurodoma, ar į jas atsižvelgta. Jeigu sprendimas skiriasi nuo susijusių asmenų nuomonės, pagrindžiama, kodėl.

Nėra.
Daiva Tamulionienė, 2024-05-08

13. **Už šio poveikio duomenų apsaugai vertinimo priežiūrą paskirtas atsakingas asmuo**

Duomenų apsaugos pareigūnas kartu su Saugumo pareigūnu
Pareigos, vardas, pavardė, data, parašas

14. **Poveikio duomenų apsaugai vertinimą atlikęs asmuo**

Advokatų profesinės bendrijos „WIDEN Legal“ vyresnioji teisininkė Daiva Tamulionienė
Pareigos, vardas, pavardė, data, parašas