Tiekėjo saugumo direktyva

Versija 8.1_LT

TURINYS

TURINYS 1
1 Aprašymas 1
2 Sąvokos 2
3 Saugumo kontaktinė informacija 4
4 Saugumo reikalavimai – organizacinės kontrolės 4
4.1 Bendrosios nuostatos 4
4.2 Saugumo valdymas 4
4.3 Saugumo rizikų nustatymas 5
4.4 Duomenų klasifikavimas ir tvarkymas 6
4.5 Prieigos valdymas 7
4.6 Dirbtinis intelektas (DI) arba autonominės technologijos (ATT) 8
4.7 Tiekėjo santykiai su Tiekėjo subrangovais 9
4.8 Debesijos saugumas 9
4.9 Reagavimas į saugumo incidentus 10
4.10 Atkūrimas po saugumo incidentų 10
5 Saugumo reikalavimai – žmogiškieji aspektai 11
5.1 Personalo saugumas 11
6 Saugumo reikalavimai – fizinės kontrolės 11
6.1 Fizinis ir aplinkos saugumas 11
7 Saugumo reikalavimai – technologinės kontrolės 12
7.1 Galinių įrenginių ir mobiliųjų įrenginių valdymas 12
7.2 Pajėgumų ir našumo planavimas 12
7.3 Pažeidžiamumų ir pataisų (*angl. patch*) valdymas 12
7.4 Konfigūracijų ir saugumo žurnalų valdymas 13
7.5 Saugumo grėsmių aptikimas 13
7.6 Tinklo saugumas 14
7.7 Interneto (*angl. Web*) saugumo rizikų valdymas 14
7.8 Kriptografinė apsauga 14
7.9 Saugi inžinerija ir architektūra 14
7.10 Technologijų kūrimas ir įsigijimas 15
7.11 Techninė priežiūra 15
7.12 Pakeitimų valdymas 15
8 Priedai 15

1 Aprašymas

„Tiekėjo saugumo direktyva“ (toliau - TSD) apibrėžia saugumo reikalavimus tiekėjams ir pagrindiniams verslo partneriams, teikiantiems perduodamus rezultatus / darbus (*angl. deliverables*) (toliau - Rezultatai) bendrovei „Telia Lietuva“ AB (toliau – Telia). TSD nustato minimalius techninius ir organizacinius saugumo reikalavimus , kurių tiekėjai privalo laikytis pagal Sutartį. Pasirašydamas TSD, Tiekėjas patvirtina, kad laikosi Lietuvos Respublikos kibernetinio saugumo įstatymo tiek, kiek šio įstatymo reikalavimai yra įtvirtinti šiame dokumente abipusiu Šalių susitarimu.

TSD taikoma visais atvejais,, kai Sutartyje dėl Rezultatų aiškiai nurodyta, kad šis Priedas yra neatsiejama jos dalis. Šalių susitarimu papildomi saugumo reikalavimai gali būti nustatyti, pakeisti arba tam tikrais atvejais netaikomi. Jei kuri nors TSD nuostata reikalauja aiškinimo, ji turi būti aiškinama vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymo tikslais ir principais bei jį įgyvendinančiais teisės aktais, kuriais Lietuvoje įgyvendinama ES NIS2 direktyva, arba ISO/IEC 27001:2022 standarto terminologija.

Toliau pateikiamos nuorodos į ISO/IEC 27001:2022 standartą yra informacinio pobūdžio gairės,skirtos tiekėjams geriau suprasti TSD reikalavimus ir užtikrinti veiksmingą jų įgyvendinimą. Šios nuorodos nenustato jokių papildomų įpareigojimų, viršijančių TSD nustatytus reikalavimus.

2 Sąvokos

1. „**Susijusi įmonė**“ (*angl. Affiliate*) – juridinis asmuo, kuris tiesiogiai ar netiesiogiai kontroliuoja Šalį, yra kontroliuojamas Šalies arba yra kontroliuojamas to paties asmens, kaip ir Šalis, kol tokia kontrolė egzistuoja. Kontrolė laikoma egzistuojančia, kai tiesiogiai ar netiesiogiai nuosavybės teise valdoma daugiau kaip 50 (penkiasdešimt)) procentų juridinio asmens įstatinio kapitalo arba akcijų, suteikiančių daugiau kaip 50 (penkiasdešimt) procentų balsų, renkant valdymo organus ar juos atitinkančius asmenis.

2. „**Sutartis**“ (*angl. Agreement*) – Pirkėjo ir Tiekėjo sudaryta sutartis, kurios neatsiejama dalis yra ši Tiekėjų saugumo direktyva.

3. „**Taikomi duomenų apsaugos teisės aktai**“ (*angl. Applicable Data Protection Laws*) – visi taikytini teisės aktai, reglamentuojantys duomenų apsaugą, įskaitant, bet neapsiribojant, Direktyva 2002/58/EB dėl privatumo ir elektroninių ryšių bei Reglamentą (ES) 2016/679 (BDAR/GDPR), taip pat visus jų pakeitimus, papildymus ar pakeičiančius teisės aktus (toliau kartu – **ES teisės aktai**), nacionalinius teisės aktus, įgyvendinančius ES teisės aktus, bei kitus galiojančius privalomus duomenų apsaugos reikalavimus.

4. „**Dirbtinis intelektas (DI) arba autonominė technologija (ATT)**“ (*angl. Artificial Intelligence (AI) or Autonomous Technology (ATT)*) – automatizuota sistema, veikianti įvairiais autonomiškumo lygiais, kuri gali būti adaptyvi ir, siekdama apibrėžtų ar numanomų tikslų, iš įvesties duomenų generuoja išvestis (pvz., prognozes, turinį, rekomendacijas ar sprendimus), galinčias daryti poveikį fizinei ar virtualiai aplinkai. Ši sąvoka taip pat apima bendrosios paskirties DI modelius (*pvz.,* didžiuosius kalbų modelius (*angl. Large Language Models*)), išskyrus modelius, naudojamus tik mokslinių tyrimų, eksperimentinės plėtros ar prototipavimo tikslais iki jų pateikimo rinkai.

5. „**Veiklos tęstinumo planai (BCP) ir atkūrimo po nelaimės planai (DR)**“ (*angl. Business Continuity Plans (BCP), Disaster Recovery Plans (DRP)*) – dokumentai, kuriuose aprašytos procedūros ir veiksmai, skirti užtikrinti organizacijos veiklos tęstinumą ir veiklos atstatymą įvykus reikšmingiems veiklos sutrikimams .

6. „**Pirkėjas**“ (*angl. Buyer*) – Telia Lietuva AB.

7. „**Pirkėjo duomenys**“ (*angl. Buyer's Data*) – visi duomenys, įskaitant asmens duomenis, kuriuos Pirkėjas, jo klientai ar kiti jo vardu veikiantys asmenys, perduoda Tiekėjui, taip pat duomenys, sukurti ar sugeneruoti naudojantis Rezultatais, įskaitant Tiekėjo atliekamo tokių duomenų tvarkymo rezultatus.

8. „**Konfidenciali informacija**“ (*angl. Confidential information*) – bet kokia nevieša informacija, duomenys ar dokumentai, perduodami kitai Šaliai bet kokia kita forma, vykdant Sutartį ar bendradarbiaujant, nepriklausomai nuo to, ar tokia informacija yra pažymėta kaip konfidenciali. Konfidenciali informacija apima bet kokią komercinę, finansinę, techninę, organizacinę ar kitą su verslu susijusią informaciją, kurios atskleidimas tretiesiems asmenims be teisėto pagrindo ar išankstinio rašytinio sutikimo yra draudžiamas.

9. „**Klientas**“ (*angl. Customer*) – Pirkėjo klientas.

10. „**CSP***“ (liet. DPT*) – debesijos paslaugų teikėjas (*angl. cloud service provider*).

11. „**Rezultatas/atliktas darbas**“ (*angl. Deliverable*) – Sutartyje apibrėžti darbai, produktai ar paslaugos.

12. „**Tiekėjo talpinamas Rezultatas**“ (*angl. Supplier-hosted Deliverable*) – Rezultatas, kuris yra valdomas ir teikiamas Tiekėjo infrastruktūroje (pvz., SaaS), , o Pirkėjas juo naudojasi nuotoliniu būdu.

13. „**Rezultatas, susijęs su Pirkėjo duomenų tvarkymu**“ (*angl. Deliverable processing Buyer's Data*) – bet koks Rezultatas, kuriuo tvarkomi Pirkėjo duomenys, įskaitant jų rinkimą, saugojimą, naudojimą, perdavimą ar kitokį apdorojimą Tai taip pat apima atvejus, kai Tiekėjas kuria, palaiko, teikia ar valdo technologiją, taikomąsias programas (-ą), paslaugas (-ą) ar sprendimus (-ą), naudojamus Pirkėjo verslo tikslais ir esančius Tiekėjo aplinkoje arba talpinamus išorėje.

14. „**Atkūrimo po nelaimės planai (DRP)**“ (*angl. Disaster Recovery Plans*) – dokumentuotos politikos ir procedūros, reglamentuojančios reagavimą į reikšmingus įmonės veiklos sutrikimus ar infrastruktūros praradimą.

15. **„Didelės rizikos šalys“** – Rusijos Federacija, Baltarusija, Kinija, Krymas (aneksuota dalis), Padniestrės (Transdniestrijos) teritorija, nekontroliuojama Moldovos Vyriausybės, Abchazijos ir Pietų Osetijos teritorijos, nekontroliuojamos Gruzijos Vyriausybės, Iranas, Šiaurės Korėja.

16. „**Registruoti**“ (*angl. Log*) – sistemingai fiksuoti informaciją ar įvykius jų įvykimo seka.

17. „**Asmens duomenys**“ (*angl. Personal Data*) – bet kokia informacija, susijusi su identifikuotu arba identifikuojamu fiziniu asmeniu (duomenų subjektu). Identifikuojamu laikomas fizinis asmuo, kurį galima tiesiogiai ar netiesiogiai identifikuoti pagal identifikatorių, pvz., vardą, pavardę, adresą, asmens socialinio draudimo numerį, buvimo vietos duomenis, internetinį identifikatorių, IP adresą arba abonento numerį, arba pagal vieną ar kelis to fizinio asmens fizinei, fiziologinei, genetinei, psichinei, ekonominei, kultūrinei ar socialinei tapatybei būdingus veiksnius, įskaitant srauto duomenis ir pranešimų turinį.

18. „**Asmens duomenų saugumo pažeidimas**“ (*angl. Personal Data Breach*) –saugumo pažeidimas, dėl kurio atsitiktinai arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami Asmens duomenys arba suteikiama prie jų neteisėta prieiga, kai tokie Asmens duomenys yra perduodami, saugomi ar kitaip tvarkomi Tiekėjo pagal Sutartį, ir kuris kartu apima Tiekėjo įsipareigojimų dėl konfidencialumo, saugumo ir (ar) Asmens duomenų apsaugos pažeidimą, susijusį su pagal Sutartį tvarkomais Pirkėjo ar Kliento Asmens duomenimis.

19. „**Duomenų tvarkytojas**“ (*angl. Processor*) ir **„duomenų tvarkymas**“ (*angl. processing*) – sąvokos, vartojamos reikšmėmis, kurios joms suteiktos BDAR ir taikytinuose duomenų apsaugos teisės aktuose.

20. „**Reguliaciniai reikalavimai**“ (*angl. Regulatory Requirements*) – visi taikytini įstatymai, įskaitant įstatymus, poįstatyminius teisės aktus ir reglamentus, taip pat tarptautinių politinių ir ekonominių organizacijų (pvz., Europos Sąjungos) privalomi teisės aktai, r ypač Lietuvos Respublikos kibernetinio saugumo įstatymas ir jį įgyvendinantys teisės aktai; kompetentingų priežiūros institucijų – finansinių paslaugų priežiūros, duomenų apsaugos, vartotojų teisių apsaugos ir kitų atitinkamų valdžios institucijų – priimti įsakymai, sprendimai ir licencijos; taip pat rekomendacijos, politikos dokumentai, standartai ir gairės, kuriuos skelbia minėtos institucijos, teismai, savireguliacinės ar patariamosios organizacijos bei pramonės sektoriaus asociacijos, – tiek, kiek jie yra privalomi arba taikytini Šalių veiklai pagal Sutartį.

21. „**Saugumo kontrolė**“ (*angl. Security Control*) – bet kuri techninė apsaugos priemonė, organizacinė struktūra ar procesas,skirtas užtikrinti IT (informacinių technologijų) sistemų konfidencialumą, vientisumą ir prieinamumą.

22. „**Saugumo įvykių žurnalas**“ (*angl. Security Event Log*) – sistema, registruojanti informacinių sistemų veiklos įvykius, pvz. prieigą prie sistemų, išteklių ir duomenų (įskaitant asmens duomenis) arba bandymus tokią prieigą gauti; sistemos konfigūracijos ir politikų pakeitimus; privilegijų ar paslauginių programų bei taikomųjų programų naudojimą; prieigą prie failų ar jų ištrynimą; prieigos kontrolės sistemos sukeltus pavojaus signalus; saugos sistemų įjungimą ir išjungimą; paskyrų valdymo įvykius; sistemos klaidas ir įspėjimus; programos ar pačios sistemos paleidimą iš naujo arba išjungimą; ar bet kokius kitus reikšmingus veiksmus, galinčius turėti įtakos sistemos saugumui.

23. „**Saugumo incidentas**“ (*angl. Security Incident*) – vienas ar keli nepageidaujami ar netikėti saugumo įvykiai, kurie kelia didelę tikimybę sutrikdyti verslo veiklos tęstinumą arba kelia grėsmę informacinių sistemų ar duomenų saugumui.

24. „**Saugumo rizika**“ (*angl. Security Risk*) –neapibrėžtumas, galintis daryti neigiamą poveikį Pirkėjo tikslų įgyvendinimui ar numatytų rezultatų pasiekimui;. paprastai išreiškiamas kaip tikimybinio pobūdžio nepageidaujamas ateities įvykis arba jo pasekmės.

25. „**Saugumo grėsmės**“ (*angl. Security Threats*) – bet kokia aplinkybė ar įvykis, galintys neigiamai paveikti organizacijos veiklą (įskaitant misiją, funkcijas, įvaizdį ar reputaciją), organizacijos turtą, asmenis, trečiąsias šalis ar nacionalinį saugumą, neteisėtai gaunant prieigą prie informacinės sistemos, naikinant, atskleidžiant ar modifikuojant informaciją ir (arba) sutrikdant paslaugų teikimą.

26. „**Tiekėjas**“ (*angl. Supplier*) – kita Sutarties šalis, tiekianti bet kokius Rezultatus Pirkėjui, Sutartyje apibrėžta ar įvardyta kaip „Tiekėjas“, „Pardavėjas“ (*angl. Vendor*), „Partneris“ ar kitu analogišku pavadinimu, taip pat bet kuris kitas Pirkėjo identifikuotas verslo partneris.

27. „**Tiekėjo personalas**“ (*angl. Supplier Personnel*) – bet kuris asmuo, dirbantis Tiekėjo vardu ar jo naudai, įskaitant darbuotojus, konsultantus, rangovus ir subtiekėjus.

28. „**Telia**“ arba „**Telia Grupė**“ – patronuojanti bendrovė *Telia Company AB* ir visi juridiniai asmenys, kuriuos *Telia Company AB* tiesiogiai ar netiesiogiai kontroliuoja turėdama kontrolinį akcijų paketą arba kitu būdu užtikrindama kontrolę.

3 Saugumo kontaktinė informacija

1. Tiekėjas privalo informuoti Pirkėją el. pašto adresais saugos_komanda@telia.lt ir cert@teliacompany.com apie bet kurį Saugumo incidentą, galintį turėti reikšmingą poveikį Rezultatui, nepagrįstai nedelsiant, bet ne vėliau kaip per 24 (dvidešimt keturias) valandas nuo tokio incidento nustatymo momento.
2. Tiekėjas privalo informuoti Pirkėją el. pašto adresais saugos_komanda@telia.lt ir cert@teliacompany.com apie bet kokius „nulinės dienos“ (*angl. „zero-day“)* pažeidžiamumus ir kitus pažeidžiamumus, galinčius turėti reikšmingą poveikį Rezultatui, nepagrįstai nedelsiant, bet ne vėliau kaip per 24 (dvidešimt keturias) valandas nuo atitinkamo pažeidžiamumo nustatymo momento.
3. Tiekėjas informuoja Pirkėją el. pašto adresais privatumas@telia.lt ir controlcenterem-security@teliacompany.com nepagrįstai nedelsiant apie bet kokį faktinį ar pagrįstai įtariamą Asmens duomenų saugumo pažeidimą, darantį poveikį Pirkėjui ar Klientui, bet ne vėliau kaip per 24 (dvidešimt keturias) valandas nuo tokio pažeidimo nustatymo momento.

4 Saugumo reikalavimai – organizacinės kontrolės

4.1 Bendrosios nuostatos

[ISO/IEC 27001:2022 A.5.1–A.5.2]

1. Tiekėjas Pirkėjo prašymu arba, kai tai pagrįstai reikalinga, pateikia Pirkėjui dokumentus ar sertifikatus, ar kitus įrodymus patvirtinančius jo atitiktį taikomiems informacijos saugumo standartams, pvz., ISO/IEC 27001, PCI DSS, SOC2, taip pat kibernetinio saugumo auditų ar, savivertinimo ataskaitas ar kitus įrodymus, patvirtinančius, kad Tiekėjo organizacijoje yra įdiegtos ir taikomos tinkamos informacijos saugumo valdymo praktikos.
2. Jei Tiekėjas pagal Lietuvos Respublikos kibernetinio saugumo įstatymą laikomas kibernetinio saugumo subjektu, jis privalo pateikti Pirkėjui išorinio audito atitikties ataskaitą arba savivertinimo ataskaitą dėl atitikties Kibernetinio saugumo reikalavimų sąrašui, kaip nustatyta taikytinuose teisės aktuose.

4.2 Saugumo valdymas

[ISO/IEC 27001:2022 A.5.1–A.5.4, A.5.29, A.5.30]

1. Tiekėjas privalo turėti patvirtintą informacijos saugumo politiką ir įdiegtus atitinkamus saugumo procesus.
2. Tiekėjas periodiškai testuoja kibernetinio saugumo ir asmens duomenų apsaugos kontrolės priemones visose su Rezultatu susijusiose aplinkose - vystymo, testavimo ir gamybinėje (produkcinėje) aplinkose.
3. Tiekėjas privalo turėti apibrėžtas ir dokumentuotas roles bei atsakomybes, užtikrinančias nuoseklų Tiekėjo požiūrį į saugumą ir privatumą bei jų nuolatinį tobulinimą.
4. Tiekėjas paskiria vieną kontaktinį asmenį, atsakingą už Pirkėjo saugumo reikalavimų įgyvendinimą, įskaitant, bet neapsiribojant saugumo konfigūracijos rekomendacijomis, planuojamais paslaugų sustabdymais, incidentų valdymu, bendrų saugumo atnaujinimų komunikavimu.
5. Tiekėjas taiko rizika grindžiamą požiūrį, leidžiantį identifikuoti, vertinti ir valdyti saugumo bei su asmens duomenimis susijusias rizikas..
6. Tiekėjas privalo turėti veiklos tęstinumo planus (BCP) ir atkūrimo po sutrikimų planus (DR), susijusius su Rezultato teikimu. Planai turi būti atnaujinami ir testuojami bent kartą per metus.

7. Tiekėjas periodiškai nustato, analizuoja ir vertina veiklos tęstinumo rizikas ir imasi būtinų priemonių šioms rizikoms valdyti bei mažinti.
8. Tiekėjas, Pirkėjui pareikalavus, pateikia informaciją ir suteikia pagrįstą pagalbą, reikalingą Pirkėjo veiklos tęstinumo (BCP/DR) veikloms, susijusioms su Rezultatu.
9. Tiekėjas užtikrina procesų, reikalingų Tiekėjo veiklos ir gamybinio (produkcinio) tęstinumo palaikymui, nustatymą ir taikymą, įskaitant priklausomybių, susijusių su Rezultato teikimu, valdymą, siekiant užtikrinti operatyvų atsistatymą po sutrikimų ir minimalų poveikį veiklai.
10. Tiekėjas privalo turėti procesus, skirtus Tiekėjo taikomų saugumo priemonių veiksmingumui vertinti ir užtikrinti.
11. Tiekėjas užtikrina reguliarių darbuotojų saugumo informuotumo mokymų organizavimą.
12. Tiekėjas užtikrina, kad darbuotojai, dalyvaujantys teikiant ir palaikant Rezultatą, būtų išklausę kibernetinio saugumo ir asmens duomenų apsaugos mokymus
13. Pirkėjas turi teisę, apie tai raštu įspėjęs Tiekėją ne vėliau kaip prieš 10 (dešimt) kalendorinių dienų, atlikti Tiekėjo veiklos patikrinimus ar auditus, įskaitant, bet apribojant, , auditus, susijusius su Rezultato teikimu. Tokie patikrinimai ar auditai atliekami ne dažniau kaip vieną kartą per kalendorinius metus, išskyrus atvejus, kai taikytini teisės aktai arba kompetentingos institucijos reikalauja dažnesnių patikrinimų ar auditų. Tokiais atvejais Tiekėjas įsipareigoja visapusiškai bendradarbiauti ir užtikrinti savalaikę prieigą, prie reikalingos informacijos.
14. Tiekėjas įsipareigoja suteikti Pirkėjui ar jo įgaliotiems asmenims prieigą prie atitinkamų verslo ar techninių patalpų (įskaitant biurus ir operacinius centrus), sistemų, tinklų, įrenginių, informacijos ir duomenų, susijusių su Rezultatu, taip pat prie su Rezultatu susijusios informacijos, būtinos patikrinimams ir auditams atlikti, siekiant įvertinti atitiktį taikytiniems teisės aktams ir Sutarties nuostatoms.
15. Pirkėjas turi teisę prašyti Tiekėjo vidaus audito ataskaitų, jei jos yra tiesiogiai susijusios su Sutarties vykdymu ir (ar) Rezultatų teikimu.

Papildomos nuostatos, taikomos tik Tiekėjams, teikiantiems Lietuvos Respublikos nacionaliniam saugumui kritines paslaugas:

16. *Autonomija*. Tiekėjas užtikrina paslaugų tęstinumą pagal Sutartyje sutartus paslaugų lygius, vadovaujantis Pirkėjo Lietuvos Respublikos elektroninių ryšių įstatymo 97 straipsnio, Lietuvos Respublikos karo padėties įstatymo 15 straipsnio bei Mobilizacijos ir priimančiosios šalies paramos įstatymo reikalavimų aiškinimu.
17. *Programinės įrangos suverenitetas*. Pirkėjui pareikalavus, Tiekėjas pateikia informaciją Pirkėjui apie galimybes užtikrinti Rezultato perkeliamumą (*angl. portability*), audituojamumą (*angl. auditability*) ir atsparumą (*angl. resilience*) išoriniams sutrikimams. Pirkėjui pareikalavus, Tiekėjas pateikia informaciją apie galimybes užtikrinti Rezultato perkeliamumą (angl. portability), audituojamumą (angl. auditability) ir atsparumą (angl. resilience) išoriniams sutrikimams.
18. *Duomenų suverenitetas*. Šalys susitaria dėl su Rezultatu susijusių duomenų saugojimo geografinės vietos, taikomų šifravimo standartų ir prieigos valdymo politikų. Bet kokia trečiųjų šalių prieiga prie tokių duomenų leidžiamą tik gavus išankstinį rašytinį Pirkėjo sutikimą.

4.3 Saugumo rizikų nustatymas

[ISO/IEC 27001:2022 A.5.4, A.5.9, A.5.12, A.5.14, A.5.21, A.5.22;]

1. Tiekėjas privalo turėti apibrėžtą ir centralizuotai valdomą turto (*angl. asset*) valdymo sprendimą bei su juo susijusius procesus.
2. Tiekėjas užtikrina, kad Tiekėjo talpinamas Rezultatas, kuriuo tvarkomi Pirkėjo duomenys, būtų tinkamai registruojamas ir valdomas turto inventorizavimo ir konfigūracijų valdymo sistemose per visą jo gyvavimo ciklą – nuo įsigijimo iki utilizavimo. Tiekėjas užtikrina, kad prieiga prie Rezultato būtų suteikiama tik įgaliotiems asmenims, ir kad visi su Rezultatu susiję duomenys, kurie yra saugomi, tvarkomi ar perduodami, būtų tinkamai apsaugoti.

3. Tiekėjas dokumentuoja Tiekėjo talpinamą Rezultatą Tiekėjo turto valdymo (AST) platformoje, pateikdamas aktualią ir naujausią informaciją bei nurodydamas atsakingus asmenis. Rezultatas Tiekėjo yra tvarkomas kaip Konfidenciali informacija.
4. Tiekėjas parengia, palaiko ir pateikia Rezultatą pagrindžiančią dokumentaciją, kurioje aprašomas Rezultatas, jo funkcionalumas bei ryšys su Tiekėju bei Pirkėju. Ši dokumentacija Pirkėjo įgaliotiems darbuotojams pateikiama Pirkėjui pareikalavus.
5. Tiekėjas privalo turėti rizikos valdymo procesus, skirtus saugumo rizikoms nustatyti, analizuoti, vertinti ir valdyti.
6. Tiekėjas privalo turėti rizikos valdymo procesus, skirtus tiekimo grandinės ir trečiųjų šalių saugumo rizikoms nustatyti, analizuoti, vertinti ir valdyti. Pirkėjui pareikalavus Tiekėjas pateikia subrangovų ir kitų trečiųjų šalių, kurias Tiekėjas yra pasitelkęs arba ketina pasitelkti Rezultatų teikimui, sąrašą.
7. Siekdamas nustatyti su saugumu susijusias rizikas, Tiekėjas ne rečiau kaip kartą per metus atlieka su Rezultatu susijusios Tiekėjo veiklos ir gamybinio (produkcinio) tęstinumo rizikos vertinimą
8. Tiekėjas dokumentuoja su Rezultatu susijusias Tiekėjo veiklos ir gamybinio (produkcinio) tęstinumo saugumo rizikas rizikų registre. Rizikų registre identifikuojamos rizikos ir joms yra priskiriami rizikos lygiai.

4.4 Duomenų klasifikavimas ir tvarkymas

[ISO/IEC 27001:2022 A.5.12–A.5.14; NIST CSF 2.0 PR.DS-01–PR.DS-08]

1. Tiekėjas įsipareigoja visą iš Pirkėjo paslaugų teikimo metu gautą informaciją tvarkyti ne žemesniu nei „**Konfidencialu“** (angl. *Confidential)* saugumo lygiu. Tokia informacija gali būti naudojama tik įgaliotiems asmenims, tik teisėtiems verslo tikslams ir tik kontroliuojamoje darbo aplinkoje ar vietoje, kuri yra apsaugota nuo stebėjimo, informacijos perėmimo ar slapto pasiklausymo. Jei informacija yra priskiriama saugumo lygiui **„Slapta“** (*angl. Secret*), ji tvarkoma laikantis papildomų reikalavimų, nustatytų Sutartyje.
2. Tiekėjas tvarko Pirkėjo duomenis tik Sutartyje nustatyta apimtimi ir būdais. Pavyzdžiui, bet koks Pirkėjo duomenų perkėlimas, įskaitant perkėlimą i iš vietinės (*angl. on-premises*) aplinkos į debesijos aplinką, galimas tik gavus išankstinį Pirkėjo patvirtinimą. Visos teisės į Pirkėjo duomenis, įskaitant bet kokias jų versijas, metaduomenis, žurnalus (*angl. logs*), analitinius duomenis, adaptacijas, modifikacijas ir jų išvestinius kūrinius, lieka Pirkėjui. Jokia šios Techninės specifikacijos dokumentacijos (toliau – TSD) nuostata negali būti aiškinama kaip suteikianti Tiekėjui nuosavybės ar kitų turtinių teisių į Pirkėjo duomenis.
3. Tiekėjas užtikrina su Rezultatu susijusių Pirkėjo asmens duomenų apsaugą, taikydamas privatumo ir saugumo principus „pagal projektavimą“ ir „pagal numatymą“ (*angl. by design and by default*).
4. Tiekėjas saugo Pirkėjo duomenis nuo neteisėtos prieigos, atskleidimo, pakeitimo ar sunaikinimo, laikydamasis Pirkėjo taikomų duomenų klasifikavimo taisyklių. Šie reikalavimai taikomi nepriklausomai nuo to, ar Pirkėjo duomenys yra perduodami, naudojami ar saugomi. Siekdamas užkirsti kelią atsitiktiniam ar neteisėtam Pirkėjo duomenų praradimui, sunaikinimui, pakeitimui ar sugadinimui, vadovaudamasis taikytinais Reguliaciniais reikalavimais, Tiekėjas viso Sutarties ir Rezultatų gyvavimo ciklo metu taiko tinkamas technines ir organizacines apsaugos priemones.
5. Šifravimo metodai ir raktų valdymo praktikos turi būti suderintos su Pirkėju ir apibrėžtos Sutartyje. Siekdamas užtikrinti tinkamą saugumo ir sistemų konfigūracijų valdymą, Tiekėjas privalo turėti dokumentuotas saugumo procedūras ir jas reguliariai peržiūrėti bei tobulinti. Kriptografinės technologijos naudojamos Rezultatų ir su jais susijusių Pirkėjo duomenų konfidencialumui ir vientisumui užtikrinti, tais atvejais, kai Pirkėjas.
6. Tiekėjas reguliaria ii atlieka vientisumo ir išbaigtumo patikras, skirtas patvirtinti atsarginių duomenų kopijų tikslumą bei informacijos, saugomos Tiekėjo Rezultate (-uose), patikimumą ir užkirsti kelią duomenų klastojimui.
7. Kai duomenų bazes administruoja Tiekėjas, jis užtikrina, kad pagrindinės Pirkėjo duomenų bazių atsarginių kopijų kopijos būtų užšifruotos ir saugomos fiziškai atskiroje vietoje nuo gamybinės (produkcinės) aplinkos. aplinkos. Tiekėjas nustato atsarginių kopijų kūrimo ir atkūrimo procesus bei procedūras ir jas reguliariai testuoja.

8. Kai Tiekėjas tvarko Pirkėjo duomenis, kurie yra asmens duomenys, jis integruoja šiuos duomenis į taikytinus duomenų saugojimo (*angl. retention*) procesus ir laikosi nustatytų saugojimo terminų, užtikrindamas šių duomenų apsaugą pagal su Pirkėju suderintą Duomenų tvarkymo sutartį (toliau – DTS); (*angl. Data Privacy Agreement*).
9. Nutraukus Sutartį, Tiekėjas Pirkėjo nurodymu grąžina arba sunaikina visus Pirkėjo duomenis ir jų kopijas bei pateikia Pirkėjui rašytinį sunaikinimo patvirtinimą. Grąžinus Pirkėjo duomenis, Tiekėjas privalo sunaikinti visas likusias jų kopijas, išskyrus atvejus, kai duomenų saugojimas aiškiai leidžiamas Sutartyje. Asmens duomenų saugojimo terminai nustatomi DTS. Pirkėjui pareikalavus, Tiekėjas raštu patvirtina, kad šis reikalavimas įvykdytas. Pirkėjo duomenys gali būti saugomi tik jei tai leidžiama Sutartyje.

4.5 Prieigos valdymas

[ISO/IEC 27001:2022 A.5.15–A.5.18]

1. Tiekėjas privalo įgyvendinti ir palaikyti šias prieigos kontrolės priemones:

   a. Apibrėžtą ir dokumentuotą prieigos kontrolės politiką patalpoms, susijusioms su paslaugų teikimu Pirkėjui, vietovėms, tinklui, sistemoms, taikomosioms programoms ir informacijos bei duomenų prieigai, įskaitant fizinę, loginę ir nuotolinę prieigos kontrolę.

   b. Procesus, skirtus saugiam tapatybių ir prisijungimo duomenų (kredencialų) valdymui.

   c. Naudotojų prieigos teisių ir privilegijų suteikimo (autorizavimo) procesus.

   d. Prieigos teisių valdymo procesus darbuotojų įdarbinimo, pareigų keitimo ir darbo santykių nutraukimo atvejais (*angl. joiners, movers, leavers*).

   e. Prieigos teisių pakeitimų valdymo procesus, apimančius naujų prieigų suteikimą, esamų prieigų keitimą ir panaikinimą) *(angl. new, changes and deletions*).

   f. Procesus, užtikrinančius saugų prieigos privilegijų naudojimą Tiekėjo personalui, kuriam būtina prieiga prie Rezultato.

   g. Reguliarų prieigos teisių ir privilegijų suteikimo, peržiūros ir panaikinimo procesą, vadovaujantis principu „reikia žinoti“ (*angl. need-to-know*) ir mažiausių privilegijų principu; ir

   h. Tiekėjo taikomosios programos privalo užtikrinti naudotojų autentifikavimą, autorizavimą ir veiksmų atsekamumą.

   i. Kiekvienas naudotojas turi būti unikaliai identifikuojamas; bendromis naudotojų paskyromis naudotis neleidžiama.

   j. Standartinėms naudotojų paskyroms negali būti suteikiamos privilegijuotos prieigos teisės. Privilegijuotai prieigai prie sistemų, tinklų ar kitos skaitmeninės infrastruktūros turi būti naudojamos atskiros administratoriaus paskyros

   k. Tiekėjas ne rečiau kaip kartą per 12 (dvylika) mėnesių peržiūri visas savo sistemoms suteiktas prieigos teises, siekdamas patvirtinti, kad tokia prieiga ar prisijungimo duomenys (kredencialai) vis dar yra reikalingi.

   l. Tiekėjas įgyvendina daugiafaktorį autentifikavimą (MFA) prieigai prie Rezultate tvarkomų duomenų, bent jau privilegijuotą prieigą turintiems naudotojams

   m. Jei naudotojas ilgiau nei 3 (tris) mėnesius aktyviai nesinaudoja kritine Tiekėjo sistema, jo prieigos teisės turi būti sustabdytos arba panaikintos. Administratoriaus paskyrų prieiga sustabdoma po 2 (dviejų) mėnesių neveikimo.

2. Jei Tiekėjas turi prieigą prie Pirkėjo IT sistemų, tinklų ar kito informacinių ir ryšių technologijų (IRT) turto, Šalys pasirašo atskirą Nuotolinės prieigos sutartį (*angl. Remote Access Agreement*) (1).
3. Jei Tiekėjas turi prieigą prie Pirkėjo fizinių patalpų, Tiekėjas privalo laikytis Pirkėjo taikomų prieigos kontrolės ir valdymo tvarkų bei šių reikalavimų:

a. Identifikavimo tikslais, kai prieigos kortelę išduoda Pirkėjas, ji turi būti naudojama ,laikantis Sutarties ir Pirkėjo vidaus taisyklių. Pirkėjo išduota kortelė visada turi būti nešiojama matomoje vietoje, o asmens tapatybę patvirtinantis dokumentas – turimas su savimi.

b. Tiekėjo naudotojai ir partneriai atsako už visus veiksmus, atliekamus naudojant jiems priskirtus prieigos raktus, prieigos korteles ir (ar) kitus prisijungimo duomenis. Draudžiama perduoti ar leisti naudotis asmens tapatybės kortelėmis, raktais, PIN kodais ar slaptažodžiais tretiesiems asmenims.

c. Pametus prisijungimo duomenis, raktus, korteles ir pan., arba kilus pagrįstam įtarimui dėl jų kompromitavimo, apie tai būtina nedelsiant pranešti el. saugos_komanda@telia.lt.d. Naudotojams draudžiama sudaryti sąlygas neįgaliotiems asmenims patekti į Pirkėjo patalpas ar turto objektus.

e. Be atskiro Pirkėjo leidimo ir kitais tikslais nei tiesioginių darbo užduočių vykdymas draudžiama Pirkėjo patalpose filmuoti, fotografuoti, atlikti su darbo užduotimis nesusijusius veiksmus, prijungti arba palikti su darbo užduotimis nesusijusius įrenginius

f. Patalpose draudžiama vartoti alkoholinius gėrimus ar kitas toksines, psichotropines ar narkotines medžiagas, taip pat būti neblaiviam ar apsvaigus nuo narkotinių, toksinių ar psichotropinių medžiagų

g. Draudžiama Pirkėjo teritorijoje ar patalpose laikyti šaudmenis, sprogmenis ar kitus ginklus, taip pat veiksmais ar neveikimu sukelti pavojų kito asmens sveikatai ar gyvybei arba įrangos veikimui

h. Pirkėjo patalpose ir teritorijoje privaloma laikytis visų taikytinų prieigos ir saugumo tvarkų, darbuotojų saugos ir sveikatos, priešgaisrinės saugos bei kitų teisės aktų reikalavimų, taip pat vykdyti atsakingų Pirkėjo darbuotojų nurodymus.

i. Draudžiama dirbti su techniškai netvarkinga darbo įranga.

4.6 Dirbtinis intelektas (DI) arba autonominės technologijos (ATT)

[ISO/IEC 27001:2022 A.5.9, A.5.12, A.5.14, A.5.15, A.5.19, A.8.25]

1. Dirbtinio intelekto (toliau – DI) arba autonominių technologijų (toliau – ATT) naudojimas Rezultatuose turi būti iš anksto suderintas su Pirkėju **prieš tokio naudojimo įgyvendinimą**.
2. Tais atvejais, kai Rezultatas apima arba naudoja DI arba ATT, Tiekėjas privalo laikytis šių reikalavimų:
    a. Pateikti Pirkėjui aktualią ir pakankamą informaciją apie Rezultatuose taikomas DI arba ATT saugumo priemones.
    b. Identifikuoti, dokumentuoti ir įgyvendinti DI ir ATT saugumo bei duomenų privatumo reikalavimus, kurie atitiktų Pirkėjo taikomus saugumo ir duomenų privatumo reikalavimus.
3. Tiekėjas gali naudoti DI arba ATT Pirkėjo duomenims tvarkyti tik tuo atveju, jei vienu metu yra įvykdyti visi šie reikalavimai:
    a. DI arba ATT neteikia subjektas, registruotas ar veikiantis didelės rizikos šalyje;
    b. DI arba ATT atitinka visus taikytinus Reguliacinius reikalavimus ir užtikrina Pirkėjo duomenų konfidencialumą, vientisumą ir prieinamumą; ir
    c. Pirkėjo duomenys nėra naudojami jokio DI ar ATT modelių, apmokymui, pakartotiniam apmokymui, tobulinimui ar testavimui.

Jei, Pirkėjo vertinimu, Tiekėjas teikia kritines paslaugas, taikomos šios papildomos DI ir ATT kontrolės priemonės:

4. Tiekėjas įgyvendina DI testavimo, vertinimo, validavimo ir verifikavimo praktikas (*angl. Artificial Intelligence Testing, Evaluation, Validation and Verification - AI TEVV*), sudarydamas sąlygas DI ir (ATT testavimui, incidentų nustatymui, analizei ir informacijos dalijimuisi su Pirkėju
5. Jei Pirkėjas įsigyja stebėsenos paslaugas, Tiekėjas stebi įdiegto dirbtinio intelekto (DI) ir autonominių technologijų (ATT), įtrauktų į Rezultatą, funkcionalumą ir elgseną. Tais atvejais, kai Pirkėjas yra įsigijęs

stebėsenos paslaugas, Tiekėjas vykdo Rezultate įdiegtų dirbtinio intelekto (DI) ir autonominių technologijų (ATT) funkcionalumo bei elgsenos stebėseną.

6. Tiekėjas identifikuoja ir taiko saugaus inžinerinio projektavimo principus, siekdamas užtikrinti, kad Rezultatai, kuriuose naudojamos ATT, būtų sukurti kaip patikimi, saugūs, teisingi, apsaugoti, atsparūs, skaidrūs, paaiškinami, taip pat sustiprinti tinkamomis duomenų privatumo apsaugos priemonėmis, siekiant sumažinti atsirandančias savybes ir (a)r nepageidaujamas pasekmes.
7. Tiekėjas atlieka išsamų vystymo ir iki diegimo funkcionalumo, saugumo bei duomenų privatumo testavimą visoms vidinėms ir trečiųjų šalių ATT, įtrauktoms į Rezultatą.
8. Tiekėjas nuolat stebi ATT naudojimą Tiekėjo gamybinėje (produkcinėje) aplinkoje, susijusį su Rezultato teikimu, siekdamas laiku nustatyti ir sumažinti atsirandančias savybės ar nepageidaujamas pasekmes.
9. Tiekėjas privalo turėti incidentų valdymo ir veiklos tęstinumo planus (angl. Business Continuity Plan - BCP), leidžiančius reaguoti į su Rezultatu susijusias ATT atsirandančias savybes, grėsmes ar nepageidaujamas pasekmes. Prireikus, Tiekėjas įsipareigoja bendradarbiauti ir padėti Pirkėjui reaguojant į tokias ATT atsirandančias savybes, grėsmes ir pasekmes.

4.7 Tiekėjo santykiai su Tiekėjo subrangovais

[ISO/IEC 27001:2022 A.5.19–A.5.22]

1. Tiekėjas įsipareigoja įtraukti šios TSD reikalavimus į susitarimus su visais subrangovais, dalyvaujančiais teikiant Rezultatą. Šie reikalavimai gali būti derinami, papildomi ar pritaikomi atsižvelgiant į subrangovo naudojamas technologijas, tačiau jie turi būti proporcingi rizikoms, susijusioms su subrangovo teikiamomis paslaugomis.
2. Pirkėjui pareikalavus, Tiekėjas pateikia pagrįstus įrodymus apie subrangovų atitiktį šios TSD reikalavimams.
3. Tiekėjas reguliariai stebi, peržiūri ir, kai taikytina, audituoja savo subrangovų atitiktį šios TSD reikalavimams.
4. Pirkėjas turi teisę audituoti, kaip Tiekėjas ir jo subrangovai laikosi bei įgyvendina šios TSD reikalavimus
5. Tiekėjas identifikuoja, vertina, valdo ir mažina subrangovų keliamas kibernetinio saugumo ir duomenų privatumo rizikas, siekdamas užtikrinti nepertraukiamą paslaugų teikimą tais atvejais, kai subrangovas patiria veiklos sutrikimus, yra kompromituojamas, tampa nepatikimas ar nutraukia veiklą. Tiekėjas identifikuoja, vertina, valdo ir mažina subrangovų keliamas kibernetinio saugumo ir duomenų privatumo rizikas, siekdamas užtikrinti nepertraukiamą paslaugų teikimą tais atvejais, kai subrangovas patiria veiklos sutrikimus, yra kompromituojamas, tampa nepatikimas ar nutraukia veiklą.
6. Tiekėjas užtikrina, kad visiems subrangovams, dalyvaujantiems teikiant Rezultatą, būtų taikomos tinkamos organizacinės ir techninės saugumo priemonės, skirtos sumažinti rizikas, susijusias su Tiekėjo tiekimo grandinės silpnybėmis ar trūkumais.

4.8 Debesijos saugumas

[ISO/IEC 27001:2022 A.5.23]

1. Prieš pradedant naudoti debesijos technologijas, Pirkėjas ir Tiekėjas Sutartyje susitaria dėl Pirkėjo duomenų saugojimo vietos ir dėl Tiekėjo prieigos prie šių duomenų
2. Tiekėjas užtikrina, kad bendroje debesijos paslaugų teikėjo (ang. *Cloud Service Provider*, toliau – CSP) aplinkoje skirtingi nuomininkai (angl. *tenants*) neturėtų galimybės pasiekti vieni kitų duomenų ar sistemų.
3. Tiekėjas užtikrina, kad CSP taikytų saugius metodus Pirkėjo duomenų importavimui, eksportavimui ar valdymui.
4. Kai techniškai įmanoma bei pagrįsta Tiekėjas debesijos aplinkoje sukuria atskirus potinklius (*angl. subnets*), skirtus saugumo priemonėms, apsaugančioms Rezultatą.
5. Tiekėjas taiko ir prižiūri tinklo saugumo taisykles visiems jo valdomiems potinkliams.

6. Tiekėjas užtikrina saugų skirtingų sistemos komponentų tarpusavio ryšį, įskaitant, bet neapsiribojant, ryšį per taikomąsias sąsajas (angl. APIs).
7. Tiekėjas užtikrina, kad CSP aplinkoje būtų galimybė generuoti, saugoti ir Pirkėjui pateikti su Rezultatu susijusius saugumo įvykių žurnalus (*angl. security event logs*).

4.9 Reagavimas į saugumo incidentus

[ISO/IEC 27001:2022 A.5.24–A.5.28]

1. Tiekėjas privalo turėti dokumentuotus ir veikiančius planus ir procesus saugumo incidentams nustatyti, valdyti, spręsti bei jų laikytis saugumo incidento atveju
2. Jei įvyksta saugumo incidentas, susijęs su Tiekėjo teikiamu Rezultatu arba turintis jam įtakos, Tiekėjas privalo:
    a. Nedelsdamas pradėti veiksmus, reikalingus incidentui lokalizuoti, suvaldyti ir sumažinti jo plitimą bei poveikį
    b. Nepagrįstai nedelsdamas informuoti Pirkėją, bet ne vėliau kaip per (24) dvidešimt keturias valandas nuo sužinojimo apie saugumo incidentą, pateikdamas pirminį pranešimą , kuriame (kiek įmanoma) nurodoma, ar saugumo incidentas galėjo kilti dėl neteisėtų ar piktavališkų veiksmų, ir ar jis gali turėti tarpvalstybinį poveikį.
    c. Pateikti išsamesnį pranešimą ne vėliau kaip per 72 (septyniasdešimt dvi)) valandas nuo sužinojimo apie saugumo incidentą, įskaitant atnaujintą informaciją, papildančią pirminį ankstyvą perspėjimą, pirminį saugumo incidento rimtumo ir poveikio vertinimą bei bet kokius turimus kompromitavimo ar įsilaužimo įrodymus.
    d. Bendradarbiauti su Pirkėju reaguojant į saugumo incidentą ir valdanti jo poveikį, taip pat pateikti turimus pirminius incidento duomenis.
    e. Pateikti galutinę incidento ataskaitą per 20 (dvidešimt) kalendorinių dienų nuo tos dienos, kai saugumo incidentas buvo suvaldytas.
3. Visos su saugumo incidentais susijusios ataskaitos laikomos konfidencialiomis ir, Pirkėjui pareikalavus, turi būti perduodamos užšifruotu būdu, naudojant patikimus pramonės standartus atitinkančias kriptografines priemones (pvz., PGP).
4. Saugumo incidento atveju, Pirkėjas turi teisę atlikti incidento auditą po incidento uždarymo, apie tai raštu įspėjęs Teikėją ne vėliau kaip prieš 5 (penkias) darbo dienas. Auditas vykdomas įprastomis darbo valandomis ir organizuojamas taip, kad būtų kiek įmanoma sumažintas poveikis Tiekėjo veiklai ir gamybinei (produkcinei) aplinkai ir jos os sutrikdymui.
5. Kiekvienam Tiekėjo talpinamam Rezultatui Tiekėjas užtikrina jo integraciją į Saugumo operacijų centro (SOC) procesus, įskaitant saugumo įvykių stebėseną, žurnalų (angl. *logs*) analizę, saugumo užklausų (angl. tickets) valdymą ir grėsmių informacijos analizę
6. Tiekėjas užtikrina, kad Rezultatas būtų įtrauktas į reagavimo incidentų planus, kurie turi apimti ir reagavimą į išpirkos reikalaujančių kenkėjiškų programų (*angl. ransomware*) atakas ir jų valdymą
7. Tiekėjas paskiria saugumo kontaktinį asmenį, kuris koordinuoja informacijos teikimą ir komunikacija su Pirkėju saugumo incidento atveju, kai incidentas paveikia Rezultatą.
8. Tiekėjas ne rečiau kaip kartą per metus peržiūri ir, prireikus, atnaujina reagavimo į incidentus planus.

4.10 Atkūrimas po saugumo incidentų

[ISO/IEC 27001:2022 A.5.29, A.5.30; NIST CSF 2.0 RC.RP-01–RC.RP-03]

1. Tiekėjas privalo turėti dokumentuotus, aiškius ir išbandytus planus bei procesus, skirtus atkūrimui po saugumo incidentų ir saugumo incidento atveju jų laikytis.
2. Tiekėjas reguliariai kuria, testuoja, peržiūri ir tobulina saugumo incidentų padarinių šalinimo ir atkūrimo planus bei procesus, siekdamas užtikrinti jų veiksmingumą ir savalaikį taikymą.
3. Jei saugumo incidentas paveikia Rezultatą, Tiekėjas įsipareigoja bendradarbiauti su Pirkėju ir teikti visą būtiną pagalbą, reikalingą Rezultato atkūrimui, įskaitant, bet neapsiribojant technine pagalba, incidento analizės duomenimis ir atkūrimo veiksmų koordinavimu.

5 Saugumo reikalavimai – žmogiškieji aspektai

5.1 Personalo saugumas

[ISO/IEC 27001:2022 A.6.1, A.6.2]

1. Tiekėjas privalo turėti darbuotojų, konsultantų, rangovų ir subrangovų patikros ir atrankos procesus (angl. *screening ir vetting*), kurie taikomi prieš suteikiant jiems prieigą prie Pirkėjo duomenų ir Rezultatų.
2. Tiekėjas įsipareigoja nedelsdamas informuoti Pirkėją apie bet kurį su Rezultatu susijusį Tiekėjo personalo narį, kuris nesilaiko Tiekėjo saugumo direktyvos saugumo politikų ir standartų.
3. Tiekėjas užtikrina, kad Tiekėjo personalas, kuris suteikiama prieiga prie neviešos Pirkėjo informacijos, prieš gaudamas tokią prieigą būtų prisiėmęs konfidencialumo ar informacijos neatskleidimo įsipareigojimus Tiekėjo naudai.
4. Tiekėjas informuoja Pirkėją apie Tiekėjo personalo pasikeitimus, susijusius su Rezultatu (pvz., perkėlimus, pareigų pasikeitimus, darbo santykių nutraukimą), tais atvejais, kai prieiga prie Rezultato nėra pilnai valdoma Pirkėjo.
5. Tiekėjas užtikrina, kad Tiekėjo personalas laikytųsi Tiekėjo saugumo direktyvos, politikų, procedūrų ar kitų taikytinų saugumo reikalavimų.
6. Tiekėjas užtikrina, kad bet kuris Tiekėjo personalas, vykdantis užduotis pagal Sutartį, būtų patikimas ir atitiktų nustatytus saugumo kriterijus, atsižvelgiant į konkrečios užduoties pobūdį ir riziką.
7. Tiekėjas užtikrina, kad Tiekėjo personalas, kuriam taikomi nacionalinio saugumo patikrinimo (*angl. security clearance*) reikalavimai, laikytųsi Pirkėjo nustatytų nacionalinio saugumo patikrinimo procedūrų.
8. Tiekėjas užtikrina, kad saugumo informuotumo ir mokymų programos būtų pritaikytos pagal darbuotojų roles ir atsakomybes.
9. Tiekėjas užtikrina, kad visi asmenys, paskirti vykdyti užduotis pagal Sutartį, turėtų reikiamus ir tinkamai dokumentuotus profesinius įgūdžius, mokymus, sertifikatus ir kvalifikacijas, būtinas Paslaugų teikimui, įskaitant pakankamas žinias ir kompetencijas informacijos ir kibernetinio saugumo srityje. Tokios kompetencijos turi atitikti pripažintus informacijos saugumo standartus ir būti proporcingos atliekamų užduočių pobūdžiui bei apimčiai, siekiant užtikrinti saugų, patikimą ir teisės aktus atitinkantį Paslaugų teikimą.

6 Saugumo reikalavimai – fizinės kontrolės

6.1 Fizinis ir aplinkos saugumas

[ISO/IEC 27001:2022 A.7.1, A.7.2]

1. Tiekėjas užtikrina, kad visos duomenų centro patalpos, naudojamos įrangai (*angl. hardware*), kuria teikiamas Rezultatas, talpinti, būtų aprūpintos tinkamomis fizinėmis ir elektroninėmis saugumo priemonėmis, taip pat perteklinėmis (angl. *redundant*) aplinkos kontrolės sistemomis (įskaitant temperatūros ir drėgmės kontrolę) bei patikimu elektros energijos tiekimu.
2. Kiekvienam Tiekėjo talpinamam Rezultatui Tiekėjas privalo užtikrinti:
    a. apsaugoti savo patalpas nuo išorinių ir aplinkos grėsmių bei pavojų, įskaitant elektros/laidų gedimus ir kitus sutrikimus, kurie gali neigiamai paveikti Rezultatą; Patalpų apsaugą nuo išorinių ir aplinkos grėsmių bei pavojų, įskaitant elektros tiekimo, laidų ar kitus techninius sutrikimus, galinčius neigiamai paveikti Rezultato veikimą.
    b. fizinę perimetro apsaugą ir prieigos kontrolės priemones, susijusias su Rezultatu;
    c. procesus, užtikrinančius saugų fizinių laikmenų, susijusių su Rezultatu, sunaikinimą ar šalinimą;
    d. nuolat atnaujinamą Tiekėjo personalo, turinčio įgaliotą fizinę prieigą prie Tiekėjo patalpų, susijusių su Rezultatu, sąrašą;
    e. fizinės prieigos kontrolės mechanizmus, skirtus identifikuoti, aptikti ir reaguoti į fizinio saugumo incidentus;
    f. rizikos valdymo procesus, skirtus fizinio saugumo rizikoms identifikuoti, vertinti, valdyti ir mažinti patalpose, kuriose talpinamas Rezultatas

g. pareigą informuoti Pirkėją apie bet kokį fizinio saugumo incidentą, susijusį su Rezultatu, laikantis šios TSD 3 skyriuje nustatytų pranešimo reikalavimų.

7 Saugumo reikalavimai – technologinės kontrolės

7.1 Galinių įrenginių ir mobiliųjų įrenginių valdymas

[ISO/IEC 27001:2022 A.8.1, A.5.18]

1. Tiekėjas privalo laikytis šių reikalavimų dėl Tiekėjo galinių įrenginių (*angl. end-point*) , naudojamų prieigai prie Pirkėjo sistemų ar informacijos:
    h. Įrenginiai negali būti palikti atrakinti, kai yra be priežiūros.
    i. Visi nešiojamieji kompiuteriai ir mobilieji įrenginiai turi būti sukonfigūruoti taip, kad automatinis ekrano užraktas įsijungtų ne vėliau kaip po 15 (penkiolikos) minučių neveikimo.
    j. Naudotojai turi autentifikuotis naudodami tik savo asmeninius prisijungimo duomenis.
    k. Bendri arba kelių naudotojų įrenginiai turi užtikrinti, kad kiekvienas vartotojas prieš naudodamasis įrenginiu prisijungtų naudodamas savo unikalią paskyrą.
    l. Visi autentifikavimo mechanizmai turi būti apsaugoti patikimomis saugumo priemonėmis, įskaitant stiprius slaptažodžius, PIN kodus, atitinkančius nustatytus saugumo sudėtingumo reikalavimus, arba patvirtintus biometrinio autentifikavimo metodus (pvz., piršto atspaudo ar veido atpažinimo).
    m. Įrenginiuose turi būti įdiegta ir nuolat atnaujinama antivirusinė ir kenkėjiškų programų prevencijos programinė įranga, įjungta realiojo laiko apsauga ir sukonfigūruoti automatiniai saugumo atnaujinimai.
2. Tiekėjas identifikuoja, vertina, valdo ir mažina visas rizikas, susijusias su Tiekėjo galinių įrenginių prieiga prie Rezultato.

7.2 Pajėgumų ir našumo planavimas

[ISO/IEC 27001:2022 A.8.6]

1. Tiekėjas įsipareigoja iš anksto informuoti Pirkėją apie bet kokius reikšmingus esamus ar numatomus našumo sutrikimus, kurie gali turėti įtakos Rezultatų teikimui. Tiekėjas taip pat privalo turėti dokumentuotus pajėgumų ir našumo planus, apimančius visą Sutarties galiojimo laikotarpį.
2. Kai taikytina, Tiekėjas privalo naudoti automatizuotus stebėsenos įrankius, skirtus nuolat stebėti Tiekėjo gamybinės (produkcinės) aplinkos būseną, siekiant laiku identifikuoti našumo ar pajėgumų problemas.

7.3 Pažeidžiamumų ir pataisų (*angl. patch*) valdymas

[ISO/IEC 27001:2022 A.8.8, A.8.9]

1. Tiekėjas užtikrina, kad Rezultatui būtų diegiami naujausi stabilūs saugumo atnaujinimai, laikantis Tiekėjo nustatytų pataisų (angl. *patch management*) diegimo procesų.
2. Tiekėjas užtikrina, kad programinės ir techninės įrangos atnaujinimai, skirti Tiekėjo naudojamai infrastruktūrai, būtų įdiegiami laiku, o Rezultatui teikti naudojama įranga ir programinė įranga būtų palaikoma gamintojo bent kibernetinio saugumo prasme.
3. Kiekvienam Tiekėjo talpinamam Rezultatui Tiekėjas privalo užtikrinti:
    a. Pažeidžiamumų skenavimą ne rečiau kaip kas 30 (trisdešimt) kalendorinių dienų.
    b. Pažeidžiamumų skenavimo rezultatų saugojimą ne trumpiau kaip 12 (dvylika mėnesių nuo skenavimo datos.
    c. Kad Rezultatas ir bet kurie jį palaikantys komponentai nebūtų naudojami pasibaigus gamintojo palaikymo laikotarpiui (*angl. End of Support*).
    d. Saugumo atnaujinimų diegimą pagal Tiekėjo pataisų valdymo procesus, u, užtikrinant savalaikį kritinių pažeidžiamumų šalinimą.
    e. Pažeidžiamumų ir naudojamų komponentų identifikavimą bei dokumentavimą, įskaitant programinės įrangos komponentų sąrašo (angl. *Software Bill of Materials*, toliau - SBOM) parengimą plačiai

naudojamu, mašininio skaitymo formatu, apimančiu bent aukščiausio lygmens priklausomybes (*angl. top-level dependencies*).

7.4 Konfigūracijų ir saugumo žurnalų valdymas

[ISO/IEC 27001:2022 A.8.9]

1. Tiekėjas įgyvendina ir palaiko saugumo konfigūracijų ir žurnalų (angl. *logging*) valdymo praktikas, taikomas Rezultatui.

2. Tiekėjas užtikrina, kad Rezultate nebūtų diegiama neautorizuota programinė įranga
3. Tiekėjas užtikrina, kad saugios bazinės konfigūracijos (*angl. secure baseline*) Rezultatui apimtų bent jau šiuos reikalavimus:
    a. Prieigos prie Rezultato apribojimą pagal nutylėjimą (*angl. default*);
    b. žurnalų generavimą, kuriuose būtų pakankamai informacijos veiklos detalėms identifikuoti ir skaitmeninei tyrimui (angl. *forensic*s) atlikti
    c. užtikrinimą, kad jautrūs ar reguliuojami Pirkėjo duomenys nebūtų fiksuojami žurnaluose;
    d. Saugumo įvykių žurnalų (*angl. Security Event Logs*) saugojimą ne trumpiau kaip 90 (devyniasdešimt) kalendorinių dienų; tokie žurnalai turi būti apsaugoti nuo neleistinų pakeitimų ar klastojimo ir saugomi atskiroje vietoje nuo sistemos, kurioje jie sugeneruoti;
    e. vidinių sistemos laikrodžių naudojimą laiko žymoms (*angl. timestamps*) generuoti, sinchronizuojant juos bent su dviem nepriklausomais autoritetingais laiko šaltiniais.

7.5 Saugumo grėsmių aptikimas

[ISO/IEC 27001:2022 A.8.15–A.8.17]

1. Tiekėjas vykdo nuolatinę saugumo grėsmių, saugumo incidentų ir neautorizuotos veiklos stebėseną. Tiekėjas identifikuoja, vertina, valdo ir mažina kibernetinio saugumo bei privatumo rizikas, susijusias su Pirkėjo duomenimis ir jų tvarkymu.

2. Tiekėjas renka ir analizuoja saugumo įvykių žurnalus (*angl. Security Event Logs*) Tiekėjo talpinamiems Rezultatams, naudodamas centralizuotas žurnalų valdymo sistemas. Tiekėjas privalo turėti dokumentuotus procesus, skirtus saugumo incidentams ar neautorizuotai veiklai aptikti, analizuoti ir valdyti, įskaitant saugumo užklausų (*angl. tickets*) valdymą, žurnalų stebėseną ir grėsmių žvalgybos (*angl. threat intelligence*) peržiūrą.

3. Tiekėjas privalo nustatyti, prioritetizuoti ir šalinti saugumo pažeidžiamumus bei nuolat tobulinti grėsmių aptikimo ir reagavimo praktikas.

4. Tiekėjo talpinamiems Rezultatams taikomi šie reikalavimai:
    a. Naudoti automatizuotus įrankius žurnalams centralizuotai rinkti ir, Pirkėjui paprašius, integruoti juos su Pirkėjo naudojamais įrankiais.
    b. Įtraukti Rezultatą į incidentų valdymo procesus, apimančius pasirengimąs, aptikimą, analizę, suvaldymą, pašalinimą ir atkūrimą
    c. Užtikrinti galimybę, Pirkėjui pareikalavus, perduoti žurnalus į Pirkėjo įvykių koreliacijos sistemas.
5. Saugumo įvykių žurnalai (*angl. Security Event Logs*) turi atitikti šiuos reikalavimus:
    a. Būti saugomi ne trumpiau kaip 6 (šešis) mėnesius.
    b. Naudoti koordinuotojo pasaulinio laiko (UTC) laiko žymas (*angl. timestamps*), o sistemų laikrodžius sinchronizuoti naudojant patikimus laiko sinchronizavimo protokolus (pvz., NTP).
    c. Apimti informaciją apie naudotojų veiksmus, pvz., naudotojo vardas, įrenginio pavadinimas, šaltinio ir paskirties IP MAC adresą (kam taikoma).
    d. Nurodyti objektą, su kuo buvo atliktas veiksmas (pvz., failo pavadinimą, įrašo ID, kompiuterio pavadinimą, sistemą ar paslaugą).
    e. Fiksuoti veiksmų rezultatą (leistas ar atmestas) ir, kiek įmanomą, pateikti priežasties kodą ar paaiškinimą
    f. Kai techniškai įmanoma, turėti žurnalų koreliacijos ID (angl. *correlation ID*).
    g. Būti struktūruoti ir tinkami automatizuotai įvykių koreliacijai ir analizei.

7.6 Tinklo saugumas

[ISO/IEC 27001:2022 A.8.20, A.8.21]

1. Tiekėjas įgyvendina tinkamas tinklo saugumo ir privatumo kontrolės priemones, užtikrinančias Pirkėjo duomenų konfidencialumą, vientisumą irprieinamumą, taip pat bendrą informacijos saugą bei privatumo apsaugą. □
2. Tiekėjo tinkle naudojami kritiniai ištekliai turi būti apsaugoti nuo galimų atakų ar užkrėtimo iš kitų tame pačiame esančių įrenginių. Tokia apsauga įgyvendinama taikant Tiekėjui prieinamas technines priemones, įskaitant, bet neapsiribojant, ugniasienėmis (*angl. firewalls*), tinklo segmentavimu, IP adresų valdymu ar kitais tinkamais sprendimais.

7.7 Interneto (*angl. Web*) saugumo rizikų valdymas

[ISO/IEC 27001:2022 A.8.22–A.8.23]

1. Tiekėjo talpinamiems Rezultatams Tiekėjas privalo valdyti rizikas, susijusias su komponentais, pasiekiamais iš interneto (pvz., API), taikydamas Rezultato griežtinimo (angl. *hardening*) priemones, failų vientisumo stebėseną, auditavimo mechanizmus ir piktavališkos veiklos aptikimo priemones, jei Šalys nesusitarta kitaip.
2. Pirkėjo perimetro apsaugos priemonės turi atitikti šiuos reikalavimus:
    a. Naudoti žiniatinklio taikomųjų programų ugniasienes (angl. *Web Application Firewalls,* WAF), užtikrinančias daugiasluoksnę (*angl. defence-in-depth*) Rezultato apsaugą nuo grėsmių.
    b. Riboti įeinantį srautą į Rezultatą tik autorizuotiems įrenginiams, sistemoms ar paslaugoms, tai pat konkrečioms geografinėms vietovėms, protokolams ir prievadams (*angl. ports*).
    c. Taikyti IP adresų leidžiamųjų (*angl. whitelist*) ir blokavimo (*angl. blacklist*) sąrašų praktikas.
    d. Atlikti į internetą atvirų (*angl. exposed*) ir Tiekėjo talpinamų Rezultatų įsiskverbimo testavimų (*angl. penetration test*) vertinimus.
3. Tiekėjas užtikrina, kad taikomosiose programose, naudojamose Rezultatui teikti, nebūtų kietai įrašytų (*angl. hard-coded*) prisijungimo duomenų ar kitų slaptų reikšmių, pvz., naudotojų vardų, slaptažodžių, API raktų, prieigos žetonų (*angl. token*), kurių atskleidimas galėtų suteikti neteisėtą prieigą prie Pirkėjo duomenų ar sistemų.

7.8 Kriptografinė apsauga

[ISO/IEC 27001:2022 A.8.24]

1. Jei tai numatyta Sutartyje, Tiekėjas užtikrina Pirkėjo duomenų šifravimą tiek jų perdavimo, tieksaugojimo metu.
2. Tiekėjas šifravimui naudoja tik tokius protokolus, kurie laikomi saugiais pagal pripažintus pramonės standartus.
3. Nuosavų (*angl. proprietary*) šifravimo algoritmų naudojimas galimas tik po išankstinės p peržiūros ir gavus rašytinį Pirkėjo patvirtinimą.
4. Tiekėjas užtikrina, kad naudotojų prisijungimo duomenys autentifikavimo proceso metu būtų perduodami tik saugiais (užšifruotais) ryšio kanalais.
5. Jei Pirkėjas nusprendžia Rezultatui naudoti Tiekėjo viešojo rakto infrastruktūrą (angl. *Public Key Infrastructure*, PKI), Tiekėjas užtikrina Pirkėjo duomenų prieinamumą tais atvejais, kai naudotojai praranda kriptografinius raktus.
6. Tiekėjas užtikrina kriptografinių raktų, susijusių su Rezultatu, periodinį keitimą ne rečiau kaip kartą per metus, taip pat nedelsiant po saugumo incidentų. Pasibaigusio galiojimo raktai yra nebenaudojami saugomi taikant tokias pačias apsaugos priemones, kaip ir aktyviai naudojamiems raktams iki jų galutinio sunaikinimo.
7. Tiekėjas užtikrina, kad kriptografiniai raktai, naudojami Rezultate, būtų saugomi tik aplinkose, atitinkančiose pripažintas saugaus raktų valdymo gerąsias praktikos (*angl. industry best practices*).

7.9 Saugi inžinerija ir architektūra

[ISO/IEC 27001:2022 A.8.25, A.8.26]

1. Kai taikoma, Tiekėjas užtikrina, kad Rezultato architektūra, kūrimo (*angl. development*) ir inžinerinės praktikos atitiktų pripažintas gerąsias praktikas (*angl. industry best practices*), atsižvelgdamas į kibernetinio saugumo ir duomenų privatumo principus, įskaitant atsparumo (*angl. resilience*) reikalavimus.
2. Tiekėjas užtikrina, kad Rezultatas būtų projektuojamas, kuriamas ir eksploatuojamas laikantis taikytinų saugios inžinerijos praktikų bei teisės aktų, reguliacinių ir sutartinių reikalavimų, siekiant užtikrinti jo saugumą ir atsparumą.
3. Tiekėjas įgyvendina tinkamas technines ir organizacines saugumo priemones, skirtas apsaugoti Rezultatą nuo neautorizuoto kodo naudojimo

7.10 Technologijų kūrimas ir įsigijimas

[ISO/IEC 27001:2022 A.8.25, A.8.26]

1. Tiekėjas užtikrina, kad jo sukurtas individualus programinis kodas (*angl. custom code*) būtų peržiūrimas kolegų (*angl. peer review*), tinkamai dokumentuojamas ir testuojamas, siekiant nustatyti saugumo pažeidžiamumus.
2. Tiekėjas užtikrina, kad bet koks trečiųjų šalių kūrimas ir (ar) įsigyjami sprendimai, darantys ar galintys daryti įtaką Rezultatui, atitiktų arba viršytų Pirkėjo nustatytus saugumo ir kokybės reikalavimus.

7.11 Techninė priežiūra

[ISO/IEC 27001:2022 A.8.32]

1. Jei Šalys nesusitaria kitaip, Tiekėjo Rezultato techninė priežiūra turi būti vykdoma laikantis Pirkėjo pakeitimų valdymo (angl. *change management*) ir valdysenos (*angl. governance*) procedūrų.
2. Tiekėjas užtikrina, kad kiekvienas Tiekėjo talpinamas Rezultatas būtų įtrauktas į Tiekėjo administracinius procesus ir taikomas technologijas, skirtas užtikrinti kontroliuojamą ir savalaikę techninę priežiūrą per visą Rezultato gyvavimo ciklą.
3. Tiekėjas palaiko aktualų įgaliotų techninės priežiūros organizacijų ar komandų, atsakingų už Rezultatą, sąrašą ir, Pirkėjui pareikalavus, jį pateikia.

7.12 Pakeitimų valdymas

[ISO/IEC 27001:2022 A.8.32]

1. Tiekėjas bendradarbiauja su Pirkėju, siekdamas užtikrinti saugų ir patikimą Rezultato veikimą, įskaitant tinkamą pakeitimų valdymą.
2. Tiekėjas įgyvendina ir taiko proaktyvų pakeitimų valdymą Tiekėjo talpinamam Rezultatui, vertindamas, autorizuodamas ir stebėdamas techninius pakeitimus, siekdamas išvengti gamybinės (produkcinės) aplinkos sutrikimų ir užtikrinti operatyvų problemų sprendimą.
3. Tiekėjas užtikrina, kad nebūtų atliekami neautorizuoti pakeitimai, pažeidžiantys Pirkėjo taikomą formalų pakeitimų valdymo (angl. *change management*, CM) procesą, taikomą Rezultatui; kad visi pakeitimai būtų tinkamai dokumentuojami; ir kad pakeitimai nesukeltų paslaugų teikimo sutrikimų.
4. Tiekėjas registruoja ir seka visus Rezultate atliekamus pakeitimus, naudodamas centralizuotą pakeitimų valdymo sistemą, skirtą pakeitimų užklausoms (angl. *request for change*, RFC) teikti, peržiūrėti, tvirtinti ir valdyti).
5. Po kiekvieno pakeitimo įgyvendinimo gamybinėje (produkcinėje) aplinkoje Tiekėjas testuoja Rezultato kibernetinio saugumo kontrolės priemones, siekdamas užtikrinti jų tinkamą veikimą.

8 Priedai