

ISO/IEC 27018:2025, informacijos saugumas, kibernetinis saugumas ir privatumo apsauga: asmens duomenų (PII) apsaugos viešuosiuose debesyse, veikiančiuose kaip PII tvarkytojai, gairės (3 leidimas, 2025-08)

PII apsauga viešajame debesyje

36 reikalavimai. Šiam standartui nėra akredituoto sertifikato. Redakcija 07/2026.

ISO/IEC 27018 nėra vadybos sistemos standartas, o gairės su išplėstomis valdymo priemonėmis, papildančiomis ISO/IEC 27002:2022. Atskiro akredituoto sertifikato pagal ISO/IEC 27018 nėra. Valdymo priemonės įtraukiamos į ISO/IEC 27001 sistemos pritaikomumo pareiškimą, o sertifikatas tuomet išduodamas pagal ISO/IEC 27001 su nuoroda į ISO/IEC 27018. Standartas skirtas viešosios debesijos paslaugos teikėjui, kuris tvarko asmens duomenis savo debesijos paslaugos klientų pavedimu. Organizacija, kuri debesijos paslaugas tik naudoja, šio vaidmens neprisiima, todėl reikalavimus prasminga vertinti savo teikėjų, o ne savo pačios atžvilgiu. Leanshift atveju šis kontrolinis sąrašas pirmiausia yra teikėjų vertinimo tinklėlis. Kiekvieną punktą galima pateikti teikėjui kaip klausimą ir įtvirtinti duomenų tvarkymo sutartyje pagal GDPR 28 straipsnį. Tokio vertinimo rezultatas yra vidinis atitikties įrašas arba teikėjo vertinimo profilis, o ne sertifikatas. Dėl numeracijos: skyriai nuo A.2 iki A.12 atitinka standarto A priede pateiktus privatumo principus, o punktai su tokiais numeriais kaip A.11.6 yra ten išvardytos papildomos valdymo priemonės. Punktai su numeriais kaip 8.10 arba 5.34 nurodo ISO/IEC 27002:2022 valdymo priemones, kurias standartas sukonkretina debesijai. Punktai su prierašu (Grundsatz), reiškiančiu principą, kyla iš paties skyriaus principo tais atvejais, kai A priede atskiros papildomos valdymo priemonės nėra.

Įmonė	Data	Pildė
-------	------	-------

A.2 Sutikimas ir pasirinkimas2

A.2.1Debesijos paslaugos teikėjas padeda debesijos paslaugos klientui įgyvendinti duomenų subjektų teises, tokias kaip susipažinimas, ištaisymas, ištrynimasis ir prieštaravimas. Atsakomybės ir terminai yra nustatyti sutartyje.

Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra duomenų tvarkymo sutartis pagal GDPR 28 straipsnį su nuostata dėl pagalbos įgyvendinant duomenų subjektų teises, kartu su techninėmis priemonėmis pačioje paslaugoje: eksporto, taisymo ir trynimo funkcijomis arba dokumentuota palaikymo procedūra su atsako terminu. Klausimas teikėjui: kokią funkciją ar procesą siūlote, kad prašymą susipažinti ar ištrinti galėtume įvykdyti per vieną mėnesį?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.2 (Grundsatz)Debesijos paslaugos klientų asmens duomenys tvarkomi tik pagal dokumentuotus kliento nurodymus. Duomenų subjektų sutikimo gavimas lieka kliento kaip duomenų valdytojo užduotis, ir teikėjas šiuo klausimu savo iniciatyva neveikia.

Iš ko tai galima atpažinti: Įrodymas yra nurodymų nuostata duomenų tvarkymo sutartyje ir įrodymas, kad teikėjas duomenų nenaudoja antriniiais savo tikslais, pavyzdžiui paslaugos privatumo pranešimas ir produkto dokumentacija. Klausimas teikėjui: ar mūsų klientų duomenis kokių nors būdu tvarkote ne pagal mūsų nurodymus, pavyzdžiui produkto tobulinimui ar modelių mokymui?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.3 Tikslas teisėtumas ir apibrėžimas2

A.3.1Tikslas, kuriuo teikėjas tvarko asmens duomenis, apsiriboja sutartos paslaugos teikimu ir yra įvardytas sutartyje. Tvarkymo savo paties tikslais teikėjas nevykdo.

Dokumentas

Iš ko tai galima atpažinti: Įrodymas yra duomenų tvarkymo sutartis, kurioje nurodytas tvarkymo dalykas, pobūdis, tikslas ir trukmė bei duomenų subjektų kategorijos pagal GDPR 28 straipsnio 3 dalį. Klausimas teikėjui: prašome pateikti sutarties priedą, kuris išsamiai aprašo tvarkymo tikslą. Mažoje įmonėje pakanka teikėjo standartinio duomenų tvarkymo priedo, jeigu jame yra ši informacija.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.3.2

Teikėjui patikėti asmens duomenys be išankstinio aiškaus sutikimo nenaudojami reklamai, rinkodarai ar kitiems komerciniams teikėjo tikslams. Paslaugos teikimas nuo tokio sutikimo nepriklauso.

Iš ko tai galima atpažinti: Įrodymas yra aiški sutarties nuostata, kuri atmeta komercinį antrinį naudojimą, kartu su paslaugos teikimo sąlygomis. Klausimas tiekėjui: raštu patvirtinkite, kad klientų duomenys nenaudojami reklamai, profiliavimui ar dirbtinio intelekto modelių mokymui. Jei tokio įsipareigojimo nėra, paslauga asmens duomenims netinka.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.4 Rinkimo ribojimas

1

A.4 (Grunda

Be duomenų, kuriuos į paslaugą įkelia klientas, teikėjas savo tikslais nerenka jokių kitų asmens duomenų, tokių kaip telemetrija, naudojimo profiliai ar turinio analizė. Renkami veiklos duomenys ir metaduomenys yra įvardyti ir pagrįsti.

Iš ko tai galima atpažinti: Įrodymas yra sąrašas duomenų, kuriuos paslauga fiksuoja šalia turinio duomenų (prieigos žurnalai, telemetrija, diagnostikos duomenys), su tikslu ir saugojimo terminu, ir nustatymo, kuriuo išjungiami pasirenkama telemetrija, ekrano nuotrauka. Klausimas tiekėjui: kokius papildomus naudojimo, telemetrijos ir diagnostikos duomenis renkate, kam juos naudojate ir ar galime rinkimą išjungti?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.5 Duomenų kiekio mažinimas

2

A.5.1

Laikinieji failai, sukuriami tvarkant asmens duomenis, tokie kaip laikinoji saugykla, podėliai ar atstatymo žurnalai, saugiai ištrinami per nustatytą laikotarpį.

Iš ko tai galima atpažinti: Įrodymas yra eksploatavimo arba trynimo procedūra su nurodytu laikinųjų duomenų saugojimo terminu, paremta sistemos konfigūracija, pavyzdžiui podėlio TTL arba suplanuota valymo užduotis su jos vykdymo žurnalu. Klausimas tiekėjui: po kokio laikotarpio ištrinami podėliai, laikinieji failai ir tarpinės būsenos ir kaip tai stebima?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

8.11

Visur, kur eksploatavimui, testavimui ar palaikymui gyvi duomenys nereikalingi, asmens duomenys yra maskuojami, pseudonimizuojami arba anonimizuojami. Tvarkomų duomenų apimtis lieka apribota tuo, ko paslaugai iš tikrųjų reikia.

Iš ko tai galima atpažinti: Įrodymas yra taisyklė, nustatanti, kurios aplinkos gali matyti gyvus duomenis, bei testavimo ir kūrimo sistemose naudojamo maskavimo ekrano nuotraukos arba scenarijai. Klausimas tiekėjui: ar palaikymo ir kūrimo komandos dirba su gamybos duomenimis ir jeigu taip, su kokiomis apsaugos priemonėmis? Mažoje įmonėje pakanka taisyklės, kad testavimo sistemos veikia tik su sugeneruotais pavyzdiniais duomenimis.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.6 Naudojimo, saugojimo ir atskleidimo ribojimas

3

A.6.1

Gavęs teisiškai saistantį reikalavimą atskleisti asmens duomenis, pavyzdžiui iš valdžios institucijos, teikėjas iš anksto informuoja debesijos paslaugos klientą tiek, kiek leidžia teisės aktai.

Iš ko tai galima atpažinti: Įrodymas yra sutartinė informavimo nuostata ir vidinis institucijų užklausų procesas su įvardytu atsakingu asmeniu. Klausimas tiekėjui: ar informuojate mus prieš perduodami duomenis ir ar skelbiate skaidrumo ataskaitą apie institucijų užklausas? Naujausia skaidrumo ataskaita yra stiprus įrodymas.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.6.2 Atskleidamas asmens duomenis tretiesiems asmenims, teikėjas šį įvykį registruoja taip, kad jį būtų galima atsekti: kas duomenis gavo, kada tai įvyko, kokie duomenys buvo perduoti ir kokių pagrindų atskleidimas remiasi.

[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra atskleidimų registras arba užklausų istorija su šiais laukais, net jeigu įrašų jame nėra. Tuščias, bet palaikomas registras yra priimtinas ir mažoje įmonėje yra praktiškiausias kelias. Klausimas tiekėjui: ar tvarkote duomenų atskleidimų registrą ir ar galite gauti iš jo išrašus?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

8.10 Asmens duomenys ištrinami pasibaigus sutartam saugojimo terminui arba nutrūkus sutarčiai, įskaitant atsarginėse kopijose laikomus egzempliorius po jų rotacijos ciklo.

Iš ko tai galima atpažinti: Įrodymas yra trynimo koncepcija su saugojimo terminais pagal duomenų kategorijas, atsarginių kopijų saugojimo terminas ir trynimo žurnalas arba trynimo patvirtinimas. Klausimas tiekėjui: kiek ilgai mūsų duomenys po sutarties nutraukimo lieka atsarginėse kopijose ir ar gauname raštišką jų ištrynimo patvirtinimą?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.7 Tikslumas ir kokybė

2

A.7 (Grunda) Teikėjas savo iniciatyva nekeičia jam patikėtų asmens duomenų. Pataisymai ir atnaujinimai atliekami tik pagal debesijos paslaugos kliento nurodymą arba per funkcijas, kurias klientas valdo pats.

Iš ko tai galima atpažinti: Įrodymas yra paslaugos redagavimo funkcijos kartu su jų pakeitimų istorija ir nurodymų nuostata duomenų tvarkymo sutartyje. Klausimas tiekėjui: ar galime įrašus taisyti patys ir ar kiekvienas pakeitimas registruojamas taip, kad jį būtų galima atsekti?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

8.13 Asmens duomenų vientisumas yra apsaugotas saugojimo, perdavimo ir atkūrimo metu. Atsarginės kopijos yra sukurtos, o jų atkuriamumas yra patikrintas.

Iš ko tai galima atpažinti: Įrodymas yra atsarginių kopijų konfigūracija, kontrolinių sumų arba vientisumo mechanizmai ir bent viena dokumentuota atkūrimo patikra per metus su data ir rezultatu. Klausimas tiekėjui: kaip dažnai testuojate atkūrimą ir kokį atkūrimo laiką įsipareigojate užtikrinti paslaugos lygio susitarime?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.8 Atvirumas, skaidrumas ir informavimas

2

A.8.1 Pasitelktų duomenų tvarkytojų, kurie tvarko asmens duomenis, naudojimas atskleidžiamas prieš sudarant sutartį. Apie sąrašo pakeitimus klientas informuojamas laiku, kad galėtų prieštarauti arba nutraukti sutartį.

[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra naujausias pasitelktų duomenų tvarkytojų sąrašas, paskelbtas arba pateiktas pagal sutartį, su pavadinimu, šalimi ir tvarkymo tikslu, ir informavimo taisyklė pagal GDPR 28 straipsnio 2 dalį. Klausimas tiekėjui: kur rasti pasitelktų duomenų tvarkytojų sąrašą, prieš kiek laiko pranešate apie pakeitimus ir kaip galime prieštarauti?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.8 (Grunda) Prieš sudarant sutartį teikėjas pateikia suprantamą informaciją apie tai, kaip tvarkomi asmens duomenys, kokios apsaugos priemonės yra sukurtos ir kokiose jurisdikcijose vyksta tvarkymas.

Iš ko tai galima atpažinti: Įrodymas yra privatumo pranešimas, saugumo aprašas, pasitikėjimo centro puslapis ir duomenų tvarkymo sutartis su techninėmis ir organizacinėmis priemonėmis kaip priedu. Klausimas tiekėjui: prašome pateikti naujausią techninių ir organizacinių priemonių sąrašą kaip sutarties priedą, o ne tik rinkodarinę medžiagą.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.9 Asmens dalyvavimas ir prieiga

2

A.9 (Grunda) Paslauga suteikia debesijos paslaugos klientui technines priemones savarankiškai įvykdyti duomenų subjektų prašymus susipažinti, ištaisyti ir ištrinti, pavyzdžiui per eksporto, paieškos ir trynimo funkcijas.

Iš ko tai galima atpažinti: Įrodymas yra eksporto ir trynimo funkcijų produkto dokumentacija, paremta vidiniu bandymu: vienas prašymas susipažinti apdorojamas nuo pradžios iki galo ir užrašoma, kiek tai trunka. Klausimas tiekėjui: ar galime rasti, eksportuoti ir ištrinti visus vieno asmens duomenis be teikėjo pagalbos?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

5.34 Kai klientas duomenų subjekto prašymo negali įvykdyti pats, teikėjas padeda per sutartą laikotarpį. Prašymai, kuriuos duomenų subjektai siunčia tiesiogiai teikėjui, perduodami klientui, o teikėjas į juos pats neatsako.

Iš ko tai galima atpažinti: Įrodymas yra atitinkama duomenų tvarkymo sutarties nuostata su konkrečiu atsako terminu ir palaikymo užklausų istorija kaip tikras pavyzdys. Klausimas tiekėjui: kokią pagalbos įgyvendinant duomenų subjektų teises terminą įsipareigojate ir kiek tai kainuoja?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.10 Atskaitomybė

4

A.10.1 Apie asmens duomenų saugumo pažeidimus debesijos paslaugos klientui pranešama nepagrįstai nedelsiant, nurodant mastą, paveiktus duomenis, priežastį ir taikytas priemones. Informavimo procesas su atsakomybėmis ir terminais yra nustatytas.[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra reagavimo į incidentus planas su eskalavimo grandine, sutartinis informavimo terminas (praktikoje tinka nuo 24 iki 48 valandų, kad klientas dar spėtų laikytis 72 valandų termino pagal GDPR 33 straipsnį) ir įrašai apie buvusius incidentus arba apie pratybas. Klausimas tiekėjui: per kokį laikotarpį pranešate apie incidentą, koku kanalu ir kokią informaciją kartu pateikiate?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.10.2 Saugumo politikos, eksploatavimo procedūros ir su jomis susiję įrašai saugomi nustatytą laikotarpį, kad tvarkymą būtų galima atkurti vėliau.[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra saugojimo taisyklė su politikų versijų istorija, pavyzdžiui dokumentų registras arba versijų valdymo sistema su patvirtinimo data. Klausimas tiekėjui: kiek ilgai saugote politikų versijas ir su jomis susijusius įrašus ir ar audito atveju gauname prie jų prieigą?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.10.3 Asmens duomenų grąžinimui, perdavimui ir sunaikinimui pasibaigus sutarčiai yra nustatyta tvarka, kurioje įvardyti formatai, terminai ir elgesys su kopijomis.[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra duomenų tvarkymo sutarties pasitraukimo nuostata ir trynimo patvirtinimas pasibaigus sutarčiai. Klausimas tiekėjui: koku formatu ir per kokį laikotarpį atgauname savo duomenis, kada sunaikinamos visos kopijos ir ar gauname raštišką patvirtinimą?

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

5.35 Apsaugos priemonių rezultatyvumas nepriklausomai peržiūrimas reguliariais intervalais, pavyzdžiui per vidaus auditus, įsilaužimo testus ar trečiųjų šalių užtikrinimo ataskaitas. Rezultatai tinkama forma pateikiami debesijos paslaugos klientui.

Iš ko tai galima atpažinti: Įrodymas yra ISO/IEC 27001 sertifikatas su pritaikomumo pareiškimu, kuriame yra ISO/IEC 27018 valdymo priemonės, arba SOC 2 ataskaita kartu su naujausiomis įsilaužimo testų santraukomis. Klausimas tiekėjui: prašome pateikti sertifikatą, jo taikymo sritį ir patvirtinimą, kad ISO/IEC 27018 atspindi pritaikomumo pareiškimą. Verta patikrinti, ar taikymo sritis iš tikrųjų apima naudojamą paslaugą.

Atviras	Vykdomas	Įvykdytas	Netaikomas
---------	----------	-----------	------------

Įrodymas / pagrindimas

A.11 Informacijos saugumas		13				
A.11.1	Kiekvienas asmuo, turintis prieigą prie asmens duomenų, yra įpareigotas laikytis konfidencialumo, nesvarbu, ar dirba pagal darbo sutartį, ar yra pasitelktas iš išorės.	Dokumentas				
Iš ko tai galima atpažinti: Įrodymas yra pasirašytos konfidencialumo sutartys arba pasižadėjimai, galiojantys ir pasibaigus bendradarbiavimui. Klausimas tiekėjui: ar visi darbuotojai ir paslaugų teikėjai, turintys prieigą prie duomenų, raštu įpareigoti laikytis konfidencialumo?						
<table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table>			Atviras	Vykdomas	Įvykdytas	Netaikomas
Atviras	Vykdomas	Įvykdytas	Netaikomas			
Įrodymas / pagrindimas						
A.11.2	Spaudiniai ir kitos popierinės kopijos su asmens duomenimis kuriami tik tada, kai tai būtina reikalinga. Leistina apimtis yra reglamentuota taisyklėje.					
Iš ko tai galima atpažinti: Įrodymas yra elgesio su spaudiniais taisyklė, kuri duomenų centruose paprastai yra visiškas spausdinimo draudimas zonose su klientų duomenimis. Klausimas tiekėjui: ar klientų duomenys apskritai spausdinami veikloje ir jeigu taip, kokiomis sąlygomis?						
<table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table>			Atviras	Vykdomas	Įvykdytas	Netaikomas
Atviras	Vykdomas	Įvykdytas	Netaikomas			
Įrodymas / pagrindimas						
A.11.3	Atkūrimai iš atsarginių kopijų yra iš anksto autorizuoti ir registruojami, nurodant asmenį, kuris atkūrimą inicijavo, ir paveiktus duomenis.	Dokumentas				
Iš ko tai galima atpažinti: Įrodymas yra atkūrimo žurnalas su laiko žyma, iniciatoriumi ir apimtimi, kurį atsarginių kopijų įrankis paprastai sukuria automatiškai. Klausimas tiekėjui: ar registruojate kiekvieną atkūrimą ir ar audito atveju galime šiuos žurnalus peržiūrėti?						
<table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table>			Atviras	Vykdomas	Įvykdytas	Netaikomas
Atviras	Vykdomas	Įvykdytas	Netaikomas			
Įrodymas / pagrindimas						
A.11.4	Laikmenos su asmens duomenimis, kurios išgabenamos iš patalpų, yra apsaugotos nuo neteisėtos prieigos ir praradimo, paprastai šifravimu ir gabenimo įrašu.					
Iš ko tai galima atpažinti: Įrodymas yra šifravimo įrodymas (visos laikmenos šifravimas), gabenimo ir perdavimo įrašai bei laikmenų inventorių. Klausimas tiekėjui: ar laikmenos su klientų duomenimis kada nors išgabenamos iš teikėjo objektų, pavyzdžiui dėl atsarginių kopijų, ir kaip jos apsaugotos gabenimo metu?						
<table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table>			Atviras	Vykdomas	Įvykdytas	Netaikomas
Atviras	Vykdomas	Įvykdytas	Netaikomas			
Įrodymas / pagrindimas						
A.11.5	Nešifruotų nešiojamųjų laikmenų ir įrenginių naudojimas asmens duomenims yra draudžiamas arba apribotas pagrįstomis išimtimis su dokumentuotu patvirtinimu.					
Iš ko tai galima atpažinti: Įrodymas yra keičiamųjų laikmenų politika ir techninis jos įgyvendinimas, pavyzdžiui priverstinis įrenginių šifravimas arba per įrenginių valdymą užblokuoti USB prievadai. Klausimas tiekėjui: ar darbuotojai gali kopijuoti klientų duomenis į nešifruotus įrenginius ir kas tam techniškai užkerta kelią?						
<table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table>			Atviras	Vykdomas	Įvykdytas	Netaikomas
Atviras	Vykdomas	Įvykdytas	Netaikomas			
Įrodymas / pagrindimas						
A.11.6	Viešaisiais tinklais perduodami asmens duomenys yra šifruojami. Naudojami mechanizmai atitinka dabartinį technikos lygį.					
Iš ko tai galima atpažinti: Įrodymas yra TLS konfigūracija (naujausia protokolo versija, jokių pasenusių šifrų) ir išorinis konfigūracijos patikrinimas kaip ataskaita. Mažoje įmonėje praktiška kartą per metus atlikti nemokamą TLS patikrą ir rezultatą įsegti į bylą. Klausimas tiekėjui: kokią perdavimo šifravimą taikote ir ar įjungtas saugomų duomenų šifravimas?						
<table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table>			Atviras	Vykdomas	Įvykdytas	Netaikomas
Atviras	Vykdomas	Įvykdytas	Netaikomas			
Įrodymas / pagrindimas						
A.11.7	Popieriniai įrašai su asmens duomenimis sunaikinami taip, kad jų atkurti nebūtų įmanoma.					
Iš ko tai galima atpažinti: Įrodymas yra tinkamo saugumo lygio smulkintuvai arba sunaikinimo pažymos iš paslaugų teikėjo, dirbančio pagal DIN 66399 ar lygiavertį standartą. Klausimas tiekėjui: kaip sunaikinate su klientais susijusius popierinius įrašus ir ar sunaikinimo pažymos saugomos byloje?						
<table><tr><td>Atviras</td><td>Vykdomas</td><td>Įvykdytas</td><td>Netaikomas</td></tr></table>			Atviras	Vykdomas	Įvykdytas	Netaikomas
Atviras	Vykdomas	Įvykdytas	Netaikomas			
Įrodymas / pagrindimas						

A.11.8 Naudotojų identifikatoriai vienareikšmiškai priskiriami vienam asmeniui ir nėra nei pakartotinai išduodami, nei bendrai naudojami. Bendros paskyros egzistuoja tik pagrįstomis išimtimis ir su papildomu atsekamumu.

Iš ko tai galima atpažinti: Įrodymas yra naudotojų sąrašas iš tapatybės valdymo sistemos be grupinių paskyrų kartu su taisykle, kad administravimo darbai atliekami iš asmeninės paskyros. Klausimas tiekėjui: ar eksploatavimo darbuotojai dirba su asmeninėmis paskyromis ir ar daugiaveiksnis autentiškumo patvirtinimas yra būtinas?

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

A.11.9 Teikėjas bet kuriuo metu gali nurodyti, kurie asmenys ar vaidmenys turi teisę pasiekti asmens duomenis, ir šią apžvalgą nuolat atnaujina.[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra prieigos teisių apžvalga pagal vaidmenis, paremta pasikartojančia prieigos peržiūra su data ir rezultatu. Mažoje įmonėje pakanka kas pusmetį eksportuoto ir pasirašyto naudotojų sąrašo. Klausimas tiekėjui: kiek darbuotojų gali pasiekti mūsų duomenis ir kaip dažnai tai peržiūrite?

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

A.11.10 Naudotojų paskyros valdomos per visą jų būvio ciklą: sukūrimas, keitimas ir nedelsiamas išjungimas, kai asmuo išeina ar keičia vaidmenį.

Iš ko tai galima atpažinti: Įrodymas yra darbuotojų priėmimo ir atleidimo procedūra su kontroliniu sąrašu ir išjungtų paskyrų žurnalai su laiko žymomis. Klausimas tiekėjui: per kokį laikotarpį atimate prieigą iš išeinančių darbuotojų ir kaip tai įrodote?

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

A.11.11 Teikėjo saugumo ir privatumo įsipareigojimai yra įtvirtinti sutartyje, įskaitant technines ir organizacines priemones, kliento nurodymų saistantį pobūdį ir kliento teisę atlikti auditą.[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra pasirašyta duomenų tvarkymo sutartis pagal GDPR 28 straipsnį su priemonių priedu ir audito arba informavimo teise. Klausimas tiekėjui: prašome pateikti pasirašytą duomenų tvarkymo sutartį su visais priedais, o ne vien nuorodą į bendrąsias paslaugų teikimo sąlygas.

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

A.11.12 Pasitelktiems duomenų tvarkytojams, kurie tvarko asmens duomenis, taikomi bent tokie patys įsipareigojimai kaip ir pačiam teikėjui. Jų atranka ir nuolatinė stebėseną vyksta pagal nustatytą procesą.

Iš ko tai galima atpažinti: Įrodymas yra įsipareigojimų perkėlimas į sutartis su pasitelktais duomenų tvarkytojais (GDPR 28 straipsnio 4 dalis) ir tiekėjų vertinimas su data. Klausimas tiekėjui: kaip vertinate pasitelktus duomenų tvarkytojus ir kokių įrodymų iš jų reikalaujate?

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

A.11.13 Prieš pakartotinai naudojant saugyklos vietą, užtikrinama, kad ankstesnių naudotojų duomenys neliktų pasiekiami nei fiziniuose laikmenose, nei virtualizuotose aplinkose.

Iš ko tai galima atpažinti: Įrodymas yra valymo arba perrašymo procedūra, taikoma atlaisvinant saugyklą, laikmenų sunaikinimo įrašai ir architektūros dokumente aprašytas nuomininkų atskyrimas. Klausimas tiekėjui: kaip užtikrinte, kad pakartotinai naudojamoje saugykloje nelieka kitų klientų liekamųjų duomenų?

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

A.12 Privatumo atitiktis

3

A.12.1 Šalys, kuriose asmens duomenys saugomi ir tvarkomi, yra įvardytos ir žinomos debesijos paslaugos klientui. Apie saugojimo vietų pakeitimus pranešama.[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra teikėjo objektų ir regionų apžvalga sutartyje arba dokumentacijoje ir naudojamos paslaugos regiono nustatymo ekrano nuotrauka. Klausimas tiekėjui: kokiose šalyse mūsų duomenys saugomi, iš kokių šalių prie jų prieinama, pavyzdžiui teikiant palaikymą, ir ar galime regioną užfiksuoti?

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

A.12.2 Asmens duomenų perdavimai į trečiąsias valstybes yra žinomi, pagrįsti ir užtikrinti tinkamomis apsaugos priemonėmis.[Dokumentas](#)

Iš ko tai galima atpažinti: Įrodymas yra standartinės sutarčių sąlygos arba sprendimas dėl tinkamumo, paremtas perdavimo poveikio vertinimu, kuris mažoje įmonėje gali būti trumpas: paveiktos duomenų kategorijos, paskirties šalis, rizika, taikytos papildomos priemonės. Klausimas tiekėjui: koku teisiniu pagrindu perduodate duomenis į trečiąsias valstybes ir kokias papildomas priemones taikote?

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas

5.31 Teisiniai ir sutartiniai reikalavimai, taikomi asmens duomenų tvarkymui, yra nustatyti ir atnaujinami keičiantis teisei padėčiai. Prieštaraujančios jurisdikcijos yra įvertintos.

Iš ko tai galima atpažinti: Įrodymas yra taikomų reikalavimų apžvalga (GDPR, nacionalinės taisyklės, sektoriui būdingos pareigos) su atsakingu asmeniu ir peržiūros data. Mažoje įmonėje pakanka vieno puslapio sąrašo, peržiūrimo kartą per metus. Klausimas tiekėjui: ar teikėjui arba pasitelktiems duomenų tvarkytojams taikomos jurisdikcijos, kurios leidžia institucijoms pasiekti mūsų duomenis, ir kaip tai sprendžiama?

Atviras Vykdomas Įvykdytas Netaikomas

Įrodymas / pagrindimas