



Autentiškas vertimas
Vyriausybės kanceliarijos
Dokumentų valdymo skyrius
2018 09 21
Dokumentų valdymo skyriaus
vyriausioji patarėja
D. Čekatauskienė
(Čekatauskienė)

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS
IR
VOKIETIJOS FEDERACINĖS RESPUBLIKOS VYRIAUSYBĖS
SUSITARIMAS
DĖL KEITIMOSI ĮSLAPTINTA INFORMACIJA IR
ĮSLAPTINTOS INFORMACIJOS ABIPUSĖS APSAUGOS

Lietuvos Respublikos Vyriausybė ir Vokietijos Federacinės Respublikos Vyriausybė (toliau – Susitariančiosios Šalys),

pripažindamos, kad norint veiksmingai bendradarbiauti politikos, ekonomikos, karinėje ir kitose srityse Šalims gali prireikti keistis įslaptinta informacija;

ketindamos užtikrinti įslaptintos informacijos, kuria keičiasi Lietuvos Respublikos ir Vokietijos Federacinės Respublikos kompetentingos institucijos, taip pat įslaptintos informacijos, kuria keičiamasi su tiekėjais arba kuria keičiasi dviejų Susitariančiųjų Šalių tiekėjai, apsaugą;

atsižvelgdamos į 1998 m. kovo 5 d. pasirašytą Lietuvos Respublikos Vyriausybės ir Vokietijos Federacinės Vyriausybės sutartį dėl įslaptintos informacijos abipusės apsaugos;

pripažindamos jų valstybėse taikytinus teisės aktus, kuriais reglamentuojama įslaptintos informacijos apsauga,

susitarė:

1 straipsnis

Tikslas ir taikymo sritis

Šio Susitarimo tikslas – nustatyti keitimosi įslaptinta informacija ir įslaptintos informacijos abipusės apsaugos taisykles, taikomas visai įslaptintai informacijai, kuria keičiamasi, kuri parengiama ar tvarkoma Susitariančiosioms Šalims bendradarbiaujant, įskaitant įslaptintus sandorius, veiklą ar susitarimus, kuriuos įgyvendinant keičiamasi įslaptinta informacija.

2 straipsnis

Apibrėžtys

Šiame Susitarime:

1. „įslaptinta informacija“

a) Vokietijos Federacinėje Respublikoje – faktai, duomenys ar žvalgybos informacija, kurie, nepaisant jų pateikimo būdo ir atsižvelgiant į viešąjį interesą, turi būti laikomi

paslapyje. Juos įslaptina oficiali įstaiga arba jie įslaptinami tokios įstaigos prašymu siekiant juos apsaugoti;

b) Lietuvos Respublikoje – informacija, neatsižvelgiant į jos formą ir parengimo ar perdavimo būdus, kuri vadovaujantis teisės aktais laikoma įslaptinta ir yra pažymėta nacionalinėmis slaptumo žymomis;

2. „įslaptintas sandoris“ – tai vienos iš Susitariančiųjų Šalių valstybės institucijos ar ūkio subjekto ir kitos Susitariančiosios Šalies valstybės ūkio subjekto (tiekėjo) sandoris, kurį vykdant keičiamasi įslaptinta informacija arba ji parengiama.

3 straipsnis

Atitikmenys

Susitariančiosios Šalys nustato, kad pagal jų valstybėse taikytinus teisės aktus toliau nurodytos slaptumo žymos laikomos atitikmenimis ir kad įslaptinta informacija žymima taip:

Lietuvos Respublikoje	Vokietijos Federacinėje Respublikoje	Atitikmuo anglų kalba
VISIŠKAI SLAPTAI	STRENG GEHEIM	TOP SECRET
SLAPTAI	GEHEIM	SECRET
KONFIDENCIALIAI	VS-VERTRAULICH	CONFIDENTIAL
RIBOTO NAUDOJIMO	VS-NUR FÜR DEN DIENSTGEBRAUCH	RESTRICTED

4 straipsnis

Slaptumo žymos

1. Gautą įslaptintą informaciją 3 straipsnyje nurodyta atitinkama nacionaline slaptumo žyma žymi gavėjo kompetentinga institucija arba tokia informacija žymima šios institucijos prašymu.

2. Atitinkamai žymima įslaptinta informacija, parengta informaciją gaunančios Susitariančiosios Šalies valstybėje įgyvendinant įslaptintus sandorius, taip pat jos kopijos, padarytos informaciją gaunančios Susitariančiosios Šalies valstybėje.

3. Slaptumo žymos negali būti keičiamos ar atšaukiamos be informaciją parengusios Susitariančiosios Šalies kompetentingos institucijos leidimo.

4. Informaciją parengusios Susitariančiosios Šalies kompetentinga institucija nedelsdama praneša kitos Susitariančiosios Šalies kompetentingai institucijai apie bet kurios slaptumo žymos pakeitimą ar atšaukimą.

5 straipsnis

Kompetentingos institucijos

1. Susitarimui įsigaliojus, Susitariančiosios Šalys nedelsdamos raštu praneša viena kitai išsamią informaciją apie savo atitinkamą nacionalinę saugumo instituciją (toliau – NSI) ar paskirtąją saugumo instituciją (toliau – PSI) ir prirėikus atnaujina šią informaciją.

2. Susitariančiųjų Šalių NSI ar PSI, keisdamosi su bendradarbiavimu susijusia informacija, bendrauja valstybine tos institucijos, kuriai pateikiama informacija, kalba arba anglų kalba.

6 straipsnis

Nacionalinės saugumo priemonės

1. Vadovaudamosi jų valstybėse taikytiniais teisės aktais Susitariančiosios Šalys imasi visų tinkamų priemonių siekdamos užtikrinti įslaptintos informacijos, kuri parengiama, kuria keičiamasi arba kuri tvarkoma pagal šio Susitarimo nuostatas, apsaugą. Tokiai įslaptintai informacijai Susitariančiosios Šalys suteikia bent tokį pat apsaugos lygį, kokį informaciją gaunanti Susitariančioji Šalis užtikrina savo atitinkamo slaptumo lygio įslaptintai informacijai.

2. Įslaptinta informacija naudojama tik nustatytu tikslu. Gavėjas neatskleidžia įslaptintos informacijos ar jos nenaudoja arba neleidžia jos atskleisti ar naudoti, išskyrus tuos atvejus, kai tai atitinka rengėjo ar jo vardu nustatytus tikslus ir laikomasi jo ar jo vardu nustatytų apribojimų. Norint susitarti kitaip, būtina gauti rašytinį įslaptintos informacijos rengėjo sutikimą.

3. Įslaptinta informacija verčiama, kopijuojama ir naikinama vadovaujantis Susitariančiųjų Šalių valstybėse taikytinų teisės aktų nuostatomis, kurios galioja jų pačių atitinkamo slaptumo lygio įslaptintai informacijai.

4. Prieiga prie įslaptintos informacijos gali būti suteikiama tik tiems asmenims, kuriems būtina ją žinoti ir kurie turi patikimumo pažymėjimą arba yra tinkami susipažinti su įslaptinta informacija pagal jų atliekamas tarnybines pareigas. Patikimumo pažymėjimas išduodamas tik atlikus patikimumo patikrinimą vadovaujantis ne mažiau griežtais standartais nei tie, kurie taikomi prieigai prie nacionalinės atitinkamo slaptumo lygio įslaptintos informacijos. Suteikiant prieigą prie RIBOTO NAUDOJIMO / VS NUR FÜR DEN DIENSTGEBRAUCH lygio įslaptintos informacijos vadovujamasi valstybėse taikytiniais teisės aktais.

5. Prieiga prie KONFIDENCIALIAI / VS-VERTRAULICH arba SLAPTAI / GEHEIM lygio įslaptintos informacijos vienos iš Susitariančiųjų Šalių valstybės piliečiui suteikiama be išankstinio informaciją parengusios Susitariančiosios Šalies leidimo.

6. Susitariančiosios Šalies valstybės piliečių, kurie gyvena toje valstybėje ir kuriems reikalinga prieiga prie įslaptintos informacijos, asmens patikimumo patikrinimą (toliau – APP) atlieka tos valstybės NSI ar PSI arba kitos nacionalinės kompetentingos institucijos.

7. Susitariančiosios Šalies valstybės piliečių, kurie ne trumpiau kaip 5 metus teisėtai gyvena kitos Susitariančiosios Šalies valstybėje ir siekia dirbti su įslaptinta informacija susijusį darbą toje valstybėje, asmens patikimumo patikrinimą, vadovaudamasi jos valstybėje

taikytiniais teisės aktais, atlieka tos Susitariančiosios Šalies kompetentinga saugumo institucija, kuri prireikus atlieka patikras pasienyje.

8. Susitariančiosios Šalys užtikrina, kad jų valstybėse būtų atlikti būtini saugumo patikrinimai ir laikomasi šio Susitarimo nuostatų.

7 straipsnis

Įslaptintų sandorių sudarymas

1. Prieš sudarydamas KONFIDENCIALIAI / VS-VERTRAULICH ar aukštesnio lygio įslaptintą sandorį užsakovas, norėdamas įsitikinti, ar būsimam tiekėjui jo valstybės NSI ar PSI taiko saugumo priežiūrą ir ar tas tiekėjas ėmėsi saugumo priemonių, kurios būtinos norint pradėti vykdyti sandorį, per savo atitinkamą NSI ar PSI gauna iš tiekėjo NSI ar PSI tiekėjo patikimumo pažymėjimą (TPP). Jei TPP tiekėjui dar neišduotas, gali būti teikiamas prašymas jį gauti.

2. TPP būtina gauti ir tuo atveju, jei ūkio subjektas buvo paprašytas pateikti pasiūlymą ir jei įslaptinta informacija bus teikiama prieš sudarant įslaptintą sandorį pagal pasiūlymų teikimo procedūrą.

3. Nurodytais 1 ir 2 dalyse atvejais taikoma tokia procedūra:

1) prašymuose išduoti TPP kitos Susitariančiosios Šalies valstybės tiekėjams nurodoma informacija apie projektą, taip pat apie įslaptintos informacijos, kuri gali būti teikiama tiekėjui arba kurią tiekėjas gali būti prašomas parengti, pobūdį, mastą ir slaptumo lygį;

2) TPP turi būti nurodomas ne tik visas ūkio subjekto pavadinimas, jo pašto adresas, saugumo pareigūno ar pareigūnės vardas ir pavardė, jo ar jos telefono ir fakso numeriai, el. pašto adresas, bet ir išsami informacija apie saugumo priemonių, kurių ėmėsi atitinkamas ūkio subjektas vadovaudamasis valstybėje taikytiniais teisės aktais, mastą ir jomis užtikrinamą įslaptintos informacijos saugumo lygį;

3) Susitariančiųjų Šalių NSI ar PSI praneša viena kitai apie visus faktų, kuriais remiantis buvo išduoti tiekėjo patikimumo pažymėjimai, pasikeitimus;

4) TPP ir Susitariančiųjų Šalių atitinkamoms NSI ar PSI skirti prašymai išduoti TPP teikiami raštu.

4. RIBOTO NAUDOJIMO / VS-NUR FÜR DEN DIENSTGEBRAUCH lygio įslaptintų sandorių atveju vadovaujamosi valstybėse taikytiniais teisės aktais.

8 straipsnis

Įslaptintų sandorių vykdymas

1. Į KONFIDENCIALIAI / VS-VERTRAULICH lygio ar aukštesnio slaptumo lygio įslaptintus sandorius turi būti įtraukta saugumo reikalavimus apimanti nuostata, kuria tiekėjas įpareigojamas imtis priemonių, būtinų įslaptintai informacijai apsaugoti vadovaujantis jo valstybėje taikytiniais teisės aktais.

2. Be to, saugumo reikalavimų nuostatoje turi būti nurodyta:

1) Susitariančiųjų Šalių valstybių slaptumo žymų atitikmenys vadovaujantis šio Susitarimo nuostatomis;

2) kiekvienos Susitariančiosios Šalies kompetentingų institucijų, įgaliotų arba teikti su įslaptintu sandoriu susijusią įslaptintą informaciją, arba koordinuoti jos apsaugą, pavadinimai;

3) kanalai, kuriais naudosis kompetentingos institucijos ir susiję tiekėjai perduodami įslaptintą informaciją;

4) tvarka ir būdai, kuriais bus naudojamosi pranešant apie galimus su įslaptinta informacija susijusius pasikeitimus, kai keičiamos slaptumo žymos arba informacija išslaptinama;

5) tiekėjų personalo vizitų patvirtinimo tvarka;

6) įslaptintos informacijos perdavimo tiekėjams, kurie tvarkys tą informaciją, tvarka;

7) reikalavimas, kad tiekėjas suteiktų prieigą prie įslaptintos informacijos tik tam asmeniui, kuriam būtina ją žinoti, kuris buvo iš anksto patikrintas ir jau turi leidimą susipažinti su atitinkamo lygio įslaptinta informacija;

8) reikalavimas, kad įslaptinta informacija būtų atskleista arba ją būtų leidžiama atskleisti trečiajai šaliai tik tuo atveju, jei tam raštu pritaria rengėjas;

9) reikalavimas, kad tiekėjas nedelsdamas praneštų savo NSI ar PSI apie įslaptintos informacijos, kuriai taikomos įslaptinto sandorio nuostatos, faktinį ar įtariamą praradimą, nutekėjimą arba neteisėtą atskleidimą;

10) reikalavimas, kad tiekėjas praneštų savo NSI ar PSI apie įslaptinto sandorio sudarymą; ir

11) reikalavimas, kad subrangovai gali būti įtraukiami į sandorį tik gavus išankstinį rengėjo sutikimą. 7 ir 8 straipsnių nuostatos taikomos ir subrangovams.

3. Užsakovo kompetentinga institucija pateikia tiekėjui atskirą visų dokumentų, kuriuos būtina žymėti slaptumo žyma, sąrašą (įslaptinimo vadovą), nustato reikiamą įslaptinimo lygį ir užtikrina, kad šis įslaptinimo vadovas būtų pridėtas prie įslaptinto sandorio kaip priedas. Užsakovo kompetentinga institucija perduoda tiekėjo kompetentingai institucijai šį įslaptinimo vadovą arba organizuoja jo perdavimą.

4. Rengėjas užtikrina, kad tiekėjui būtų suteikta prieiga prie įslaptintos informacijos tik po to, kai iš tiekėjo NSI ar PSI bus gautas atitinkamas TPP.

5. RIBOTO NAUDOJIMO / VS-NUR FÜR DEN DIENSTGEBRAUCH lygio įslaptintų sandorių atveju vadovaujamosi valstybėse taikytiniais teisės aktais.

9 straipsnis

Įslaptintos informacijos perdavimas

1. VISIŠKAI SLAPTAI / STRENG GEHEIM lygio įslaptintą informaciją Susitariančiosios Šalys perduoda viena kitai tik savo vyriausybių kanalais, vadovaudamosi atitinkamais jų valstybėse taikytiniais teisės aktais.

2. KONFIDENCIALIAI / VS-VERTRAULICH lygio ir SLAPTAI / GEHEIM lygio įslaptintą informaciją iš vienos valstybės į kitą valstybę paprastai perduoda oficialus kurjeris. Susitariančiųjų Šalių NSI ar PSI gali susitarti dėl kitų informacijos perdavimo kanalų. Įslaptinta informacija gavėjui perduodama vadovaujantis valstybėse taikytiniais teisės aktais, o įslaptintos informacijos gavimą patvirtina kompetentinga institucija arba informacijos gavimas patvirtinamas jos vardu.

3. NSI ar PSI, taikydamos apribojimus arba jų netaikydamos, gali susitarti, kad KONFIDENCIALIAI / VS-VERTRAULICH lygio ir SLAPTAI / GEHEIM lygio įslaptintą informaciją būtų galima perduoti ne tik per oficialų kurjerį, bet ir kitais kanalais. Tokiais atvejais:

1) informaciją pristatantis subjektas turi turėti leidimą susipažinti su atitinkamo slaptumo lygio įslaptinta informacija;

2) siuntėjas turi saugoti perduotos įslaptintos informacijos dokumentų sąrašą; šio sąrašo kopija perduodama gavėjui, kuris turi ją perduoti kompetentingai institucijai;

3) įslaptintos informacijos dokumentai pakuojami vadovaujantis vežimą valstybės teritorijoje reglamentuojančiomis taisyklėmis;

4) įslaptintos informacijos dokumentai įteikiami paprašius patvirtinti jų gavimą; ir

5) informaciją pristatantis subjektas turi turėti siuntėjo arba gavėjo kompetentingos institucijos išduotą kurjerio sertifikatą.

4. Nurodytais 3 dalyje atvejais dėl transporto priemonių, maršruto ir prireikus palydos kompetentingos institucijos tariai kiekvienu atveju atskirai, vadovaudamosi išsamiau vežimo planu.

5. KONFIDENCIALIAI / VS-VERTRAULICH lygio arba SLAPTAI / GEHEIM lygio įslaptinta informacija elektroniniu būdu perduodama tik šifruota. Nurodytų slaptumo lygių įslaptinta informacija gali būti šifruojama tik tokiais šifravimo būdais, kuriuos bendru sutarimu patvirtina Susitariančiųjų Šalių NSI ar PSI.

6. RIBOTO NAUDOJIMO / VS-NUR FÜR DEN DIENSTGEBRAUCH lygio įslaptinta informacija kitos Susitariančiosios Šalies valstybės teritorijoje esantiems gavėjams gali būti perduodama paštu arba naudojantis kitomis pristatymo paslaugomis pagal valstybėse taikytinus teisės aktus.

7. RIBOTO NAUDOJIMO / VS-NUR FÜR DEN DIENSTGEBRAUCH lygio įslaptinta informacija gali būti perduodama elektroniniu būdu arba gali tapti prieinama naudojantis atitinkamos kompetentingos saugumo institucijos patvirtinta komercine šifravimo įranga.

10 straipsnis

Vizitai

1. Teisė susipažinti su įslaptinta informacija kitos Susitariančiosios Šalies valstybėje suteikiama ir patekti į patalpas, kuriose dirbama su įslaptinta informacija, paprastai suteikiama tik tiems iš vienos Susitariančiosios Šalies valstybės atvykusiems asmenims, kurie turi tos Susitariančiosios Šalies, kurios valstybėje bus lankomasi, NSI ar PSI iš anksto išduotą leidimą.

Toks leidimas išduodamas tik tiems asmenims, kuriems būtina žinoti įslaptintą informaciją ir kurie turi teisę su ja susipažinti.

2. Prašymai surengti vizitą turi būti pateikti laiku tos valstybės, į kurios teritoriją atvykstantys asmenys nori patekti, kompetentingai institucijai, vadovaujantis jos teisės aktais. Kompetentingos institucijos perduoda viena kitai išsamią informaciją apie tokius prašymus ir užtikrina asmens duomenų apsaugą.

3. Prašymai surengti vizitą teikiami valstybės, į kurią norima atvykti, valstybine kalba arba anglų kalba; juose nurodoma tokia informacija:

1) atvykstančio asmens vardas ir pavardė, gimimo data ir vieta, paso ar tapatybės kortelės numeris;

2) atvykstančio asmens pilietybė;

3) atvykstančio asmens tarnybos pavadinimas, aukštesniosios institucijos ar įstaigos pavadinimas;

4) atvykstančio asmens patikimumo pažymėjimo, leidžiančio susipažinti su įslaptinta informacija, lygis;

5) vizito tikslas ir numatoma data; ir

6) įstaigų pavadinimai, kontaktiniai asmenys ir patalpos, kuriose ketinama apsilankyti.

4. Jei vizitų metu bus susipažįstama su RIBOTO NAUDOJIMO / VS-NUR FÜR DEN DIENSTGEBRAUCH slaptumo lygio informacija, vadovaujama valstybėse taikytiniais teisės aktais, ypač kai tai susiję su Susitariančiosios Šalies, kurioje lankomasi, piliečiais.

11 straipsnis

Konsultacijos ir ginčų sprendimas

1. Susitariančiosios Šalys atsižvelgia į jų valstybėse taikytinus teisės aktus, kurie reglamentuoja įslaptintos informacijos apsaugą ir kurie galioja kitos Susitariančiosios Šalies valstybėje.

2. Siekdamas užtikrinti glaudų bendradarbiavimą įgyvendinant šį Susitarimą, NSI ar PSI konsultuojasi tarpusavyje, vienai iš šių institucijų paprašius.

3. Be to, kiekviena Susitariančioji Šalis leidžia kitos Susitariančiosios Šalies NSI ar PSI arba kurios nors kitos bendru sutarimu paskirtos institucijos atstovams atvykti į jos valstybės teritoriją aptarti su jos NSI ar PSI įslaptintos informacijos, gautos iš kitos Susitariančiosios Šalies, apsaugos procedūras ir sąlygas. Kiekviena Susitariančioji Šalis padeda tai institucijai įsitikinti, ar iš kitos Susitariančiosios Šalies gauta įslaptinta informacija tinkamai saugoma.

4. Visi Susitariančiųjų Šalių ginčai dėl šio Susitarimo aiškinimo ar taikymo sprendžiami tik Susitariančiųjų Šalių konsultacijomis ar derybomis ir neperduodami spręsti nacionaliniam ar tarptautiniam tribunolui arba trečiajai šaliai.

12 straipsnis

Nuostatų, reglamentuojančių įslaptintos informacijos abipusę apsaugą, pažeidimas

1. Jei negalima atmesti galimybės, kad įslaptinta informacija buvo neteisėtai atskleista, arba jei toks atskleidimas įtariamas ar nustatomas, apie tai nedelsiant pranešama kitai Susitariančiajai Šaliai.

2. Nuostatų, reglamentuojančių įslaptintos informacijos abipusę apsaugą, pažeidimai tiriami, o Susitariančiosios Šalies valstybės kompetentingos institucijos ir teismai, kurių jurisdikcijai tai priklauso, imasi atitinkamų teisinių veiksmų vadovaudamiesi jų valstybėse taikytiniais teisės aktais. Kita Susitariančioji Šalis padeda atlikti minėtus tyrimus, jei jos to prašoma, ir yra informuojama apie tyrimų rezultatus.

13 straipsnis

Išlaidos

Kiekviena Susitariančioji Šalis padengia savo išlaidas, patirtas įgyvendinant šio Susitarimo nuostatas.

14 straipsnis

Ryšys su kitais susitarimais, sutartimis ir susitarimo memorandumais

Šis Susitarimas neturi įtakos šiuo metu galiojantiems Susitariančiųjų Šalių arba kompetentingų institucijų susitarimams, sutartims ir susitarimo memorandumams dėl įslaptintos informacijos apsaugos tiek, kiek jie neprieštarauja jo nuostatoms.

15 straipsnis

Baigiamosios nuostatos

1. Šis Susitarimas įsigalioja tą dieną, kurią Lietuvos Respublikos Vyriausybė praneša Vokietijos Federacinės Respublikos Vyriausybei įvykdžiusi nacionalinius reikalavimus, būtinus šiam Susitarimui įsigalioti. Susitarimo įsigaliojimo diena yra pranešimo gavimo diena.

2. Šis Susitarimas sudaromas neribotam laikui.

3. Šis Susitarimas gali būti keičiamas abipusiu rašytiniu Susitariančiųjų Šalių sutarimu. Bet kuri Susitariančioji Šalis gali bet kada pateikti rašytinį prašymą pakeisti šį Susitarimą. Jei tokį prašymą pateikia viena iš Susitariančiųjų Šalių, Susitariančiosios Šalys pradeda derybas dėl Susitarimo pakeitimo. Tokie pakeitimai įsigalioja šio straipsnio 1 dalyje nustatyta tvarka.

4. Bet kuri Susitariančioji Šalis gali denonsuoti šį Susitarimą, diplomatiniais kanalais prieš šešis mėnesius perduodama rašytinį pranešimą. Denonsavimo atveju pagal šį Susitarimą perduota arba tiekėjo parengta informacija ir toliau tvarkoma vadovaujantis 5 straipsnio nuostatomis tol, kol informacija laikoma įslaptinta.

5. Kai tik Susitarimas įsigalioja, ta Susitariančioji Šalis, kurios valstybėje jis buvo pasirašytas, inicijuoja jo registravimą Jungtinių Tautų sekretoriato vadovaudamasi Jungtinių

Tautų Chartijos 102 straipsniu. Kitai Susitariančiai Šaliai pranešama apie registravimą, nurodant JT registracijos numerį, kai tik tai patvirtina Jungtinių Tautų sekretoriatas.

6. Įsigaliojus šiam Susitarimui, 1998 m. gegužės 5 d. Lietuvos Respublikos Vyriausybės ir Vokietijos Federacinės Vyriausybės sutartis dėl įslaptintos informacijos abipusės apsaugos netenka galios. Įsigaliojęs šis Susitarimas taikomas ir įslaptintai informacijai, kuria pasikeista pagal 1998 m. gegužės 5 d. Lietuvos Respublikos Vyriausybės ir Vokietijos Federacinės Vyriausybės sutartį dėl įslaptintos informacijos abipusės apsaugos.

Pasirašyta d. dviem originaliais egzemplioriais lietuvių, vokiečių ir anglų kalbomis. Visi trys tekstai yra autentiški. Kilus nesutarimų dėl tekstų lietuvių ir vokiečių kalbomis aiškinimo, vadovaujamasi tekstu anglų kalba.

**Lietuvos Respublikos
Vyriausybės vardu**

**Vokietijos Federacinės Respublikos
Vyriausybės vardu**

Agreement

between

the Government of the Federal Republic of Germany

and

the Government of the Republic of Lithuania

on the

Exchange and Mutual Protection of Classified Information

The Government of the Federal Republic of Germany
and
the Government of the Republic of Lithuania
(hereinafter referred to as the Contracting Parties),

Recognising that effective co-operation in political, economic, military and any other area may require exchange of classified information,

Intending to ensure the protection of classified information that is exchanged between the competent authorities of the Federal Republic of Germany and the Republic of Lithuania as well as with contractors or between contractors of the Contracting Parties,

Referring to the Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Lithuania on the mutual protection of classified information of 5 March 1998,

Acknowledging nationally applicable laws and regulations governing the protection of classified information,

Have agreed as follows:

Article 1 Objective and Scope

The objective of this Agreement is to establish a set of rules regulating the exchange and mutual protection of classified information that shall apply to all classified information exchanged, generated or handled in the process of cooperation between the Contracting Parties including classified contracts, activities or arrangements involving an exchange of classified information.

Article 2
Definitions

For the purposes of this Agreement

1. “classified information” is

(a) in the Federal Republic of Germany

facts, items or intelligence which, regardless of how they are presented, are to be kept secret in the public interest. They shall be classified by, or at the instance of, an official agency in accordance with their need for protection;

(b) in the Republic of Lithuania

any data, regardless of its form and the means it was generated or transmitted that in accordance with laws and regulations was recognized as classified and is marked with national classification markings;

2. a “classified contract” is a contract between an authority or an enterprise from the state of one Contracting Party and an enterprise from the state of the other Contracting Party (contractor) which involves the exchange and generation of Classified Information.

Article 3
Comparability

The Contracting Parties stipulate that according to the nationally applicable laws and regulations the following classifications shall be comparable and that classified information

shall be marked as follows:

Federal Republic of Germany	Republic of Lithuania	Equivalent in English
STRENG GEHEIM	VISIŠKAI SLAPTAI	TOP SECRET
GEHEIM	SLAPTAI	SECRET
VS-VERTRAULICH	KONFIDENCIALIAI	CONFIDENTIAL
VS-NUR FÜR DEN DIENSTGEBRAUCH	RIBOTO NAUDOJIMO	RESTRICTED

Article 4

Classification Markings

- (1) Received classified information shall be marked with the comparable national classification as provided under Article 3 by, or at the instance of, the competent authority of the recipient.
- (2) Classified information which is generated in the state of the receiving Contracting Party in connection with classified contracts as well as copies made in the state of the receiving Contracting Party shall be marked accordingly.
- (3) Classifications shall not be amended or revoked without authorization of the competent authority of the originating Contracting Party.
- (4) The competent authority of the originating Contracting Party shall inform the competent authority of the other Contracting Party immediately of the amendment or revocation of any classification.

Article 5

Competent Authorities

(1) The Contracting Parties shall inform each other in writing about the details of their respective National Security Authorities (hereinafter – NSAs) or Designated Security Authorities (hereinafter – DSAs) immediately after the Agreement has entered into force and shall also provide updates to these details as necessary.

(2) The exchange of cooperation related information between the NSAs or DSAs of the Contracting Parties shall be effected either in the national language of the authority to be informed or in English.

Article 6

National Security Measures

(1) Within the scope of their nationally applicable laws and regulations, the Contracting Parties shall take all appropriate measures to guarantee the protection of classified information generated, exchanged or handled under the terms of this Agreement. They shall afford such classified information a degree of protection at least equal to that required by the receiving Contracting Party for its own classified information of the comparable level of classification.

(2) The classified information shall be used solely for the designated purpose. The recipient shall not disclose or use, or permit the disclosure or use of, any classified information except for the purposes and within any limitations stated by or on behalf of the originator. The originator of the classified information must have given its written consent to any arrangement to the contrary.

(3) The translation, reproduction and destruction of classified information shall be carried out according to the provisions that are set in the nationally applicable laws and regulations

of the Contracting Parties for their own classified information of the comparable level of classification.

(4) Access to classified information may be granted only to individuals having a need-to-know and – having been security-cleared or being eligible to access classified information by virtue of their function. Security clearance shall be granted only after completion of a security screening under standards no less stringent than those applied for access to national classified information of the comparable classification level. In the case of classified information at the VS-NUR FÜR DEN DIENSTGEBRAUCH/RIBOTO NAUDOJIMO level nationally applicable laws and regulations apply.

(5) Access to classified information at the VS-VERTRAULICH/KONFIDENCIALIAI or GEHEIM/SLAPTAI level by a national of the state of one Contracting Party shall be granted without the prior authorization of the originating Contracting Party.

(6) Personnel Security Clearances (hereinafter – PSCs) for nationals of the state of one Contracting Party who reside and require access to classified information in their own state shall be undertaken by their NSAs or DSAs or other competent national authorities.

(7) In accordance with nationally applicable laws and regulations PSCs for nationals of the state of a Contracting Party who have been legally resident in the territory of the state of the other Contracting Party for at least 5 years and apply for a security-sensitive job in that state shall be undertaken by the competent security authority of the latter Contracting Party conducting cross-border checks as appropriate.

(8) The Contracting Parties shall, each within their state, ensure that the necessary security inspections are carried out and that this Agreement is complied with.

Article 7

Award of Classified Contracts

(1) Prior to the award of a classified contract of the VS-VERTRAULICH/KONFIDENCIALIAI level or higher, the contract owner shall, through its respective NSA or DSA, obtain a Facility Security Clearance (hereinafter – FSC) from the NSA or DSA of the contractor in order to obtain assurance as to whether the prospective contractor is subject to security oversight by the NSA or DSA of its state and whether such contractor has taken the security precautions required for discharging the performance of the classified contract. Where a contractor has not yet been granted an FSC, an application may be made to that end.

(2) An FSC shall also be obtained if an enterprise has been requested to submit a bid and if classified information will have to be released prior to the award of a classified contract under the bid procedure.

(3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:

1. Requests for the issuance of an FSC for contractors from the state of the other Contracting Party shall contain information on the project as well as the nature, the scope and the level of classification of the classified information expected to be released to the contractor or to be generated by it.
2. In addition to the full name of the enterprise, its postal address, the name of its security official, his or her telephone, fax number and e-mail address, FSCs must include information in particular on the extent to which, and the level of classification up to which, security measures have been taken by the respective enterprise on the basis of nationally applicable laws and regulations.
3. The NSAs or DSAs of the Contracting Parties shall inform each other of any

changes in the facts covered by the issued FSCs.

4. FSCs and requests addressed to the respective NSAs or DSAs of the Contracting Parties for the issuance of FSCs shall be transmitted in writing.

(4) In the case of classified contracts at the VS-NUR FÜR DEN DIENSTGEBRAUCH/RIBOTO NAUDOJIMO level nationally applicable laws and regulations apply.

Article 8

Performance of Classified Contracts

(1) Classified contracts of the VS-VERTRAULICH/KONFIDENCIALIAI level or higher must contain a security requirements clause under which the contractor is under an obligation to make the arrangements required for the protection of classified information pursuant to the nationally applicable laws and regulations of its state.

(2) In addition, the security requirements clause shall contain the following provisions:

1. the comparable classifications of the states of the Contracting Parties in accordance with the provisions of this Agreement;
2. the names of the competent authorities of each Contracting Party empowered either to authorize the release or to coordinate the safeguarding of classified information related to the classified contract;
3. the channels to be used for the transfer of classified information between the competent authorities and contractors involved;
4. the procedures and mechanisms for communicating changes that may arise in

respect of classified information either because of changes in its classification level or its declassification;

5. the procedures for the approval of visits of the contractor's personnel;
6. the procedures for transmitting classified information to contractors where such information is to be handled;
7. the requirement that the contractor shall grant access to classified information only to a person who has a need-to-know, has been security-cleared and authorized to the appropriate level in advance;
8. the requirement that classified information shall only be disclosed to a third party, or that such disclosure shall only be permitted, if this has been approved by the originator in writing;
9. the requirement that the contractor shall immediately notify its NSA or DSA of any actual or suspected loss, leak or unauthorized disclosure of the classified information covered by the classified contract;
10. the requirement that the contractor shall inform its NSA or DSA in case it has been awarded a classified contract; and
11. the requirement that subcontractors may only be involved upon prior approval of the originator. The provisions of Articles 7 and 8 also apply to subcontractors.

(3) The competent authority of the contract owner shall provide the contractor with a separate list (classification guide) of all documentary records requiring security classification, shall determine the required classification level and shall arrange for this classification guide to be enclosed as an appendix to the classified contract. The competent authority of the contract owner shall also transmit, or arrange for the transmission of, this

classification guide to the competent authority of the contractor.

(4) The originator shall ensure that the contractor will be given access to classified information only after the appropriate FSC has been received from the NSA or DSA of the contractor.

(5) In the case of classified contracts at the VS-NUR FÜR DEN DIENSTGEBRAUCH/RIBOTO NAUDOJIMO level nationally applicable laws and regulations apply.

Article 9

Transmission of Classified Information

(1) Classified information at the STRENG GEHEIM/VISIŠKAI SLAPTAI level shall only be transmitted between Contracting Parties through Government-to-Government channels pursuant to the respective nationally applicable laws and regulations.

(2) As a matter of principle, classified information at the VS-VERTRAULICH/KONFIDENCIALIAI and GEHEIM/SLAPTAI levels shall be transmitted from one state to another by official courier. The NSAs or DSAs of the Contracting Parties may agree on alternative channels of transmission. In accordance with nationally applicable laws and regulations classified information shall be forwarded to the recipient and receipt of classified information shall be confirmed by, or at the instance of, the competent authority.

(3) The NSAs or DSAs may agree – generally or subject to restrictions – that classified information at the VS-VERTRAULICH/KONFIDENCIALIAI and GEHEIM/SLAPTAI levels may be transmitted through channels other than official courier. In such cases:

1. the bearer must be authorized to have access to classified information of the comparable level of classification;

2. a list of the items of classified information transmitted must be retained by the sender; a copy of this list shall be handed over to the recipient for forwarding to the competent authority;
 3. items of classified information must be packed in accordance with the regulations governing transportation within national boundaries;
 4. items of classified information must be delivered against receipt; and
 5. the bearer must carry a courier certificate issued by the competent authority of the sender or the recipient.
- (4) In the case referred to in paragraph (3) above, the means of transportation, the route, and, if needed, the escort shall be determined on a case-by-case basis by the competent authorities on the basis of a detailed transport plan.
- (5) The electronic transmission of classified information at the VS-VERTRAULICH/KONFIDENCIALIAI or GEHEIM/SLAPTAI level must only take place in an encrypted form. Classified information of these levels of classification may only be encrypted by encryption means approved by mutual agreement by the NSAs or DSAs of the Contracting Parties.
- (6) Classified information at the VS-NUR FÜR DEN DIENSTGEBRAUCH/RIBOTO NAUDJOJIMO level may be transmitted by post or other delivery services to recipients within the territory of the state of the other Contracting Party, taking into account nationally applicable laws and regulations.
- (7) Classified information at the VS-NUR FÜR DEN DIENSTGEBRAUCH/RIBOTO NAUDJOJIMO level may be electronically transmitted or made available by means of commercial encryption devices approved by the relevant competent security authority.

Article 10

Visits

(1) As a matter of principle, it is only with the prior permission of the NSAs or DSAs of the Contracting Party whose state is to be visited that visitors from the state of one Contracting Party will, in the state of the other Contracting Party, be granted access to classified information and to facilities in which classified information is being handled. Such permission shall be given only to individuals having a need-to-know and having been authorized to have access to classified information.

(2) Requests for visits shall be submitted, on a timely basis and in accordance with the regulations of the Contracting Party's state whose territory such visitors wish to enter, to the competent authority of that state. The competent authorities shall inform each other of the details regarding such requests and shall ensure that personal data are protected.

(3) Requests for visits shall be submitted in the language of the state to be visited or in English and shall contain the following information:

1. the visitor's first name and surname, date and place of birth, and his or her passport or identity card number;
2. the visitor's citizenship;
3. the visitor's service designation, and the name of his or her parent authority or agency;
4. the level of the visitor's security clearance for access to classified information;
5. the purpose of the visit, and the proposed date of the visit; and

6. the designation of the agencies, the contact persons and the facilities to be visited.

(4) In the case of visits that involve access to classified information at the VS-NUR FÜR DEN DIENSTGEBRAUCH/RIBOTO NAUDOJIMO level nationally applicable laws and regulations apply, especially with regard to nationals of the Contracting Party visited.

Article 11

Consultations and Settlement of Disputes

(1) The Contracting Parties shall take note of the nationally applicable laws and regulations governing the protection of classified information that apply within the state of the other Contracting Party.

(2) To ensure close cooperation in the implementation of this Agreement, the NSAs or DSAs shall consult each other at the request of one of these authorities.

(3) Each Contracting Party shall, in addition, allow the NSA or DSA of the other Contracting Party or any other authority designated by mutual agreement to visit the territory of its state in order to discuss, with its NSA or DSA, the procedures and facilities for the protection of classified information received from the other Contracting Party. Each Contracting Party shall assist that authority in ascertaining whether classified information received from the other Contracting Party is adequately protected.

(4) Any dispute between the Contracting Parties arising from the interpretation or application of this Agreement shall be resolved solely by consultation or negotiation between the Contracting Parties and shall not be referred to any national or international tribunal or third party for settlement.

Article 12

Violation of Provisions Governing the Mutual Protection of Classified Information

(1) Whenever unauthorized disclosure of classified information cannot be ruled out or if such disclosure is suspected or ascertained, the other Contracting Party shall immediately be informed.

(2) Violations of provisions governing the protection of classified information shall be investigated, and appropriate legal action shall be taken, by the competent authorities and courts in the state of the Contracting Party having jurisdiction, according to nationally applicable laws and regulations. The other Contracting Party should, if so requested, support such investigations and shall be informed of the outcome.

Article 13

Costs

Each Contracting Party shall pay the expenses incurred by it in implementing the provisions of this Agreement.

Article 14

Relationship with Other Agreements, Arrangements and Memoranda of Understanding

Any existing Agreements, Arrangements and Memoranda of Understanding between the Contracting Parties or the competent authorities on the protection of classified information shall be unaffected by the present Agreement in so far as they do not conflict with its provisions.

Article 15
Final Provisions

(1) This Agreement shall enter into force on the date on which the Government of the Republic of Lithuania has notified the Government of the Federal Republic of Germany that the national requirements for such entry into force have been fulfilled. The relevant date shall be the date of receipt of the notification.

(2) This Agreement is concluded for an indefinite period of time.

(3) This Agreement may be amended in writing by mutual agreement between the Contracting Parties. Either Contracting Party may at any time submit a written request for the amendment of this Agreement. If such a request is submitted by one of the Contracting Parties, the Contracting Parties shall initiate negotiations on the amendment of the Agreement. Such amendments shall enter into force in accordance with the provisions of paragraph 1 of this Article.

(4) Either Contracting Party may, through diplomatic channels, denounce this Agreement by giving six months' written notice. In the event of denunciation, classified information transmitted, or generated by the contractor, on the basis of this Agreement shall continue to be treated in accordance with the provisions of Article 5 above for as long as is justified by the existence of the classification.

(5) Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the Charter of the United Nations, shall be initiated by the Contracting Party in the state of which the Agreement is signed immediately following its entry into force. The other Contracting Party shall be informed of registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat of the United Nations.

(6) Upon the entry into force of this Agreement, the Agreement between the Government

of the Federal Republic of Germany and the Government of the Republic of Lithuania on the Mutual Protection of Classified Information of 5 March 1998 shall be terminated. Upon entry into force, of the present Agreement, it shall also apply to classified information exchanged under the Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Lithuania on the Mutual Protection of Classified Information of 5 March 1998.

Done at _____ on _____ in two originals, in the German, Lithuanian and English languages, all three texts being authentic. In the case of any divergence of interpretation of the German and Lithuanian texts, the English text shall prevail.

For the Government of the
Federal Republic of Germany

For the Government of
Republic of Lithuania