

PATVIRTINTA

Lietuvos Respublikos konkurencijos
tarybos pirmininko

2026 m. d. įsakymu Nr. 2V-

TIEKIMO GRANDINĖS SAUGUMO VALDYMO TVARKA

I SKYRIUS

BENDROSIOS NUOSTATOS

1. Tiekimo grandinės saugumo valdymo tvarka (toliau – Tvarka) reglamentuoja Lietuvos Respublikos konkurencijos tarybos (toliau – KT) trečiųjų šalių teikiamoms paslaugoms ir (ar) produktams (įrangai), susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra ir modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, kibernetinio saugumo, kokybės ir prieigos kontrolės reikalavimus.

2. Tvarka taikoma, kai KT bendradarbiauja (pvz., vykdo bendrus projektus, sudaro sutartis, vykdo paslaugų ir (ar) produktų pirkimą) arba planuoja bendradarbiauti su trečiaja šalimi, kurios paslaugos ir (ar) produktai, tiesiogiai ar netiesiogiai susiję su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, naujinimu ar kibernetinio saugumo užtikrinimu, siekiant mažinti galimas kilti organizacijos tinklų ir informacinių sistemų kibernetinio saugumo rizikas.

3. Tvarkoje vartojamos sąvokos:

3.1. **„Būtina žinoti“** – minimalus informacijos kiekis, kurį būtina žinoti prekėms pateikti, darbui atlikti ar paslaugai suteikti;

3.2. **Kibernetinio saugumo vadovas** – KT pirmininko paskirtas asmuo atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

3.3. **Privalomas paslaugų teikimo lygis** (angl. *Service Level Agreement*) (toliau – SLA) – sutartinis susitarimas tarp trečiosios šalies ir KT, kuriame nustatomi konkretūs paslaugų teikimo kokybės, prieinamumo, reagavimo į incidentus, problemų sprendimo ir kiti su paslaugų teikimu susiję rodikliai;

3.4. **Sutartis** – tarp KT ir trečiosios šalies pasirašyta tinklų ir informacinių sistemų valdymo ir (ar) kibernetinio saugumo užtikrinimo paslaugų ir (ar) produktų pirkimo sutartis;

3.5. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupę arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

3.6. **Trečioji šalis** – tai išorinė organizacija, asmuo ar subjektas, kuris teikia KT TIS ir kibernetinio saugumo valdymo paslaugas, produktus ar vykdo veiklą, susijusią su organizacijos tinklais, informacinėmis sistemomis ar duomenimis pagal sudarytą sutartį.

4. Kitos šioje Tvarkoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

II SKYRIUS

TREČIŲJŲ ŠALIŲ ATITIKTIES VALDYMAS

5. Kibernetinio saugumo reikalavimai nustatomi vadovaujantis šia Tvarka ir aktualiais teisės aktais, reglamentuojančiais kibernetinį saugumą:

5.1. Kibernetinio saugumo įstatymu;

5.2. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas Nr. 818);

5.3. Kitais teisės aktais, reglamentuojančiais kibernetinį saugumą ar visuotinai pripažintais gerosios praktikos standartais.

6. Trečioji šalis privalo atitikti šioje Tvarkoje ir kituose aktuose nustatytus reikalavimus, kurie perkeltami į sutartis ir viešojo pirkimo dokumentus.

III SKYRIUS

KOKYBĖS REIKALAVIMAI TREČIŲJŲ ŠALIŲ TEIKIAMOMS PASLAUGOMS IR (AR) PRODUKTAMS

7. KT valstybės pareigūnai, valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartį (toliau kartu – darbuotojai), atsakingi už trečiųjų šalių paslaugų ir (ar) produktų įsigijimo inicijavimą, rengdami technines specifikacijas, užduoties aprašymus ar kitus dokumentus, turi nustatyti detalius įsigyjamų TIS valdymo ir (ar) kibernetinio saugumo užtikrinimo paslaugų ir (ar) produktų reikalavimus, kokybės vertinimo kriterijus bei SLA, tačiau neapsiribojant reagavimo į problemas ir problemų sprendimo laikais.

8. Su trečiosiomis šalimis sudarant TIS valdymo ir (ar) kibernetinio saugumo užtikrinimo paslaugų ir (ar) produktų sutartis, į jas turi būti perkelti visi įsigyjamų paslaugų ir (ar) produktų kokybės vertinimo kriterijai ir SLA, o organizacijos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, šioje Tvarkoje numatyta tvarka turi užtikrinti įsigyjamų paslaugų ir (ar) produktų kokybės vertinimo atitiktį kriterijams ir SLA stebėjimą bei fiksavimą.

9. Trečiosios šalies fizinė apsauga užtikrinama vadovaujantis fizinės apsaugos reikalavimais pagal Kibernetinio saugumo reikalavimų aprašą, patvirtintą Nutarimu Nr. 818 (toliau – Kibernetinio saugumo reikalavimo aprašas). Privaloma užtikrinti ne žemesnį fizinės apsaugos lygį nei nurodyta Fizinės apsaugos tvarkoje.

10. Trečioji šalis įsipareigoja saugoti organizacijos konfidencialią informaciją pasirašydama konfidencialumo ir duomenų neatskleidimo įsipareigojimus.

11. Kibernetinio saugumo vadovas priklausomai nuo įsigyjamos paslaugos ir (ar) produktų turi teisę įsitikinti trečiosios šalies darbuotojų kvalifikacija prašydamas pateikti atitinkamus kvalifikaciją patvirtinančius įrodymus leidžiančius dirbti su TIS.

12. Trečioji šalis, ne rečiau kaip kartą per metus, privalo organizuoti darbuotojų kibernetinio saugumo mokymus.

13. KT turi nustatyti trečiajai šaliai keliamus kvalifikacijos ir pajėgumų reikalavimus, įskaitant, tačiau neapsiribojant personalui reikalingais įgūdžiais, mokymais, sertifikatais, kvalifikacija, bei prašyti pateikti jų atitiktį pagrindžiančius dokumentus, pvz., įmonės sertifikatus, ekspertų gyvenimo aprašymus ir sertifikatus ir pan.). Šie reikalavimai turi būti aiškiai apibrėžti techninėje specifikacijoje, reikalavimų sąvade ar kituose pirkimo dokumentuose.

14. KT turi užtikrinti, kad prieš paslaugų ir (ar) produktų įsigijimą trečiajai šaliai būtų aiškiai apibrėžti taikytini kibernetinio saugumo reikalavimai:

- 14.1. Sutartyje turi būti nustatytos sąlygos, kad trečioji šalis:
 - 14.1.1. bendradarbiaus su organizacijos atsakingais asmenimis;
 - 14.1.2. teiks informaciją ir įrodymus apie reikalavimų įgyvendinimą;
 - 14.1.3. kartą per metus atliks TIS veiklos tęstinumo valdymo plano išbandymą;
 - 14.1.4. kartą per metus atliks atitikties vertinimą teisės aktams, reglamentuojantiems kibernetinio saugumo valdymą;
 - 14.1.5. kartą per 6 mėnesius atliks TIS spragų testavimą;
 - 14.1.6. leis atlikti patikrinimus ar vertinimus, jei tai būtina.
- 14.2. trečiosios šalies prieiga prie TIS suteikiama tik sutartyje nurodytai paslaugai įgyvendinti, tiksliai apibrėžtam laikotarpiui.
- 14.3. trečiosios šalies galimi, pagrįsti nukrypimai nuo reikalavimų turi būti aiškiai įvardinti ir dokumentuoti.
- 14.4. trečioji šalis užtikrins:
 - 14.4.1. žurnalinių įrašų rinkimą, saugojimą ir prieinamumą;
 - 14.4.2. prieigos valdymo kontrolę ar audito vykdymo galimybes;
 - 14.4.3. įsipareigojimus dėl programinės įrangos atnaujinimų vykdymo.
15. Trečioji šalis turi iš anksto pranešti apie bet kokią esminį paslaugų teikimo pakeitimą, įskaitant TIS pakeitimus (pvz., perkėlimas, techninės ar programinės įrangos pakeitimas ir perkonfigūravimas), kurie turi įtakos paslaugų teikimo sutarčiai, informacijos apdorojimui arba saugojimui naujoje geografinėje ar teisinėje jurisdikcijoje, sprendimui naudotis naujų subrangovų paslaugomis (įskaitant esamų subrangovų keitimą).

IV SKYRIUS

TREČIŲJŲ ŠALIŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO RIZIKOS VALDYMAS

16. Trečioji šalis, vadovaujantis Kibernetinio saugumo reikalavimo aprašo reikalavimais ne rečiau kaip kartą per metus arba įvykus esminiams organizaciniais ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliame kibernetiniame incidentui, nustatomam pagal Kibernetinių incidentų valdymo planą, turi atlikti TIS kibernetinio saugumo rizikos vertinimą.
17. KT prašymu trečioji šalis turi neatlygintinai sudaryti sąlygas kibernetinio saugumo vadovui ar saugos įgaliotiniui atlikti TIS kibernetinio saugumo rizikos vertinimą ar kitus kibernetinio saugumo patikrinimo veiksmus potencialių pažeidžiamumų nustatymui.
18. Trečioji šalis neatlygintinai turi pateikti duomenis, kurie reikalingi įsitikinti, jog trečioji šalis atitinka ir laikosi sutartyje, kibernetinį saugumą ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose ir visuotinai pripažintuose gerosios praktikos standartuose nustatytų reikalavimų.

V SKYRIUS

PRIEIGŲ VALDYMAS

19. Trečiųjų šalių prieigos yra valdomos vadovaujantis Prieigų valdymo tvarka, papildomai įgyvendinant šioje Tvarkoje toliau numatytus reikalavimus.
20. Trečioji šalis gali gauti prieigas prie TIS tik pasirašę sutartį ir konfidencialumo, duomenų neatskleidimo įsipareigojimus su organizacija, įskaitant abiejų šalių atsakomybes dėl

organizacijos informacijos saugumo reikalavimų įgyvendinimo užtikrinimo bei baudų už įsipareigojimų nevykdymą.

21. Prieigos suteikimo faktas turi būti aprašytas sutartyje nurodant kaip identifikuojami asmenys, kurie turės prieigą, prieigos naudotojų teisės, suteikiamos prieigos laikotarpis ir prieigos aktyvumo periodas (pvz., darbo valandas).

22. Suteikus trečiajai šaliai galimybę dirbti kompiuterinėje darbo vietoje priklausančioje trečiajai šaliai, bei suteikiant nuotolinę prieigą prie TIS, privaloma:

22.1. kompiuterinę darbo vietą sukonfigūruoti taip, jog prisijungti prie TIS būtų galima tik naudojant VPN (angl. *Virtual Private Network*) arba alternatyvią, didesnę ar tą patį saugumą užtikrinančią technologiją;

22.2. įsitikinti, kad TIS iš kurios jungiamasi per nuotolį yra saugi;

22.3. užtikrinti nuolatinę prieigos teisių kontrolę;

22.4. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę arba rinkti ir ne trumpiau kaip 90 dienų saugoti žurnalinius įrašus apie atliktus veiksmus, užtikrinant jų vientisumą, konfidencialumą ir prieinamumą pagal pareikalavimą;

22.5. užtikrinti organizacijos viešai neskelbtinos informacijos apsaugą organizacinėmis ir techninėmis priemonėmis;

22.6. užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas ir sutaptų su iš anksto tarpusavyje suderintais keliamais tikslais;

22.7. užtikrinti, kad prisijungimas per nuotolinį ryšį ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „būtina žinoti“ bei turėtų sutartą galiojimo terminą, kuris būtų nurodytas sutartyje;

22.8. kiekvienam vartotojui turi būti sukurtas individualus prisijungimo identifikatorius;

22.9. prisijungdama nuotoline prieiga prie TIS trečioji šalis privalo patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksmų tapatumo nustatymo priemonės, angl. *Multi-factor authentication*);

22.10. prisijungimo slaptažodis trečiajai šaliai privalo būti perduotas atskirai nuo naudotojo prisijungimo identifikatoriaus, naudojant saugius ryšio kanalus.

23. Bet kokia nuotolinė prieiga neatitinkanti šiame skyriuje aprašytų reikalavimų prie TIS yra draudžiama.

24. Pasibaigus sutarties terminui ar pilnai suteikus paslaugas prieš sutarties pasibaigimo terminą, trečiųjų šalių prieigos prie TIS turi būti nedelsiant sustabdytos ir (ar) panaikintos.

VI SKYRIUS

SUTARČIŲ SUDARYMO REIKALAVIMAI

25. Organizacijos darbuotojai, įgyvendindami organizacijos sutarčių sudarymo ir trečiųjų šalių valdymo procesus, privalo užtikrinti, kad perkant TIS ar kibernetinio saugumo valdymo paslaugas ir (ar) produktus būtų derinamos sutarties sąlygos su organizacijos kibernetinio saugumo vadovu ar saugos įgaliotiniu, siekiant įtraukti kibernetinio saugumo reikalavimus.

26. Organizacijos sutartyse su trečiosiomis šalimis (tiekėjais, įskaitant subtiekejus), kiek tai susiję su teikiamomis paslaugomis ir (ar) produktais, turi numatyti:

26.1. trečiosios šalies atitiktį Kibernetinio saugumo reikalavimų aprašo reikalavimams;

26.2. trečiosios šalies personalui reikalingus įgūdžius, mokymus, sertifikatus, kvalifikaciją;

26.3. trečiosios šalies pareigą ne rečiau kaip kartą per metus arba įvykus esminiams trečiosios šalies organizaciniais ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliame kibernetiniame incidentui atlikti TIS kibernetinio saugumo rizikos vertinimą (toliau – Rizikos vertinimas), parengti ir organizacijos atsakingiems darbuotojams pateikti rizikos vertinimo ataskaitą ir rizikų valdymo planą;

26.4. trečiosios šalies pareigą pranešti organizacijai apie visus didelius ir kitus incidentus, susijusius su organizacijos TIS, kai tik trečioji šalis sužino apie incidentą, ir neatlygintinai pateikti organizacijai kibernetinio incidento tyrimo ataskaitą pagal Kibernetinių incidentų valdymo tvarką;

26.5. teisę organizacijai arba jo įgaliotiems paslaugų teikėjams atlikti trečiosios šalies Kibernetinio saugumo reikalavimų aprašo auditą (įskaitant neplaninį) ir trečiosios šalies pareigą neatlygintinai sudaryti sąlygas tokiam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliame incidentui;

26.6. trečiosios šalies pareigą užtikrinti spragų, keliančių riziką TIS, valdymą;

26.7. trečiosios šalies konfidencialumo ir duomenų neatskleidimo įsipareigojimus pagal Turto valdymo tvarką;

26.8. trečiajai šaliai taikomą SLA;

26.9. apibrėžti trečiosios šalies prieigos (loginės ir fizinės) prie TIS lygius ir sąlygas pagal šios Tvarkos V skyrių;

26.10. numatyti reikalavimus, keliamus trečiosios šalies patalpoms, įrangai, TIS priežiūrai, informacijos perdavimui tinklais;

26.11. numatyti trečiosios šalies ir organizacijos teises ir pareigas.

27. Organizacijos su interneto paslaugos, jei duomenų perdavimo paslauga yra esminė paslaugai teikti, teikėju turi būti sudaręs sutartį (-is), kurioje (-iose) būtų numatyta:

27.1. reagavimas į kibernetinius incidentus įprastomis darbo valandomis;

27.2. reagavimas į kibernetinius incidentus po darbo valandų;

27.3. nepertraukiamas interneto paslaugos teikimas: 24 valandas per parą, 7 dienas per savaitę;

27.4. paslaugos sutrikimų registravimas: 24 valandas per parą, 7 dienas per savaitę;

27.5. apsaugos nuo TIS trikdymo taikymas (angl. *Denial of Service, DoS*).

VII SKYRIUS

TREČIŲJŲ ŠALIŲ SĄRAŠO VALDYMAS, TEIKIAMŲ PASLAUGŲ IR (AR) PRODUKTŲ KOKYBĖS VALDYMAS

28. Organizacijos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą pagal Trečiųjų šalių sąrašo formą (1 priedas) rengia ir nuolat atnauja Trečiųjų šalių sąrašą, kuriame pateikia informaciją apie trečiąją šalį, jos teikiamas paslaugas ir (ar) produktus, atsakingus asmenis, apie sutartį ir joje numatytus pagrindinius SLA bei įvykusius incidentus. Sąrašas gali būti rengiamas bei saugomas skaitmeninėje darbo aplinkoje (pvz., SharePoint Lists ar Excel) arba užpildant popierinę formą, užtikrinant jame pateikiamos informacijos prieinamumą ir saugumą.

29. Organizacijos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, turi vertinti užfiksuotus trečiųjų šalių SLA neatitikimus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais bei nutarti, ar šie neatitikimai organizacijai yra priimtini. Nustačius, kad trečiųjų šalių neatitikimai organizacijai yra nepriimtini, organizacijos darbuotojai, atsakingi už

sutarties su trečiosiomis šalimis įgyvendinimą, turi inicijuoti sutartyje numatytų sankcijų taikymą ir (ar) sutarties su trečiąja šalimi nutraukimą.

30. Trečiųjų šalių sąrašas turi būti peržiūrimas ir atnaujinamas inicijuojant numatytus IT ir kibernetinio saugumo reikalavimų pakeitimus naujoms sutartims ir pasikeitus sutartims arba kai įvyksta reikšmingi pokyčiai ar reikšmingi incidentai, susiję su trečiosiomis šalimis.

VIII SKYRIUS

BAIGIAMOSIOS NUOSTATOS

31. Sutartyse dėl paslaugų ir (ar) produktų pirkimo privaloma numatyti, kad šios Tvarkos reikalavimai yra neatsiejama sutarties dalis. Taip pat organizacija ir trečioji šalis gali susitarti dėl šios Tvarkos reikalavimų taikymo papildomais susitarimais.

32. Tvarkos reikalavimai trečiajai šaliai galioja tol, kol galioja sutartis.

33. Jei kuri nors šios Tvarkos nuostata pripažįstama negaliojančia dėl prieštaravimo imperatyvioms teisės aktų nuostatoms, ji keičiama vadovaujantis sutartyje nustatyta tvarka.

34. Ši Tvarka turi būti peržiūrima ir atnaujinama bent kartą per metus arba kai atsiranda esminiai pokyčiai KT, kurie turi įtakos šiai Tvarkai. Už šios Tvarkos peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas.

TREČIŲJŲ ŠALIŲ SĄRAŠAS
(Trečiųjų šalių sąrašo forma)

Eil. Nr.	Trečiosios šalies pavadinimas	Teikiamos paslaugos ir (ar) produkto pobūdis	Trečiosios šalies kontaktinis asmuo	Už sutarties vykdymą atsakingas KT darbuotojas	Sutarties numeris	Sutarties terminas	Sutarties kokybės reikalavimai	Suteiktos prieigos prie tinklų ir informacinių sistemų	Ar įvyko incidentas (Taip/ Ne)	Incidentų skaičius	Paslaugų prieinamumas proc. (SLA sutartyje)	Paslaugų prieinamumas proc. (SLA pagal faktą)
1.	[Nurodykite trečiosios šalies, su kuria sudaryta sutartis pavadinimą]	[Nurodykite trečiosios šalies, pagal sutartį teikiamą paslaugą ir (ar) produktą]	[Nurodykite trečiosios šalies kontaktinį asmenį]	[Už sutarties vykdymą atsakingą darbuotoją]	[Nurodykite sutarties numerį]	[Nurodykite, kad baigtis sutarties galiojimas]	[Nurodykite kokybės reikalavimus, pvz. ISO 27001 sertifikatas]	[Nurodykite pagal sutartį suteiktas prieigos prie tinklų ir informacinių sistemų]	[Nurodykite, ar įvyko incidentas (-ai) - Taip arba Ne]	[Nurodykite įvykusių incidentų skaičių]	[Nurodykite paslaugų prieinamumą, pvz., 99% per mėnesį ar metus]	[Nurodykite koks buvo paslaugų prieinamumas pagal faktą po incidentų]
