PATVIRTINTA
2021-11-25
Akcinės bendrovės „Klaipėdos nafta“
Generalinio direktoriaus įsakymu
Nr. BV-137

AKCINĖS BENDROVĖS „KLAIPĖDOS NAFTA“ MINIMALŪS INFORMACIJOS IR KIBERNETINIO SAUGUMO REIKALAVIMAI IŠORĖS ŠALIMS

1. Taikymo sritis

1.1. Šie akcinės bendrovės „Klaipėdos nafta“ (toliau – *KN*) minimalūs informacijos ir kibernetinio saugumo reikalavimai išorės šalims (toliau – *Reikalavimai*) taikomi visiems fiziniams ir juridiniams asmenims, su kuriais *KN* sudaro sutartis ir tokių sutarčių vykdymas apima *KN* valdomos informacijos ir informacinių išteklių apsaugos principus bei jų tvarkymo veiksmus.

1.2. Dokumentas skelbiamas viešai KN interneto svetainėje https://www.kn.lt

2. Pagrindas ir objektas

2.1. *Reikalavimų* pagrindas – tarp *KN* ir *Išorės šalies* sudaryta *Sutartis* bei *Sutarties* šalių pareiga užtikrinti informacijos ir kibernetinio saugumo reikalavimų laikymąsi *Sutarties* vykdymo metu.

2.2. *Reikalavimų* objektas – *Sutarties* šalių teisės ir pareigos *KN* pavedimu *Išorės šaliai* naudojantis KN informacija ir informaciniais ištekliais.

3. Vartojamos sąvokos

3.1. *Asmens duomenys* – kaip jie apibrėžti Bendrojo duomenų apsaugos reglamento 4 straipsnio 1 dalyje, kuriuos KN pateikia *Išorės šaliai Sutarties* vykdymui arba sudaro prieigą prie jų, laikantis šiuose *Reikalavimuose* nustatytų sąlygų;

3.2. *„Būtina darbui/būtina žinoti“* – prieiga suteikiama tik prie minimalios ir atitinkamai veiklai būtinos informacinės sistemos ar duomenų perdavimo tinklo dalies.

3.3. *Duomenų perdavimo tinklas* – KN skirstomas į informacijos perdavimo ir elektroninių ryšių (toliau – *Bendrąjį*) tinklą ir pramoninių procesų valdymo sistemų (toliau – *Technologinį*) duomenų tinklą.

3.4. *Informaciniai ištekliai* - informacija (duomenų bazės, duomenų rinkmenos, sutartys ir kiti dokumentai, sisteminė ir projektinė dokumentacija, mokymų medžiaga, eksploatavimo ir priežiūros procedūros, tęstinumo ir atkūrimo planai); programinė įranga (taikomoji ir sisteminė programinė įranga, jos kūrimo priemonės); aparatinė įranga (duomenų laikmenos, organizacinė, kompiuterinė ir ryšių įranga); informacinių technologijų, pramoninių procesų valdymui ir telekomunikacijų funkcionavimui reikalingos paslaugos.

3.5. *Išorės šalys* – paslaugų teikėjai, partneriai, klientai, kiti asmenys, turintys ar galintys turėti prieigą prie KN informacinių išteklių;

3.6. *Sutartis* – KN ir *Išorės šalies* sudaryta sutartis, kurios vykdymas apima, KN pavedimu, darbą su KN valdomais informaciniais ištekliais, KN informacija ir kurioje teikiama nuoroda į šiuos *Reikalavimus* arba kai *Reikalavimų* taikymas tokiai Sutarčiai tarp KN ir *Išorės šalies* sutartas kitu būdu;

3.7. Kitos sąvokos *Reikalavimuose* suprantamos taip, kaip jos apibrėžtos ir vartojamos *Sutartyje* ir Informacijos bei kibernetinį saugumą reglamentuojančiuose teisės aktuose bei vidiniuose KN dokumentuose.

4. Atitikties reikalavimai

4.1. Šie *Reikalavimai* apibrėžia minimalius informacijos ir kibernetinio saugumo principus, kurie turi būti įvykdyti bet kokiomis sąlygomis pagal atitinkamą sutartį su *KN*, kurioje yra nuoroda į šiuos *Reikalavimus*.

4.2. *KN* prašymu leisti *KN* ar jo įgaliotam asmeniui atlikti Informacijos ir kibernetinio saugumo vertinimą ar kitus Informacijos ir kibernetinio saugumo patikrinimo veiksmus, susijusius su *KN* informacinių išteklių naudojimu, bei pateikti visą reikalingą informaciją, kiek tai reikalinga patikrinti, ar *Išorės šalis* laikosi šių *Reikalavimų* ir taikomų Informacijos ir kibernetinio saugumo teisės aktų nurodymų.

4.3. Galimi ir tikėtini nukrypimai nuo *Reikalavimų* turi būti aiškiai pažymėti ir dokumentuoti.

4.4. Priklausomai nuo prieigos ir darbo su informacinėmis sistemomis, informacija bei duomenų tinklais gali būti taikomi papildomi techniniai ir organizaciniai reikalavimai nurodyti:

4.4.1. Lietuvos Respublikos vyriausybės 2018 m. gruodžio mėn. 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“ patvirtintame Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše,

4.4.2.2002 m. spalio mėn. 10 d. Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme Nr. IX-1132 (su vėlesniais pakeitimais),

4.4.3.2020 m. birželio mėn. 18 d. Valstybinės duomenų apsaugos inspekcijos Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėse duomenų valdytojams ir duomenų tvarkytojams.

5. Nuotolinio darbo saugumo reikalavimai

5.1. Suteikiant *Išorės šaliai* galimybę dirbti nuotolinėje kompiuterizuotoje darbo vietoje priklausančioje *Išorės šaliai* bei suteikiant nuotolinę prieigą prie *KN* informacinių sistemų *Bendrajame* duomenų tinkle būtina:

5.1.1. drausti nuotolinę prieigą jei nenaudojamas saugus VPN ryšys;

5.1.2. įsitikinti, kad informacinės sistemos, kompiuterinė įranga ir duomenų tinklai, iš kurių jungiamasi per nuotolį, yra saugūs ir patikimi (atnaujinta operacinė sistema ir kita programinė įranga, įdiegta antivirusinė programinės įranga, įjungta ir sukonfigūruota ugniasienė ir t.t.);

5.1.3. užtikrinti savalaikę ir reguliarią prieigos teisių kontrolę;

5.1.4. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę;

5.1.5. užtikrinti *KN* konfidencialios informacijos, įskaitant asmens duomenų, apsaugą tinkamomis techninėmis priemonėmis (pvz., šifruojant informacijos perdavimą, saugojimą ir pan.);

5.1.6. užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas su iš anksto tarpusavyje suderintais tikslais;

5.1.7. nuotolinio ryšio sujungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „*Būtina darbui/būtina žinoti*“ bei turėtų sutartą galiojimo terminą.

6. Saugus programinės įrangos kūrimo ciklas

6.1. *Išorės šalis* nustato, dokumentuoja ir įgyvendina iniciatyvas, atitinkančias bendrai priimtus informacijos ir kibernetinio saugumo standartus bei praktiką siekiant sukurti saugius programinės ar techninės įrangos kūrimo procesus. Tokios iniciatyvos turi užtikrinti informacijos ir kibernetinį saugumą visuose plėtros etapuose: mokymuose, reikalavimų apibrėžimuose, dizaino kūrime, diegime, patvirtinime, išleidime ir priežiūroje.

6.2. Produktas neturi naudotojo paskyrų, slaptažodžių ar privačių/slaptų raktų, kurių negali pakeisti arba pašalinti įgaliotasis produkto galutinis vartotojas.

6.3. Produktas neturi jokių naudotojo paskyrų (individualių, bendrų, testavimo aplinkos), kurios nėra dokumentuotos (tai nereiškia, kad susijusių naudotojų prieigos duomenys turi būti atskleisti).

6.4. *Išorės šalis* turi aktyviai imtis priemonių, kad būtų pagerinta produkto saugumo kokybė. Šios priemonės turi atitikti bendrai priimtus IT ir pramoninių procesų valdymo kibernetinio saugumo standartus ir praktiką bei, jei tai techniškai įmanoma, apimti patikimumo bandymus, pažeidžiamumų valdymą ir programinio kodo saugumo testavimus (įskaitant statinio ar binarinio kodo analizę).

6.5. Turi būti užtikrinta kuriamo programinio kodo higiena (negali būti pavyzdinės imties duomenų ir scenarijaus kodo, nuorodų į nenaudojamas bibliotekas, derinimo kodo ir kt. naudotų įrankių) perkeliant vystomą programinę įrangą į darbinę aplinką.

6.6. Vystomos programinės įrangos kūrimo, testavimo ir darbinės aplinkos turi būti atskirtos. Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Testuojant sistemas, turi būti naudojami testiniai duomenys. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros.

6.7. Programinės įrangos naudotojams neturi būti rodomi vystomos programinės įrangos klaidų apie programinį kodą ar tarnybinės stoties pranešimai.

7. Saugumo reikalavimai personalui

7.1. *Išorės šaliai* dirbančių asmenų patikrinimai vykdomi vadovaujantis Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu.

8. Sąmoningumo ugdymas ir mokymai

8.1. *Išorės šalis* turi vykdyti savo darbuotojų informacijos ir kibernetinio saugumo sąmoningumo ugdymą suteikiant technines, procedūrines ir saugios veiklos kibernetinėje erdvėje žinias.

8.2. Kiekvienas *Išorės šaliai* su *KN* informaciniais ištekliais dirbantis asmuo privalo būti atsakingo *Išorės šalies* darbuotojo supažindintas su *KN* galiojančia Informacijos ir kibernetinio saugumo politika ir kitais informacijos, asmens duomenų ir kibernetinį saugumą reglamentuojančiais KN dokumentais skelbiamais viešai *KN* interneto svetainėje https://www.kn.lt ir reikalingais darbui su *KN* informaciniais ištekliais ar *KN* valdomais asmens duomenimis.

8.3. *Išorės šalies* darbuotojai ir jai dirbantys asmenys privalo pateikti atitinkantį kvalifikacijos įrodymą leidžiantį dirbti su konkrečiu *KN* informaciniu ištekliumi kur tai yra būtina arba reikalaujama.

8.4. *Išorės šalis* turi būti pasitvirtinusi informacijos ir kibernetinių incidentų valdymo bei veiklos tęstinumo planus ar kitą dokumentaciją, reglamentuojančią *Išorės šalies* darbuotojų veiksmus informacijos ir kibernetinių incidentų metu.

9. Fizinė sauga

9.1. *Išorės šalių* atstovai ir jų transporto priemonės į *KN* teritorijas įleidžiami tik su *KN* išduotais leidimais, o gabenamas krovinys - su krovinį lydinčiais dokumentais.

9.2. Techniškai netvarkingas *Išorės šalių* autotransportas ir mechanizmai bei autotransportas su pašaliniais kroviniais į *KN* teritoriją neįleidžiamas.

9.3. Visi leidimai yra vardiniai, juos draudžiama perduoti ir/ar kitokiu būdu perleisti naudotis tretiesiems asmenims.

9.4. Vienkartiniai leidimai išduodami vienkartiniam apsilankymui *KN* teritorijoje nurodytu leidime laiku ir galioja tik su kartu apsaugą vykdančiam pareigūnui/darbuotojui pateiktu asmens tapatybę patvirtinančiu dokumentu (pasu, asmens tapatybės kortele, vairuotojo pažymėjimu).

9.5. *Išorės šalių* atstovai, įtariami esant neblaivūs, apsvaigę nuo narkotinių ar toksinių medžiagų, į *KN* teritoriją neįleidžiami.

9.6. *KN* teritorijoje draudžiama filmuoti ar fotografuoti negavus už apsaugą atsakingų asmenų leidimo.

9.7. Draudžiama į *KN* teritoriją įvežti/įnešti šiuos daiktus:

9.7.1. Lietuvos Respublikos Ginklų ir šaudmenų kontrolės įstatyme įrašytus visų kategorijų ginklus, jų priedėlius ir šaudmenis ar jų imitacijas;

9.7.2. sprogstamuosius įtaisus ir sprogiąsias medžiagas ar jų imitacijas;

9.7.3. narkotikus ir narkotines medžiagas bei alkoholinius gėrimus;

9.7.4. kitus, atvirą liepsną naudojančius ar kibirkštį skleidžiančius/sukeliančius, pavojingus daiktus, išskyrus tiesioginiam darbui, kuriam turi būti išduotas leidimas, naudojamus įrankius ar prietaisus.

9.8. *Išorės šalių* atstovams gali būti atimta teisė lankytis *KN* už šių ir kitų saugumą *KN* terminaluose reglamentuojančių reikalavimų nesilaikymą.

9.9. Visi *Išorės šalių* atstovai ir jų transporto priemones neteisėtai patekę į *KN* teritoriją yra sulaikomi ir apie tai pranešama Valstybės sienos apsaugos tarnybos Pakrančių apsaugos rinktinės Uosto užkardos budėtojui ir policijos budėtojui.

10. Informacijos apsauga

10.1. Informacija *KN* skirstoma į viešą, vidinio naudojimo ir konfidencialią.

10.2. *Išorės šalis* turi būti informuojama apie konfidencialios informacijos perdavimą, kurį apibrėžia informacijos klasifikavimą, saugojimą ir naudojimą reglamentuojantys *KN* dokumentai.

10.3. Komunikacijos planuose turi būti nurodyta, kad komunikacija, kurios turinį sudaro vidinio naudojimo ir konfidenciali informacija ar asmens duomenys su *Išorės šalimi* vyksta tik saugiu ryšio kanalu, naudojantis saugaus el. pašto žinučių ir failų apsikeitimo sprendimu **https://box.kn.lt.**

11. Bendrieji kibernetinio saugumo reikalavimai

11.1. *Išorės šalis* turi užtikrinti, kad bet kokia nauja jos įdiegta technologija *KN*, yra sankcionuota ir yra gautas *KN* sutikimas ją naudoti, taip pat užtikrinti, kad šios technologijos sauga yra pakankama.

11.2. Informacinių sistemų naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone ir papildomu autentifikavimo faktoriumi (jei informacinė sistema palaiko tokį funkcionalumą).

11.3. Suteikiant laikinus slaptažodžius Informacinių sistemų naudotojams ir administratoriams, šie slaptažodžiai turi būti unikalūs kiekvienam ištekliaus naudotojui ir perduodami saugiu būdu (pvz. per https://box.kn.lt).

11.4. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo naudotojo vardo, jeigu Informacinių sistemų naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių Informacinių sistemų naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroniniu ryšių tinklu.

11.5. Visose Informacinėse sistemose, prieš pradedant jas eksploatuoti, Informacinių sistemų administratoriai privalo pakeisti standartinius (gamintojų) slaptažodžius į šiuos *Reikalavimus* atitinkančius slaptažodžius.

11.6. Informacinių sistemų dalys, patvirtinančios Informacinių sistemų naudotojo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius.

11.7. Informacinių sistemų administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą naudotojo vardą, kuris negali būti naudojamas kasdienėms Informacinių sistemų naudotojo funkcijoms atlikti.

11.8. Informacinių sistemų naudotojams negali būti suteikiamos Informacinių sistemų administratoriaus teisės.

11.9. Kiekvienas Informacinių sistemų naudotojas ar administratorius turi būti unikaliai atpažįstamas.

11.10. Informacinėse sistemose turi būti išjungiamos visos nereikalingos gamyklinės naudotojų paskyros (tame tarpe svečio paskyra).

11.11. Viešai prieinamose kompiuterizuotose darbo vietose paskutinio naudotojo vardas neturi būti matomas prisijungimo metu.

11.12. Prieiga turi būti suteikiama vadovaujantis principu „Būtina darbui/būtina žinoti".

11.13. Nuotolinė prieiga prie *Informacinių sistemų* su administratoriaus paskyra turi būti draudžiama.

11.14. Prisijungdamas nuotoline prieiga prie *Informacinių sistemų* naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.

11.15. Bet kokia nesankcionuota nuotolinė prieiga prie KN informacinių sistemų ir duomenų ar įrangos turi būti draudžiama.

11.16. Nuotolinė prieiga prie KN informacinių sistemų ir duomenų tinklo iš viešųjų duomenų tinklų turi būti šifruojama taikant VPN technologiją.

12. Papildomi kibernetinio saugumo reikalavimai pramoninių procesų valdymo sistemoms

12.1. Pramoninių procesų valdymo sistemos ir jų duomenų tinklas bei jo komponentai negali turėti nuotolinės prieigos iš viešųjų duomenų tinklų.

12.2. Technologiniame duomenų tinkle informacinių išteklių (tarnybinių stočių, komutatorių, maršrutizatorių, ugniasienių ir pan.) administravimui turi būti naudojama atskira techninė įranga neturinti el. pašto paskyros, prieigos prie viešųjų duomenų tinklų ar naudojama darbui su konfidencialia informacija.

13. Išorės šalies įsipareigojimai

13.1. Išorės šalis įsipareigoja:

13.1.1. laikytis šių *Reikalavimų* ir įdiegtų *KN* saugumą bei asmens duomenų apsaugą užtikrinančių procesų.

13.1.2. be *KN* išankstinio raštiško sutikimo neatskleisti tvarkomų *asmens duomenų*, konfidencialios *KN* informacijos jokioms trečiosioms šalims ar gavėjams.

13.1.3. dirbdama su *KN* išduotais informaciniai ištekliais (kompiuteriu, informacijos laikmena, dokumentais, duomenimis ir informacija) vadovautis ir laikytis *KN* Informacijos ir kibernetinio saugumo politikos, šių Reikalavimų, kitų įdiegtų *KN* informacijos ir kibernetinio saugumo procesų bei nustatytų prievolių, su kuriomis supažindina už *Išorės šalį* atsakingas *KN* darbuotojas.

13.1.4. atsakyti už visus *KN* duomenų perdavimo tinklams ar informacinėms sistemoms *Išorės šalies* raštišku prašymu suteiktų informacinių sistemų naudotojų *ar jų* prašyme nurodytų asmenų kaltės atliktus žalingus veiksmus ir jais *KN* padarytus nuostolius.

13.1.5. užtikrinti *KN* informacinės sistemos elektroninės informacijos konfidencialumą bei vientisumą, savo veiksmais netrikdyti informacinės sistemos elektroninės informacijos prieinamumo.

13.1.6. saugoti tvarkomus asmens duomenis.

13.1.7. naudoti tik tas prieigos prie informacinės sistemos teises (sukurti, redaguoti, papildyti ar panaikinti), kurios buvo suteiktos.

13.1.8. baigus darbą ar informacinės sistemos naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri tvarkoma informacinėje sistemoje, negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžio reikalavimu. Šio punkto reikalavimas netaikomas pramoninių procesų valdymui arba apsaugos sistemų stebėjimui skirtose kompiuterizuotose darbo vietose, kuriose dirbama su specialiai šioms funkcijoms vykdyti sukurta paskyra.

13.1.9. naudotis tik tomis informacinės sistemos funkcijomis ir tokia informacijos apimtimi informacinėse sistemose, prie kurios prieiga jam suteikta vadovaujantis prieigų suteikimą prie informacinių sistemų *KN* reglamentuojančiais dokumentais.

13.1.10. nedelsiant, tačiau, bet kokiu atveju, ne vėliau nei per 24 val. po to, kai sužinojo apie tai, raštu informuoti *KN* apie Informacijos ir kibernetinio saugumo incidentą, kuris gali būti susijęs su *KN* asmens duomenimis, informaciniais ištekliais ar duomenų perdavimo tinklu, tel. **+370 46 297 009** ir el. p. **incidentai@kn.lt**, pateikiant visą turimą informaciją bei duomenis, susijusius su tokiu pažeidimu.

13.1.11. užtikrinti, kad imsis pakankamų priemonių rizikoms susijusioms su subrangovais, jų atliekamais darbais ir tiekimo grandine suvaldyti.

13.1.12. tais atvejais kai bus tvarkomi asmens duomenys, sudaryti KN nustatytos formos duomenų tvarkymo susitarimą.

13.1.13. tvarkyti asmens duomenis laikantis KN nurodymų, išdėstytų KN nustatytos formos duomenų tvarkymo susitarime ir papildomuose KN nurodymuose, jeigu tokie būtų pateikti išorės šaliai.

13.1.14. laikyti KN perduotus tvarkyti asmens duomenis taikant tinkamas duomenų saugumo priemones, nustatytas vadovaujantis BDAR 32 str. bei 2020 m. birželio 18 d. Valstybinės duomenų apsaugos inspekcijos Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėse duomenų valdytojams ir duomenų tvarkytojams.

13.1.15. pateikti KN informaciją apie taikomas duomenų saugumo priemones, užpildant KN apklausos anketą dėl taikomų asmens duomenų apsaugos priemonių KN duomenų tvarkytojams bei kitus KN prašomus dokumentus taikomoms duomenų saugumo priemonėms pagrįsti.

13.2. Išorės šaliai draudžiama:

13.2.1. skenuoti *KN* informacines sistemas ar *KN* duomenų perdavimo tinklą, ieškant pažeidžiamumų ar kitais būdais stebėti *KN* duomenų perdavimo tinklo srautą. Jei šiame punkte išvardintos priemonės, reikalingos tiesioginėms pareigoms atlikti, jas panaudoti galima tik suderinus su už informacijos ir kibernetinį saugumą *KN* atsakingu asmeniu.

13.2.2. be atskiro *KN* leidimo ir žinios prie *KN* duomenų perdavimo tinklo ar informacinių sistemų jungtis naudojant ne *KN* išduotą įrangą (išskyrus *KN* svečiams skirtame belaidžiame tinkle).

13.2.3. gerti, valgyti ir rūkyti šalia informacijos apdorojimo priemonių.

13.2.4. savavališkai keisti suteiktus tinklo parametrus (IP adresą ir pan.).

13.2.5. naudoti programas, kurios gali trikdyti *KN* informacinių sistemų bei duomenų perdavimo tinklo veikimą (duomenų perdavimo tinklo skenavimo ir blokavimo programos ir pan.).

13.2.6. savarankiškai keisti ir taisyti *KN* išduotą techninę ir programinę įrangą.

13.2.7. naudoti *KN* išduotą techninę ir programinę įrangą Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižikiško, įžeidžiančio, grasinamojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai veiklai, kompiuterių virusams, masinei piktybiškai informacijai siųsti ar kitiems tikslams, kurie gali pažeisti *KN* ar kitų asmenų teisėtus interesus.

13.2.8. diegti, saugoti naudoti, kopijuoti ar platinti nelegalią, autorines teises pažeidžiančią programinę įrangą.

14. Atsakomybė ir ginčų sprendimo tvarka

14.1. Kiekvienas ginčas, nesutarimas ar reikalavimas, kylantis iš *Reikalavimų* ar susijęs su *Reikalavimais*, jų pažeidimu, nutraukimu bei galiojimu, turi būti sprendžiamas *Sutartyje* nustatyta tvarka.

14.2. *Išorės šalis* yra atsakinga už visas būtinas priemones ir veiksmus siekiant laikytis šių *Reikalavimų* bei kituose taikomuose teisės aktuose nustatytų pareigų vykdymą.

14.3. Jei dėl *Išorės šalies* veiksmų ar neveikimo vykdant *Sutartį* Lietuvos Respublikos kibernetinio saugumo įstatyme numatytoms kontroliuojančioms institucijoms nustačius informacijos ir kibernetinio saugumo pažeidimą *KN* skiriama piniginė sankcija, *Išorės šalis* įsipareigoja *KN* pareikalavus atlyginti *KN* tokios sankcijos sumą, laikantis *Sutartyje* numatytos baudų sumokėjimo *KN* tvarkos.

14.4. Už *Išorės šalies* pasitelktų trečiųjų asmenų vykdomą tinkamą *Reikalavimų* įgyvendinimą prieš *KN* atsako *Išorės šalis*.

15. Reikalavimų galiojimas ir baigiamosios nuostatos

15.1. Šie *Reikalavimai* yra 3.5. punkte nurodytų sutarčių neatsiejama dalis, kai tai numatyta su *Išorės šalimi* sudaromoje *Sutartyje,* arba kai dėl šių *Reikalavimų* taikymo KN ir *Išorės šalis* susitarė kitu būdu. Reikalavimai, apibrėžti *Sutartyje* ir papildomi susitarimai, įskaitant dėl asmens duomenų tvarkymo, kai jie sudaryti, yra viršesni už šiuos *Reikalavimus*.

15.2. *Reikalavimų* galiojimas *Išorės šaliai* yra neatsiejamas nuo *KN* ir *Išorės šalies* sudarytos *Sutarties* galiojimo termino.

15.3. Bet kurios iš *Reikalavimų* sąlygos pripažinimo negaliojančia dėl prieštaravimo imperatyvioms teisės aktų nuostatoms atveju, ši sąlyga keičiama, vadovaujantis bendra *Sutartyje* nustatyta tvarka;

15.4. Šie *Reikalavimai* nėra atskirai pasirašomi. *Reikalavimai* yra skelbiami *KN* internetiniame puslapyje https://www.kn.lt arba kitame *Išorės šaliai* prieinamame šaltinyje, arba sudarant kitokią individualią ar viešo pobūdžio prieigą prie *Reikalavimų*.

SUDERINTA
Akcinės bendrovės „Klaipėdos nafta“
duomenų apsaugos pareigūnė

UAB „Juridicon“ teisininkė Miglė Žvinytė
2021-11-12 paraiška Nr. DAP-1873