Pirkimo dalyviams
(siunčiama CVP IS priemonėmis)

2026-05-19

CVP IS pirkimo numeris	7412742
Pirkimo būdas arba priemonė	Skelbiamos derybos
Pirkimo objekto dalis	-
Pirkimo pavadinimas	34072 Privilegijuotų Prieigų Valdymo (PPV) sprendimo prenumerata, palaikymas ir pradinis parengimas

**toliau bendrai – Pirkimas*

PRAŠYMAS (-Ų) PAAIŠKINTI IR PATIKSLINTI PIRKIMO DOKUMENTUS

UAB „LTG Kompetencijų centras“ (toliau – KC), vadovaudamasi Pirkimo sąlygose nustatytais reikalavimais ir tvarka, išnagrinėjusi CVP IS susirašinėjimo priemonėmis suinteresuoto (-ų) tiekėjo (-ų) pateiktą (-us) prašymą (-us) paaiškinti ir patikslinti Pirkimo dokumentus, teikia atsakymą (-us):

Eil. Nr.	Klausimas/ prašymas*	Atsakymas**
1.	Vadovaudamiesi Pirkimo sąlygomis, teikiame klausimus (prašymus) dėl Techninės specifikacijos reikalavimų paaiškinimo (patikslinimo). **1. Dėl reakcijos laiko SaaS tipo sprendimų atveju** Vadovaujantis Techninės specifikacijos 3.2.1 punkto 10 papunkčiu, tiekėjas gali siūlyti gamintojų sprendimus, diegiamus tiek kliento infrastruktūroje (on-premise), tiek debesijos pagrindu, t. y. SaaS modeliu. Pažymime, kad SaaS modelio atveju: • sprendimo veikimas, incidentų šalinimas ir jų sprendimo terminai yra tiesiogiai valdomi programinės įrangos gamintojo; • tiekėjas / partneris neturi techninės galimybės savarankiškai daryti įtakos incidentų sprendimo terminams ar garantuoti jų laikymosi kitaip, nei tai numatyta gamintojo palaikymo politikoje; • gamintojas, pavyzdžiui „Delinea“, SLA sąlygas apibrėžia savo standartinėje palaikymo politikoje:	Vadovaujantis Techninės specifikacijos 3.2.1 punkto 10 papunkčiu, tiekėjas gali siūlyti gamintojų sprendimus, diegiamus tiek Perkančiosios organizacijos infrastruktūroje (on-premise), tiek debesijos pagrindu, t. y. SaaS (Software as a Service) modeliu. Atsižvelgiant į tai, pažymime, kad SaaS tipo sprendimų atveju sprendimo veikimas, incidentų valdymas, reakcijos laikas ir trūkumų šalinimo terminai yra tiesiogiai nustatomi ir valdomi sprendimo gamintojo, vadovaujantis jo standartine palaikymo ir paslaugų teikimo politika (SLA). Tiekėjas, veikdamas kaip gamintojo partneris ar atstovas, neturi techninių ir organizacinių galimybių savarankiškai daryti įtakos gamintojo nustatytiems reakcijos ir incidentų šalinimo terminams ar juos garantuoti kitaip, nei tai numatyta gamintojo standartinėse SLA sąlygose. Papildomai atkreipiame dėmesį, kad Techninės specifikacijos 3.2.2 punkte nustatyta, jog techninės pagalbos ir konsultacijų teikimas turi būti užtikrinamas pagal gamintojo nustatytą tvarką, kas SaaS modelio atveju reiškia, jog taikomi gamintojo standartiniai, visiems klientams vienodai galiojantys SLA reikalavimai, kurie paprastai

	<table><tr><th>Priority Level & Definitions</th><th>Examples</th><th>Standard Support Response Time</th><th>Premium Support Response Time</th></tr><tr><td>1 – Severe Error Production server(s) or other mission-critical system(s) are down, and no workaround is immediately available.</td><td>· System down · All or a substantial portion of your mission-critical data is at significant risk of loss or corruption.</td><td>2 Business Hours</td><td>1 Hour 24/7</td></tr><tr><td>2 – Major functionality is severely impaired Operations can continue in a restricted fashion, although long-term productivity might be adversely affected. A workaround is required.</td><td>· Major system function is unavailable or degraded · Repeated failures · Error will create intolerable delays if not addressed · Issue has halted deployment of product</td><td>6 Business Hours</td><td>4 Hour 24/7</td></tr><tr><td>3 – Partial, non-critical loss of functionality A problem that involves partial, non-critical loss of use of the software for production or development purposes.</td><td>· Failure in a software component that is non-critical · Impaired operations of some components but use of software is possible</td><td>8 Business Hours</td><td>6 Business Hours</td></tr><tr><td>4 – General usage problem There is no impact on production or other environments</td><td>· General configuration or usage questions · Documentation errors · Cosmetic errors</td><td>24 Business Hours</td><td>12 Business Hours</td></tr><tr><td>5 – Ideas & features</td><td>· Request for new general product functionality</td><td>24 Business Hours</td><td>24 Business Hours</td></tr></table> Taip pat pažymėtina, kad Techninės specifikacijos 3.2.2 punkte nurodyta, jog techninės pagalbos ir konsultacijų teikimas turi būti užtikrintas pagal gamintojo nustatytą tvarką. Atkreipiame dėmesį, kad SaaS tipo sprendimų atveju reakcijos ir trūkumų šalinimo terminai įprastai priklauso nuo gamintojo taikomų standartinių SLA sąlygų, kurios yra vienodai taikomos visiems klientams ir negali būti individualiai keičiamos tiekėjo nuožiūra. Todėl pernelyg trumpas reakcijos laiko reikalavimas gali nepagrįstai riboti tiekėjų galimybes pasiūlyti rinkoje plačiai naudojamus SaaS tipo sprendimus, nors tokie sprendimai iš esmės atitiktų Perkančiosios organizacijos funkcinius ir saugumo poreikius.	nėra individualiai keičiami konkretaus tiekėjo ar kliento pageidavimu. Atsižvelgiant į aukščiau išdėstytas aplinkybes, pažymime, kad Techninės specifikacijos 7.3.2.1 papunktyje nustatytas reakcijos laiko reikalavimas nėra tiesiogiai taikomas SaaS tipo sprendimams tokiu pat mastu, kaip sprendimams, diegiamiems Perkančiosios organizacijos valdomoje infrastruktūroje (on-premise). SaaS modelio atveju reakcijos laikas turi būti vertinamas pagal gamintojo taikomą reakcijos laiką, nustatytą jo standartinėse SLA sąlygose. Todėl, siekiant užtikrinti proporcingus reikalavimus, realistišką sutartinių įsipareigojimų vykdymą ir sąžiningą tiekėjų konkurenciją, laikytina pagrįsta, kad SaaS tipo sprendimų atveju būtų taikomas ne trumpesnis kaip 4 valandų reakcijos laikas, jei toks terminas atitinka gamintojo nustatytas SLA sąlygas. Priešingu atveju, pernelyg trumpas reakcijos laiko reikalavimas galėtų nepagrįstai apriboti galimybę pasiūlyti rinkoje plačiai naudojamus, brandžius ir Perkančiosios organizacijos funkcinius bei saugumo poreikius atitinkančius SaaS tipo sprendimus.

	Siekdami užtikrinti sąžiningą tiekėjų konkurenciją, proporcingus reikalavimus ir realistišką sutartinių įsipareigojimų vykdymą, prašome patikslinti Techninės specifikacijos 7.3.2.1 papunktį ir nustatyti, kad SaaS tipo sprendimų atveju reakcijos laikas būtų ne trumpesnis kaip 4 valandos, arba aiškiai pagrįsti, kodėl trumpesnis reakcijos laikas yra būtinas Perkančiosios organizacijos poreikiams ir kodėl toks poreikis negalėtų būti užtikrinamas taikant 4 valandų reakcijos terminą.	
2.	**2. Dėl gamintojo pagalbos tarnybos naudojimo** Kaip nurodyta aukščiau, debesijos pagrindu teikiamo SaaS modelio sprendimo atveju incidentų ir trūkumų šalinimas yra tiesiogiai valdomas programinės įrangos gamintojo. Tokiu atveju būtent gamintojas užtikrina trūkumų ir techninių problemų registravimą, nagrinėjimą bei šalinimą, naudodamas savo pagalbos tarnybą ir tam skirtas sistemas. Atsižvelgdami į Techninės specifikacijos 3.2.2 punkto nuostatą, kad techninės pagalbos ir konsultacijų teikimas turi būti užtikrintas pagal gamintojo nustatytą tvarką, prašome atitinkamai patikslinti Techninės specifikacijos 7 punktą arba patvirtinti, kad trūkumų ir techninių problemų registravimui, nagrinėjimui bei šalinimui Užsakovas turi naudotis gamintojo pagalbos tarnyba / sistema.	Vadovaujantis Techninės specifikacijos 3.2.2 punkto nuostata, nustatančia, kad techninės pagalbos ir konsultacijų teikimas turi būti užtikrintas pagal gamintojo nustatytą tvarką, paaiškiname, kad debesijos pagrindu teikiamo SaaS (Software as a Service) modelio sprendimo atveju incidentų ir trūkumų valdymas yra tiesiogiai organizuojamas ir vykdomas sprendimo gamintojo. SaaS modelio atveju sprendimo veikimas, infrastruktūra, programinės įrangos palaikymas, atnaujinimai bei incidentų ir techninių problemų šalinimas yra centralizuotai valdomi gamintojo, kuris užtikrina: • incidentų ir trūkumų registravimą, • jų nagrinėjimą, • techninių problemų šalinimą, naudodamas savo pagalbos tarnybą ir tam skirtas sistemas, vadovaudamasis gamintojo nustatytais procesais ir paslaugų teikimo tvarka. Atsižvelgiant į tai, Techninės specifikacijos 7 punkto reikalavimai nėra tiesiogiai taikomi SaaS sprendimui analogiškai kaip sprendimams, diegiamiems Užsakovo infrastruktūroje (on-premise). SaaS modelio atveju laikoma, kad reikalavimas dėl techninės pagalbos įgyvendinamas per gamintojo pagalbos tarnybą, kuri yra integrali SaaS paslaugos dalis. Todėl patvirtiname, kad trūkumų ir techninių problemų registravimui, nagrinėjimui bei šalinimui SaaS sprendimo atveju Užsakovas naudojasi gamintojo pagalbos tarnyba / sistema, veikiančia gamintojo nustatyta tvarka, kaip tai numatyta Techninės specifikacijos 3.2.2 punkte.
3.	**3. Dėl infrastruktūros reikalavimo taikymo SaaS paslaugai** Prašome patikslinti, ar Techninės specifikacijos priedo Nr. 2 „NFR — nefunkciniai reikalavimai informacijos saugai ir BDAR“ 15 punkto	Vadovaujantis Techninės specifikacijos 3.2.1 punkto 10 papunkčiu, tiekėjas gali siūlyti gamintojų sprendimus, diegiamus tiek

	reikalavimas „Infrastruktūra“ taikomas tuo atveju, jeigu siūloma SaaS paslauga. Pažymime, kad SaaS modelio atveju sprendimo infrastruktūrą valdo gamintojas, todėl tik gamintojas disponuoja detalia informacija apie tai, kokioje infrastruktūroje veikia jo SaaS sistema / platforma.	Perkančiosios organizacijos infrastruktūroje (on-premise), tiek debesijos pagrindu, t. y. SaaS (Software as a Service) modeliu. Atsižvelgiant į tai, pažymime, kad Techninės specifikacijos priedo Nr. 2 „NFR — nefunkciniai reikalavimai informacijos saugai ir BDAR“ 15 punkte nustatytas reikalavimas „Infrastruktūra“ nėra tiesiogiai taikomas tuo atveju, kai siūlomas sprendimas teikiamas SaaS modeliu. SaaS modelio atveju sprendimo infrastruktūrą valdo ir administruoja sprendimo gamintojas / paslaugos teikėjas, todėl tiekėjas neturi galimybės ir prievolės detalizuoti infrastruktūros, analogiškai kaip tai būtų taikoma sprendimams, diegiamiems Perkančiosios organizacijos valdomoje infrastruktūroje (on-premise). Tokiu atveju infrastruktūros aspektai vertinami ne kaip techniniai diegimo reikalavimai, o per paslaugos teikėjo taikomas informacijos saugos, atitikties (pvz., sertifikatai, saugumo politikos), BDAR ir kitas sutartines bei organizacines priemones.
4.	Siekdami tinkamai suprasti techninės specifikacijos reikalavimus ir parengti kuo konkurencingesnį bei perkančiosios organizacijos poreikius atitinkantį pasiūlymą, prašome paaiškinti / patikslinti žemiau nurodytus techninės specifikacijos punktus. 3.2.1. 10. b. „PAM sprendimo nuotoliniu būdu valdomoje įrangoje ar sistemose neturi būti diegiami agentai ar kita su sprendimu susijusi programinė įranga“ ir 3.2.1. 18.b. „Privilegijuota RDP ir SSH sesija turi būti įrašoma net ir kuomet jungiamasi tiesiogiai į PAM valdomą sistemą (ne per įgaliotąjį serverį (angl. proxy/jumphost)“ Prašome paaiškinti, kokiu būdu tikimasi realizuoti privilegijuotų sesijų įrašymą tiesioginių prisijungimų atveju, kai PAM sprendimo nuotoliniu būdu valdomoje įrangoje ar sistemose negali būti diegiami agentai ar kita su sprendimu susijusi programinė įranga. Taip pat prašome patikslinti, ar bus laikoma atitinkančiu sprendimu, kuris pilną privilegijuotų sesijų kontrolę, auditavimą ir įrašymą realizuoja naudojant saugią įgaliotojo serverio (proxy/jumphost) architektūrą.	Vadovaujantis Techninės specifikacijos 3.2.1 punkto 10 papunkčio b papunkčiu, numatyta, kad PAM sprendimo nuotoliniu būdu valdomoje įrangoje ar sistemose neturi būti diegiami agentai ar kita su sprendimu susijusi programinė įranga. Tuo pačiu Techninės specifikacijos 3.2.1 punkto 18 papunkčio b papunktyje nustatyta, jog privilegijuota RDP ir SSH sesija turi būti įrašoma net ir tuo atveju, kai jungiamasi tiesiogiai į PAM valdomą sistemą (ne per įgaliotąjį serverį (angl. proxy / jumphost)). Paaiškiname, kad agentų nediegimo reikalavimas nereiškia, jog PAM sprendimas privalo techniškai įrašyti privilegijuotas sesijas visiškai apeinant bet kokį tarpinį komponentą tinklo lygmeniu. Praktikoje, agentų nenaudojant, pilnas privilegijuotų sesijų valdymas, auditas ir įrašymas yra realizuojamas taikant agentless (be agentų) PAM architektūrą, kuri grindžiama: • centralizuotu prisijungimų valdymu, • autentifikacijos ir autorizacijos kontrole prieš sesijos inicijavimą, • sesijų srauto nukreipimu per centralų PAM komponentą (proxy / jumphost arba jam ekvivalentišką architektūrinį

		sprendimą), ne diegiant jokios papildomos programinės įrangos galutinėse valdomose sistemose. Atsižvelgiant į tai, reikalavimas įrašyti privilegijuotas RDP ir SSH sesijas jungiantis „tiesiogiai“ turi būti suprantamas kaip jungimasis be agentų diegimo valdomoje sistemoje, o ne kaip tiesioginis prisijungimas, visiškai aplenkiant PAM sprendimo kontrolės ir audito mechanizmus. Be agentų diegimo galutinėje sistemoje, technologiškai neįmanoma užtikrinti pilno sesijų įrašymo, komandų lygmens audito ir realaus laiko kontrolės, jei sesija nebūtų valdoma per specializuotą PAM komponentą. Todėl patikslinam, kad sprendimas, kuris pilną privilegijuotų sesijų kontrolę, auditavimą ir įrašymą realizuoja naudojant saugią įgaliotojo serverio (proxy / jumphost) arba jam funkciškai lygiavertę agentless architektūrą, bus laikomas atitinkančiu Techninės specifikacijos reikalavimus. Esminis kriterijus yra tai, kad: • valdomose sistemose nėra diegiami agentai ar kita papildoma programinė įranga, • visos privilegijuotos sesijos yra centralizuotai valdomos, registruojamos ir įrašomos PAM sprendimo priemonėmis, • užtikrinamas pilnas saugumo, audito ir atsekamumo funkcionalumas.
5.	3.2.1. 13. b. „Sprendimas turi turėti integracijas su trečiųjų šalių programine ir aparatine įranga ir turi pateikti biometrinį autentifikavimą (pagal išmaniojo telefono veido ID, pirštų atspaudų nuskaitymus), kad būtų galima autentifikuoti trečiųjų šalių pardavėjus (prieš užmezgant ryšį nereikia įvesti prieigos duomenų, kaip vartotojo slaptažodžio).“ Prašome patikslinti, ar bus laikoma atitinkančiu sprendimu, kuris integruojasi su trečiųjų šalių tapatybės valdymo ir MFA sprendimais (pvz. SAML / SSO / Identity Provider sprendimais), suteikiančiais biometrinio autentifikavimo funkcionalumą (Face ID, pirštų atspaudų autentifikavimą) bei „passwordless“ autentifikavimo scenarijus, kai prieš užmezgant ryšį nereikia įvesti vartotojo slaptažodžio.	Vadovaujantis Techninės specifikacijos 3.2.1 punkto 13 papunkčio b papunkčiu, reikalaujama, kad sprendimas turėtų integracijas su trečiųjų šalių programine ir aparatine įranga bei sudarytų galimybę taikyti biometrinį autentifikavimą (pvz., veido atpažinimo ar pirštų atspaudų pagrindu), užtikrinant „passwordless“ autentifikavimo scenarijus, kai prieš užmezgant ryšį nereikia įvesti vartotojo slaptažodžio. Paaiškiname, kad šis reikalavimas nėra skirtas apriboti sprendimo architektūrinio pasirinkimo ar reikalauti, jog biometrinio autentifikavimo funkcionalumas būtų realizuotas tik paties PAM sprendimo priemonėmis. Praktikoje biometrinis autentifikavimas ir „passwordless“ prisijungimo scenarijai yra realizuojami naudojant centralizuotus tapatybės ir prieigos valdymo (Identity and Access Management, IAM) bei daugiafaktorės autentifikacijos (MFA)

		sprendimus, kurie integruojami su PAM sprendimu per standartinius autentifikavimo ir federacijos mechanizmus. Atsižvelgiant į tai, sprendimas, kuris integruojasi su trečiųjų šalių tapatybės valdymo, SSO ar Identity Provider (pvz., per SAML, OpenID Connect ir panašius protokolus) sprendimais, užtikrinančiais: biometrinį autentifikavimą (pvz., „Face ID“, pirštų atspaudų autentifikavimą per išmanųjį telefoną ar kitą patikimą įrenginį), „passwordless“ autentifikavimo scenarijus, naudotojo autentifikavimą prieš užmezgant ryšį nesinaudojant slaptažodžiu, bus laikomas atitinkančiu Techninės specifikacijos 3.2.1 punkto 13 papunkčio b papunkčio reikalavimus, su sąlyga, kad: autentifikavimas yra techniškai integruotas į PAM sprendimo prieigos suteikimo procesą, užtikrinamas patikimas naudotojo tapatybės patvirtinimas prieš suteikiant privilegijuotą prieigą, išlaikomas pilnas audituojamumas ir atsekamumas pagal sprendimo saugumo modelį. Tokiu būdu laikytina, kad biometrinio autentifikavimo ir „passwordless“ funkcionalumo realizavimas per integruotus trečiųjų šalių IAM / MFA sprendimus atitinka Techninės specifikacijos reikalavimų esmę ir tikslą – padidinti trečiųjų šalių pardavėjų prieigų saugumą, sumažinti slaptažodžių naudojimą ir užtikrinti modernius autentifikavimo scenarijus.
6.	3.2.1. 9. a. „Siūlomo PAM administravimas turi turėti aiškiai išskirtas teises, kurios leistų realizuoti „keturių akių“ administravimo principą: vienas naudotojas suteikia super-administratoriaus teises, kitas tomis teisėmis pasinaudoja. Teikėjas jomis negali pasinaudoti, gavėjas negali jų sau suteikti.“ Prašome patikslinti, ar bus laikoma atitinkančiu sprendimu, kuris „keturių akių“ principą realizuoja naudojant teisių atskyrimo, daugiasluoksnio patvirtinimo (multi-level approval) ir privilegijuotų	Vadovaujantis Techninės specifikacijos 3.2.1 punkto 9 papunkčio a papunkčiu, reikalaujama, kad siūlomo PAM sprendimo administravimas turėtų aiškiai išskirtas teises, leidžiančias įgyvendinti „keturių akių“ administravimo principą, t. y. kad: • vienas įgaliotas naudotojas galėtų suteikti (inicijuoti) super-administratoriaus ar kitas privilegijuotas teises, • kitas, atskiras ir įgaliotas naudotojas galėtų tomis teisėmis pasinaudoti,

	veiksmų kontrolės mechanizmus, užtikrinančius, kad naudotojas negalėtų savarankiškai suteikti sau privilegijuotų teisių bei jomis pasinaudoti be kito įgalioto asmens patvirtinimo.	• tas pats naudotojas negalėtų vienu metu tiek suteikti, tiek pasinaudoti tomis pačiomis privilegijomis. Paaiškiname, kad šis reikalavimas nėra apribotas tik siauru techniniu modeliu, tačiau yra skirtas užtikrinti esminį „keturių akių“ principo tikslą – privilegijų eskalacijos rizikos mažinimą, funkcijų atskyrimą ir administracinių veiksmų kontrolę. Atsižvelgiant į tai, sprendimas, kuris „keturių akių“ principą realizuoja naudojant teisių atskyrimo, daugiasluoksnio patvirtinimo (angl. *multi-level approval*) ir privilegijuotų veiksmų kontrolės mechanizmus, bus laikomas atitinkančiu Techninės specifikacijos 3.2.1 punkto 9 papunkčio a papunkčio reikalavimus, jeigu užtikrinama, kad: • naudotojas negali savarankiškai suteikti sau privilegijuotų teisių, • privilegijuotų teisių suteikimas ar aktyvavimas reikalauja kito įgalioto asmens patvirtinimo, • tas pats naudotojas negali tiek inicijuoti, tiek patvirtinti bei panaudoti privilegijuotų teisių be nepriklausomos kito naudotojo kontrolės, • visi tokie veiksmai yra registruojami, audituojami ir atsekami. Tokiu būdu laikytina, kad „keturių akių“ principas gali būti įgyvendinamas ne tik tiesioginiu administratorių teisių suteikimo modeliu, bet ir naudojant modernius PAM sprendimams būdingus patvirtinimo, delegavimo ir privilegijuotų veiksmų valdymo mechanizmus, jei jie funkcionaliai užtikrina Techninės specifikacijos reikalavimo esmę.
7.	3.2.1. 18. d. „Turi leisti atlikti paiešką vaizdo įraše pagal tekstą iš fiksuojamų klavišų paspaudimų.“ Prašome patikslinti, ar bus laikoma atitinkančiu sprendimu, kuris privilegijuotų sesijų paiešką ir auditavimą realizuoja naudojant komandų analizės, sesijų metaduomenų indeksavimo, komandų rekonstrukcijos ar kitus lygiaverčius sesijų stebėsenos mechanizmus, užtikrinančius privilegijuotų veiksmų atsekamumą ir paiešką sesijų įrašuose.	Vadovaujantis Techninės specifikacijos 3.2.1 punkto 18 papunkčio d papunkčiu, reikalaujama, kad PAM sprendimas sudarytų galimybę atlikti paiešką sesijų vaizdo įrašuose pagal tekstą iš fiksuojamų klavišų paspaudimų, siekiant užtikrinti privilegijuotų veiksmų atsekamumą ir efektyvų auditą. Paaiškiname, kad šio reikalavimo esminis tikslas yra ne konkretaus techninio realizavimo būdo įtvirtinimas, o galimybė efektyviai identifikuoti, analizuoti ir audituoti privilegijuotus naudotojų

		veiksmus sesijų įrašuose, įskaitant galimybę atlikti tikslingą paiešką pagal vykdytas komandas, veiksmus ar sesijos turinį. Atsižvelgiant į tai, pažymime, kad sprendimas, kuris privilegijuotų sesijų paiešką ir auditavimą realizuoja naudodamas lygiaverčius techninius mechanizmus, tokius kaip: • komandų analizė ir rekonstrukcija (angl. *command-level auditing*), • sesijų metaduomenų indeksavimas, • komandų žurnalų (command logs) koreliavimas su sesijų įrašais, • ar kiti funkciškai lygiaverčiai sesijų stebėsenos ir analizės metodai, bus laikomas atitinkančiu Techninės specifikacijos 3.2.1 punkto 18 papunkčio d papunkčio reikalavimus, jeigu: • užtikrinamas privilegijuotų veiksmų atsekamumas, • sudaroma galimybė efektyviai vykdyti paiešką sesijų įrašuose pagal vykdytas komandas ar veiksmus, • išlaikomas pilnas audito, kontrolės ir tyrimo funkcionalumas, nepriklausomai nuo to, ar paieška realizuojama tiesiogiai vaizdo įraše, ar per su vaizdo įrašu susietus struktūrizuotus duomenis. Tokiu būdu laikytina, kad reikalavimas yra įgyvendintas, jei sprendimas funkciškai leidžia identifikuoti ir analizuoti konkrečius privilegijuotus veiksmus sesijų įrašuose, net ir naudojant alternatyvius ar pažangesnius techninius sprendimus, atitinkančius šio reikalavimo esmę ir tikslą.

*

Suinteresuoto (-ų) tiekėjo (-ų) prašymo (-ų) paaiškinti/ patikslinti Pirkimo dokumentus tekstas neredaguotas.
*** Paaiškinimas/ patikslinimas ir jo nuostatos turi viršenybę prieš ankstesnes Pirkimo dokumentuose išdėstytas nuostatas.*