

ISO/IEC 27018:2025, infoturve, küberturvalisus ja privaatsuse kaitse: juhised isikuandmete (PII) kaitseks avalikes pilvedes, mis tegutsevad PII volitatud töötlejana (3. väljaanne, 2025-08)

PII kaitse avalikus pilves

36 nõuet. Selle standardi kohta akrediteeritud sertifikaati ei ole. Versioon 07/2026.

ISO/IEC 27018 ei ole juhtimissüsteemi standard, vaid juhiste kogum, mis lisab standardile ISO/IEC 27002:2022 laiendatud ohjemeetmeid. ISO/IEC 27018 järgi eraldiseisvat akrediteeritud sertifikaati ei ole. Ohjemeetmed võetakse ISO/IEC 27001 süsteemi rakendatavuse avaldusse ja sertifikaat väljastatakse seejärel standardi ISO/IEC 27001 järgi koos viitega standardile ISO/IEC 27018. Standard on suunatud avaliku pilveteenuse pakkujale, kes töötleb isikuandmeid oma pilveteenuse klientide nimel. Organisatsioon, kes pilveteenuseid üksnes kasutab, sellesse rolli ei astu ja hindab nõudeid mõistlikult oma pakkujate, mitte iseenda suhtes. Leanshifti jaoks on see kontrollnimekiri seetõttu eelkõige tarnijate hindamise raamistik. Iga punkti saab pakkujale küsimusena esitada ja GDPR artikli 28 kohase andmetöötluslepinguga kindlustada. Sellise hindamise tulemus on sisemine vastavuskirje või pakkuja hindamisprofiil, mitte sertifikaat. Nummerdamisest: peatükid A.2 kuni A.12 järgivad standardi lisas A toodud privaatsuse põhimõtteid ja punktid numbriga nagu A.11.6 on seal loetletud lisaohjemeetmed. Punktid numbriga nagu 8.10 või 5.34 viitavad ISO/IEC 27002:2022 ohjemeetmetele, mida standard pilve jaoks täpsustab. Punktid lisandiga (Grundsatz), mis tähendab põhimõtet, tulenevad peatüki enda põhimõttest, kui lisa A eraldi lisaohjemeetmed ei sisalda.

Ettevõtte	Kuupäev	Täitja
-----------	---------	--------

A.2 Nõusolek ja valikuvõimalus2

A.2.1Pilveteenuse pakkuja toetab pilveteenuse klienti andmesubjektide õiguste täitmisel, näiteks andmetega tutvumine, parandamine, kustutamine ja vastuväite esitamine. Vastutus ja tähtajad on lepingus määratud.

Dokument

Mille järgi seda näeb: Tõendiks on GDPR artikli 28 kohane andmetöötlusleping klausliga andmesubjektide õiguste täitmise toetamise kohta, koos teenuse enda tehniliste vahenditega: ekspordi-, parandamis- ja kustutamiskutsed või dokumenteeritud tugikord koos reageerimistähtajaga. Küsimus tarnijale: millise funktsiooni või protsessi pakute, et saaksime andmetega tutvumise või kustutamise taotluse ühe kuu jooksul täita?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.2 (Grundsatz)Pilveteenuse klientide isikuandmeid töödeldakse üksnes kliendi dokumenteeritud juhiste alusel. Andmesubjektide nõusoleku hankimine jääb kliendi kui vastutava töötleja ülesandeks ja pakkuja sellest ette ei rutta.

Mille järgi seda näeb: Tõendiks on juhiste klausel andmetöötluslepingus ja tõend selle kohta, et pakkuja andmeid teisesel eesmärgil ei kasuta, näiteks teenuse privaatsusteade ja tootedokumentatsioon. Küsimus tarnijale: kas töötlete meie kliendiandmeid mingil viisil väljaspool meie juhiseid, näiteks toote parandamiseks või mudelite treenimiseks?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.3 Eesmärgi õiguspärasus ja määratlemine2

A.3.1Eesmärk, milleks pakkuja isikuandmeid töötleb, piirdub kokkulepitud teenuse osutamisega ja on lepingus nimetatud. Töötlemist pakkuja oma eesmärkidel ei toimu.

Dokument

Mille järgi seda näeb: Tõendiks on andmetöötlusleping, milles on esitatud töötlemise ees, laad, eesmärk ja kestus ning andmesubjektide kategooriad vastavalt GDPR artikli 28 lõikele 3. Küsimus tarnijale: palume lepingu lisa, mis kirjeldab töötlemise eesmärki ammendavalt. Väikesele ettevõttele piisab pakkuja standardsest andmetöötluse lisast, kui see sisaldab seda teavet.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.3.2

Pakkujale usaldatud isikuandmeid ei kasutata reklaamiks, turunduseks ega pakkuja muudel ärilistel eesmärkidel ilma eelneva sõnaselge nõusolekuta. Teenuse osutamine ei sõltu sellisest nõusolekust.

Mille järgi seda näeb: Tõendiks on sõnaselge lepingusäte, mis välistab ärilise teisese kasutuse, koos teenuse kasutustingimustega. Küsimus tarnijale: kinnitage kirjalikult, et kliendiandmeid ei kasutata reklaamiks, profiilialalüüsiks ega tehisintellekti (AI) mudelite treenimiseks. Kui see kinnitus puudub, ei sobi teenus isikuandmete jaoks.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.4 Kogumise piiramine

1

A.4 (Grund)

Lisaks andmetele, mille klient teenusesse sisestab, pakkuja oma eesmärkidel täiendavaid isikuandmeid ei kogu, näiteks telemeetriat, kasutusprofiile ega sisuanalüüse. Kogutavad tegevusandmed ja metaandmed on nimetatud ja põhjendatud.

Mille järgi seda näeb: Tõendiks on loend andmetest, mida teenus sisuandmete kõrval salvestab (pääsulogid, telemeetria, diagnostikaandmed), koos eesmärgi ja säilitusajaga, ning ekraanitõmmis seadistusest, millega valikuline telemeetria välja lülitatakse. Küsimus tarnijale: milliseid kasutus-, telemeetria- ja diagnostikaandmeid kogute lisaks, milleks neid kasutate ja kas saame kogumise välja lülitada?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.5 Andmete minimeerimine

2

A.5.1

Isikuandmete töötlemisel tekkivad ajutised failid, näiteks ajutine salvestusruum, vahemälud või tagasivõtmise päevikud, kustutatakse turvaliselt kindlaksmääratud aja jooksul.

Mille järgi seda näeb: Tõendiks on töö- või kustutamiskord, milles on nimetatud ajutiste andmete säilitusaeg, mida toetab süsteemi konfiguratsioon, näiteks vahemälu eluiga (TTL) või ajastatud puhastustöö koos täitmislogiga. Küsimus tarnijale: millise aja järel kustutatakse vahemälud, ajutised failid ja vaheseisundid ning kuidas seda seiratakse?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

8.11

Kõikjal, kus käitamine, testimine või tugi reaalandmeid ei vaja, on isikuandmed maskeeritud, pseudonümiseeritud või anonümiseeritud. Töödeldavate andmete maht piirdub sellega, mida teenus tegelikult vajab.

Mille järgi seda näeb: Tõendiks on reegel selle kohta, millised keskkonnad tohivad reaalandmeid näha, ning ekraanitõmmised või skriptid maskeerimisest, mida test- ja arendussüsteemides kasutatakse. Küsimus tarnijale: kas tugi- ja arendusmeeskonnad töötavad tootmisandmetega ja kui jah, siis milliste kaitsemeetmete all? Väikesele ettevõttele piisab reeglist, et testsüsteimid töötavad üksnes genereeritud näidisandmetega.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.6 Kasutamise, säilitamise ja avalikustamise piiramine

3

A.6.1

Kui pakkuja saab õiguslikult siduva nõude isikuandmete avaldamiseks, näiteks ametiasutuselt, teavitab ta pilveteenuse klienti eelnevalt niivõrd, kui võrd seadus seda lubab.

Mille järgi seda näeb: Tõendiks on lepinguline teavitamisklausel ja sisemine protsess ametiasutuste päringute jaoks koos nimetatud vastutajaga. Küsimus tarnijale: kas teavitate meid enne andmete üleandmist ja kas avaldate läbipaistvusaruande ametiasutuste päringute kohta? Ajakohane läbipaistvusaruanne on tugev tõend.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.6.2	Kui pakkuja avaldab isikuandmeid kolmandatele isikutele, registreerib ta sündmuse jälgitaval kujul: kes andmed sai, millal see toimus, millised andmed olid hõlmatud ja millisele alusele avaldamine tugineb.			Dokument
	Mille järgi seda näeb: Tõendiks on avalikustamiste register või tugipiletite ajalugu nende väljadega, isegi kui kandeid ei ole. Tühi, kuid ajakohasena hoitav register on vastuvõetav ja on väikesele ettevõttele praktiline tee. Küsimus tarnijale: kas peate andmete avaldamise registrit ja kas saame sellest väljavõtteid?			

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8.10	Isikuandmed kustutatakse, kui kokkulepitud säilitusaeg lõpeb või leping lõpeb, sealhulgas varukoopiates olevad koopiad pärast nende rotatsioonitsükli.
Mille järgi seda näeb: Tõendiks on kustutamise kontseptsioon koos säilitusaegadega andmekategooriate kaupa, varukoopiate säilitusaeg ning kustutamislõgi või kustutamise kinnitus. Küsimus tarnijale: kui kaua meie andmed pärast lepingu lõppu varukoopiates püsivad ja kas saame nende kustutamise kohta kirjaliku kinnituse?	

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7 Õigus ja kvaliteet

2

A.7 (Grund)	Pakkuja ei muuda talle usaldatud isikuandmeid omal algatusel. Parandused ja uuendused tehakse üksnes pilveteenuse kliendi juhisel või funktsioonide kaudu, mida klient ise kasutab.
-------------	--

Mille järgi seda näeb: Tõendiks on teenuse muutmisfunktsioonid koos muudatuste ajalooga ning juhiste klausel andmetöötuslepingus. Küsimus tarnijale: kas saame kirjeid ise parandada ja kas iga muudatus logitakse jälgitaval kujul?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8.13	Isikuandmete terviklus on kaitstud salvestamisel, edastamisel ja taastamisel. Varukoopiad on olemas ja nende taastatavus on testitud.
------	--

Mille järgi seda näeb: Tõendiks on varukoopiate konfiguratsioon, kontrollsummad või terviklust tagavad mehhanismid ning vähemalt üks dokumenteeritud taastamise test aastas koos kuupäeva ja tulemusega. Küsimus tarnijale: kui sageli taastamist testite ja millise taasteaja teenustasemes tagate?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8 Avatus, läbipaistvus ja teavitamine

2

A.8.1	Isikuandmeid töötlevate alltöötajate kasutamine avaldatakse enne lepingu sõlmimist. Loendi muudatustest teavitatakse klienti aegsasti, et klient saaks esitada vastuväite või lepingu lõpetada.	Dokument
-------	--	--------------------------

Mille järgi seda näeb: Tõendiks on ajakohane alltöötajate loend, mis on avaldatud või lepinguga kättesaadavaks tehtud, koos nime, riigi ja töötlemise eesmärgiga, ning teavitamisreegel vastavalt GDPR artikli 28 lõikele 2. Küsimus tarnijale: kust leiame alltöötajate loendi, kui pika eettetamisaajaga muudatustest teatate ja kuidas saame vastuväite esitada?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8 (Grund)	Enne lepingu sõlmimist teeb pakkuja kättesaadavaks arusaadava teabe selle kohta, kuidas isikuandmeid töödeldakse, millised kaitsemeetmed on olemas ja millistes õigusruumides töötlemine toimub.
-------------	---

Mille järgi seda näeb: Tõendiks on privaatsusteade, turbe ülevaadetokument, usalduskeskuse leht ja andmetöötusleping koos tehniliste ja korralduslike meetmetega lisana. Küsimus tarnijale: palume ajakohast tehniliste ja korralduslike meetmete loendit lepingu lisana, mitte üksnes turundusmaterjali.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.9 Isiku kaasatus ja juurdepääs

2

A.9 (Grundstuen) Teenus annab pilveteenuse kliendile tehnilised vahendid, et andmesubjektide tutvumis-, parandamis- ja kustutamistaotlusi ise täita, näiteks ekspordi-, otsingu- ja kustutamiskutsingute kaudu.

Mille järgi seda näeb: Tõendiks on ekspordi- ja kustutamiskutsingute tootdokumentatsioon, mida toetab sisemine proovikäik: üks tutvumistaotlus tehakse algusest lõpuni läbi ja pannakse kirja, kui kaua see võtab. Küsimus tarnijale: kas saame ühe isiku kõik andmed leida, eksportida ja kustutada ilma teie toeta?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.34 Kui klient ei saa andmesubjekti taotlust ise täita, aitab pakkuja kokkulepitud aja jooksul. Taotlused, mille andmesubjektid saadavad otse pakkujale, edastatakse kliendile ja pakkuja neile ise ei vasta.

Mille järgi seda näeb: Tõendiks on vastav klausel andmetöötluslepingus koos konkreetse reageerimistähtajaga ning tugipileti ajalugu tegeliku näitena. Küsimus tarnijale: millise tähtaja tagate andmesubjektide õiguste täitmise toetamisel ja mida see maksab?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.10 Aruandekohustus

4

A.10.1 Isikuandmetega seotud rikkumistest teatatakse pilveteenuse kliendile põhjendamatu viivitusega, nimetades ulatuse, mõjutatud andmed, põhjuse ja võetud meetmed. Teavitamisprotsess koos vastutuse ja tähtaegadega on määratletud.[Dokument](#)

Mille järgi seda näeb: Tõendiks on juhtumile reageerimise plaan koos eskaleerimisahelaga, lepinguline teavitamistähtaeg (praktikas toimib 24 kuni 48 tundi, et klient jõuaks veel täita GDPR artiklis 33 sätestatud 72 tunni tähtaja) ning kirjed varasematest juhtumitest või õppusest. Küsimus tarnijale: millise aja jooksul juhtumist teatate, millise kanali kaudu ja millist teavet sellega edastate?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.10.2 Infoturbepoliitika, töökordi ja nendega seotud kirjeid säilitatakse kindlaksmääratud aja, et töötlemise käiku saaks tagantjärele taastada.[Dokument](#)

Mille järgi seda näeb: Tõendiks on säilitamisreegel koos poliitika versioonijaloga, näiteks dokumendiregistri või versioonihaldussüsteemi kaudu, milles on kinnitamise kuupäev. Küsimus tarnijale: kui kaua hoiate poliitika versioone ja nendega seotud kirjeid ning kas saame auditi korral neile juurdepääsu?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.10.3 Isikuandmete tagastamiseks, üleandmiseks ja hävitamiseks lepingu lõppedes on olemas määratletud kord, milles on nimetatud vormingud, tähtajad ja koopiade käsitlemine.[Dokument](#)

Mille järgi seda näeb: Tõendiks on lepingu lõpetamise klausel andmetöötluslepingus ning kustutamise kinnitus pärast lepingu lõppu. Küsimus tarnijale: millises vormingus ja millise aja jooksul saame oma andmed tagasi, millal hävitatakse kõik koopiad ja kas saame selle kohta kirjaliku kinnituse?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.35 Kaitsemeetmete tulemuslikkust vaadatakse sõltumatult üle kindlaksmääratud sagedusega, näiteks siseauditite, läbistustestide või kolmanda poole kinnitusaruannete kaudu. Tulemused tehakse pilveteenuse kliendile sobival kujul kättesaadavaks.

Mille järgi seda näeb: Tõendiks on ISO/IEC 27001 sertifikaat koos rakendatavuse avaldusega, mis hõlmab ISO/IEC 27018 ohjemeetmeid, või SOC 2 aruanne, koos ajakohaste läbistustestide kokkuvõtetega. Küsimus tarnijale: palume sertifikaati, selle käsitusala ja kinnitust, et ISO/IEC 27018 kajastub rakendatavuse avalduses. Kontrollimist väärleb, kas käsitusala hõlmab tegelikult kasutatavat teenust.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.11 Infoturve

13

A.11.1

Kõik, kellel on juurdepääs isikuandmetele, on seotud konfidentsiaalsuskohustusega, olenemata sellest, kas nad on otse tööle võetud või väljastpoolt kaasatud.

Mille järgi seda näeb: Tõendiks on allkirjastatud konfidentsiaalsuslepingud või kohustused, mis kehtivad ka pärast koostöö lõppu. Küsimus tarnijale: kas kõik andmetele juurdepääsu omavad töötajad ja teenusepakkujad on kirjalikult konfidentsiaalsuskohustusega seotud?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.2

Isikuandmeid sisaldavaid väljatrükke ja muid paberkoopiaid tehakse üksnes hädavajaduse korral. Lubatud ulatus on reeglina määratud.

Mille järgi seda näeb: Tõendiks on väljatrükkide käsitlemise reegel, mis andmekeskustes tähendab tavaliselt üldist printimise keeldu aladel, kus hoitakse kliendiandmeid. Küsimus tarnijale: kas kliendiandmeid teie tegevuses üldse prinditakse ja kui jah, siis millistel tingimustel?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.3

Varukoopiatest taastamine kiidetakse eelnevalt heaks ja logitakse, sealhulgas taastamise käivitanud isik ja mõjutatud andmed.

Mille järgi seda näeb: Tõendiks on taastamislogi koos ajatempli, algataja ja ulatusega, mille varunduse tööriist tavaliselt automaatselt loob. Küsimus tarnijale: kas logite iga taastamise ja kas saame auditi korral neid logisid vaadata?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.4

Isikuandmeid sisaldavad andmekandjad, mis viiakse tegevuskohast välja, on kaitstud volitamata pääsu ja kaotsimineku eest, üldjuhul krüpteerimise ja transpordikirje abil.

Mille järgi seda näeb: Tõendiks on krüpteerimise tõend (andmekandja täielik krüpteerimine), transpordi- ja üleandmiskirjed ning andmekandjate register. Küsimus tarnijale: kas kliendiandmeid sisaldavad andmekandjad lahkuvad kunagi teie asukohtadest, näiteks varukoopiade jaoks, ja kuidas need on teel kaitstud?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.5

Krüpteerimata kaasaskantavate andmekandjate ja seadmete kasutamine isikuandmete jaoks on keelatud või piiratud põhjendatud eranditega, millel on dokumenteeritud heakskiit.

Mille järgi seda näeb: Tõendiks on irdkandjate poliitika ning tehniline jõustamine, näiteks kohustuslik seadme krüpteerimine või seadmehalduse kaudu blokeeritud USB-pordid. Küsimus tarnijale: kas töötajad saavad kliendiandmeid krüpteerimata seadmetele kopeerida ja mis seda tehniliselt takistab?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.6

Avalike võrkude kaudu edastatavad isikuandmed on krüpteeritud. Kasutatavad mehhanismid vastavad praegusele tehnika tasemele.

Mille järgi seda näeb: Tõendiks on TLS-i konfiguratsioon (ajakohane protokolliversioon, vananenud šifreid ei ole) ja väline konfiguratsioonitest aruandena. Väikesele ettevõttele on praktiline teha kord aastas tasuta TLS-i skannimine ja tulemus talletada. Küsimus tarnijale: millise transpordikrüpteerimise jõustate ja kas salvestatud andmete krüpteerimine on aktiivne?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.7

Isikuandmeid sisaldavad paberkirjed hävitatakse viisil, mis välistab nende taastamise.

Mille järgi seda näeb: Tõendiks on piisava turvasemega dokumendihävitid või hävitamistõendid teenusepakkujalt, kes töötab standardi DIN 66399 või samaväärse standardi järgi. Küsimus tarnijale: kuidas hävitatakse klientidega seotud paberkirjed ja kas hävitamistõendid on talletatud?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.8 Kasutajatunnused on omistatud üheselt ühele isikule ning neid ei anta uuesti välja ega jagata. Jagatud kontod on olemas üksnes põhjendatud eranditena ja täiendava jälgitavusega.

Mille järgi seda näeb: Tõendiks on identiteedisüsteemist pärit kasutajate loend, milles rühmakontosid ei ole, koos reegluga, et haldustööd tehakse isikliku konto alt. Küsimus tarnijale: kas teie halduspersonal töötab isiklike kontodega ja kas mitmeastmeline autentimine on kohustuslik?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.11.9 Pakkuja saab igal ajal öelda, millised isikud või rollid tohivad isikuandmetele juurde pääseda, ja hoiab selle ülevaate ajakohasena. Dokument

Mille järgi seda näeb: Tõendiks on pääsuõiguste ülevaade rollide kaupa, mida toetab korduv pääsuõiguste ülevaatus koos kuupäeva ja tulemusega. Väikesele ettevõttele piisab kasutajate loendi poolaastasest väljavõttest koos kinnitusega. Küsimus tarnijale: kui paljud teie töötajad pääsevad meie andmetele ligi ja kui sageli seda üle vaatate?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.11.10 Kasutajakontosid hallatakse kogu olelusringi ulatuses: loomine, muutmine ja kiire deaktiveerimine, kui keegi lahkub või rolli vahetab.

Mille järgi seda näeb: Tõendiks on tööle võtmise ja töölt lahkumise kord koos kontrollnimekirjaga ning deaktiveeritud kontode logid koos ajatemplitega. Küsimus tarnijale: millise aja jooksul võtate lahkuvatelt töötajatelt pääsuõigused ära ja kuidas seda tõendate?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.11.11 Pakkuja turbe- ja privaatsuskohustused on lepingus kindlaks määratud, sealhulgas tehnilised ja korralduslikud meetmed, kliendi juhiste siduvus ning kliendi õigus auditeerida. Dokument

Mille järgi seda näeb: Tõendiks on allkirjastatud GDPR artikli 28 kohane andmetöötlusleping koos meetmete lisaga ning auditi- või teabeõigusega. Küsimus tarnijale: palume allkirjastatud andmetöötluslepingut koos lisadega, mitte üksnes viidet üldistele kasutustingimustele.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.11.12 Isikuandmeid töötlevatele alltöötlejatele kehtivad vähemalt samad kohustused mis pakkuja endale. Nende valikut ja jooksvat seiret reguleerib määratletud protsess.

Mille järgi seda näeb: Tõendiks on kohustuste edasiandmine alltöötlejatega sõlmitud lepingutes (GDPR artikli 28 lõige 4) ja kuupäeva kandev tarnija hindamine. Küsimus tarnijale: kuidas hindate oma alltöötlejaid ja milliseid tõendeid neilt nõuate?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.11.13 Enne salvestusruumi taaskasutamist on tagatud, et varasemate kasutajate andmed ei jää kättesaadavaks, ei füüsilistel andmekandjatel ega virtualiseeritud keskkondades.

Mille järgi seda näeb: Tõendiks on puhastamise või ülekirjutamise kord, mida kohaldatakse salvestusruumi vabastamisel, andmekandjate hävitamise kirjed ning arhitektuuridokumendis kirjeldatud klientide eraldatus. Küsimus tarnijale: kuidas tagate, et taaskasutatavas salvestusruumis ei ole teiste klientide jääkandmeid?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.12 Privaatsusnõuetele vastavus3

A.12.1

Riigid, kus isikuandmeid säilitatakse ja töödeldakse, on nimetatud ja pilveteenuse kliendile teada. Salvestuskohtade muudatustest teavitatakse.

Mille järgi seda näeb: Tõendiks on pakkuja ülevaade asukohtadest ja piirkondadest, kas lepingus või dokumentatsioonis, ning ekraanitõmmis kasutatava teenuse piirkonnaseadistusest. Küsimus tarnijale: millistes riikides meie andmed salvestatuna asuvad, millistest riikidest neile ligi pääsetakse, näiteks toe käigus, ja kas saame piirkonna fikseerida?

AvatudTöösTäidetudEi kohaldu

Tõend / põhjendus

A.12.2

Isikuandmete edastamine kolmandatesse riikidesse on teada, põhjendatud ja kaetud asjakohaste kaitsemeetmetega.

Mille järgi seda näeb: Tõendiks on lepingu tüüptingimused või kaitse piisavuse otsus, mida toetab edastuse mõjuhindang, mis väikeses ettevõttes võib olla lühike: hõlmatud andmekategooriad, sihtriik, risk, võetud lisameetmed. Küsimus tarnijale: millisel õiguslikul alusel edastate andmeid kolmandatesse riikidesse ja milliseid täiendavaid meetmeid kohaldate?

AvatudTöösTäidetudEi kohaldu

Tõend / põhjendus

5.31

Isikuandmete töötlemisele kohalduvad õiguslikud ja lepingulised nõuded on tuvastatud ning neid hoitakse õigusliku olukorra muutudes ajakohasena. Vastuolulised õigusruumid on hinnatud.

Mille järgi seda näeb: Tõendiks on kohalduvate nõuete ülevaade (GDPR, riigisisesed reeglid, valdkonnapõhised kohustused) koos vastutaja ja ülevaatuse kuupäevaga. Väikeses ettevõttes piisab ühelehelisest loendist, mis vaadatakse üle kord aastas. Küsimus tarnijale: kas teie või teie alltöötlejad alluvad õigusruumidele, mis lubavad ametiasutustel meie andmetele ligi pääseda, ja kuidas sellega toime tulete?

AvatudTöösTäidetudEi kohaldu

Tõend / põhjendus

Nõuded on sõnastatud iseseisvalt ega asenda standardi teksti. Siduv on ainult vastava väljaandja originaalstandard. See loend on töövahend, mitte vastavuse tõend ega sertifitseerimine. Leanshift ei ole ühegi nimetatud standardi järgi sertifitseeritud, ei ole sertifitseerimisasutus ega ole seotud ISO, IEC, DIN, IATF, IAQG ega SAEga. Kahtluse korral kehtib selle loendi saksakeelne versioon.