

ISO/IEC 27018:2025, Tietoturvallisuus, kyberturvallisuus ja yksityisyyden suoja:
Ohjeita henkilötietojen (PII) suojaamiseen julkisissa pilvipalveluissa, jotka toimivat
henkilötietojen käsittelijöinä (3. painos, 2025-08)

Henkilötietojen suoja julkisessa pilvipalvelussa

36 vaatimusta. Tälle standardille ei ole akkreditoitua sertifiikaattia. Versio 07/2026.

ISO/IEC 27018 ei ole johtamisjärjestelmästandardi vaan ohjeisto, joka laajentaa standardin ISO/IEC 27002:2022 hallintakeinoja. Standardille ISO/IEC 27018 ei ole erillistä akkreditoitua sertifiikaattia. Hallintakeinot otetaan mukaan ISO/IEC 27001 -järjestelmän soveltuvuuslausuntoon, ja sertifiikaatti myönnetään tällöin standardin ISO/IEC 27001 mukaisena viittauksella standardiin ISO/IEC 27018. Standardi kohdistuu julkisen pilvipalvelun tarjoajaan, joka käsittelee henkilötietoja pilvipalvelun asiakkaidensa lukuun. Organisaatio, joka pelkästään käyttää pilvipalveluja, ei ota tätä roolia, ja sen on järkevää kohdistaa vaatimukset toimittajiinsa eikä itseensä. Leanshiftille tämä lista on siksi ennen kaikkea toimittaja-arvioinnin kehikko. Jokainen kohta voidaan esittää toimittajalle kysymyksenä ja varmistaa GDPR:n artiklan 28 mukaisella käsittelysopimuksella. Tällaisen arvioinnin tulos on sisäinen vaatimustenmukaisuuden tallenne tai toimittajan arviointiprofiili, ei sertifiikaatti. Numeroinnista: luvut A.2:sta A.12:een noudattavat standardin liitteen A yksityisyyden suojan periaatteita, ja kohdat, joiden numero on muotoa A.11.6, ovat siellä luetellut lisähallintakeinot. Kohdat, joiden numero on muotoa 8.10 tai 5.34, viittaavat standardin ISO/IEC 27002:2022 hallintakeinoihin, jotka tämä standardi tarkentaa pilvipalvelua varten. Kohdat, joissa on lisäys (Grundsatz) eli periaate, johdetaan luvun omasta periaatteesta silloin, kun liitteessä A ei ole erillistä lisähallintakeinoja.

Yritys

Päivämäärä

Täyttäjä

A.2 Suostumus ja valinnanmahdollisuus

2

A.2.1

Pilvipalvelun tarjoaja tukee pilvipalvelun asiakasta rekisteröityjen oikeuksien toteuttamisessa, kuten tarkastusoikeuden, oikaisun, poiston ja vastustamisen osalta. Vastuut ja määräajat on sovittu sopimuksessa.

Asiakirja

Mistä sen tunnistaa: Näyttönä on GDPR:n artiklan 28 mukainen käsittelysopimus, jossa on ehto avustamisesta rekisteröityjen oikeuksissa, yhdessä palvelun omien teknisten keinojen kanssa: vienti-, korjaus- ja poistotoiminnot tai dokumentoitu tukimenettely vastausmääräaikaan. Kysymys toimittajalle: mitä toimintoa tai prosessia tarjoatte, jotta voimme hoitaa tarkastus- tai poistopyynnön kuukauden kuluessa?

Avoin

Kesken

Täytetty

Ei koske

Näyttö / perustelu

A.2 (Grundsatz)

Pilvipalvelun asiakkaiden henkilötietoja käsitellään vain asiakkaan dokumentoitujen ohjeiden mukaisesti. Suostumuksen hankkiminen rekisteröidyiltä jää asiakkaan tehtäväksi rekisterinpitäjänä, eikä tarjoaja ota sitä hoitaakseen.

Mistä sen tunnistaa: Näyttönä on käsittelysopimuksen ohjeistusehto sekä osoitus siitä, ettei tarjoaja käytä tietoja toissijaisesti, esimerkiksi palvelun tietosuojaseloste ja tuotedokumentaatio. Kysymys toimittajalle: käsittelettekö asiakastietojamme jollain tavalla ohjeidemme ulkopuolella, esimerkiksi tuotteen parantamiseen tai mallien kouluttamiseen?

Avoin

Kesken

Täytetty

Ei koske

Näyttö / perustelu

A.3 Käyttötarkoituksen oikeutus ja määrittely

2

A.3.1

Tarkoitus, johon tarjoaja käsittelee henkilötietoja, rajoittuu sovitun palvelun tuottamiseen ja on nimetty sopimuksessa. Käsittelyä tarjoajan omiin tarkoituksiin ei tapahdu.

Asiakirja

Mistä sen tunnistaa: Näyttönä on käsittelysopimus, jossa ilmoitetaan käsittelyn kohde, luonne, tarkoitus ja kesto sekä rekisteröityjen ryhmät GDPR:n artiklan 28 kohdan 3 mukaisesti. Kysymys toimittajalle: toimittakaa sopimusliite, joka kuvaa käsittelyn tarkoituksen tyhjentävästi. Pienelle yritykselle riittää toimittajan vakiomuotoinen käsittelyliite, kunhan se sisältää nämä tiedot.

Avoin

Kesken

Täytetty

Ei koske

Näyttö / perustelu

A.3.2	Tarjoajalle uskottuja henkilötietoja ei käytetä tarjoajan mainontaan, markkinointiin tai muihin kaupallisiin tarkoituksiin ilman etukäteen annettua nimenomaista suostumusta. Palvelun toimittamista ei aseteta riippuvaiseksi tällaisesta suostumuksesta.
Mistä sen tunnistaa: Näyttönä on nimenomainen sopimusehto, joka sulkee pois kaupallisen toissijaisen käytön, yhdessä palveluehtojen kanssa. Kysymys toimittajalle: vahvistakaa kirjallisesti, ettei asiakastietoja käytetä mainontaan, profilointiin tai tekoälymallien kouluttamiseen. Jos tämä sitoumus puuttuu, palvelu ei sovellu henkilötiedoille.	
Näyttö / perustelu	

A.4 Keräämisen rajoittaminen				1
A.4 (Grund)	Sen lisäksi mitä asiakas syöttää palveluun, tarjoaja ei kerää omiin tarkoituksiinsa muita henkilötietoja, kuten telemetriaa, käyttöprofiileja tai sisällön analyysia. Kerättävät toimintatiedot ja metatiedot on nimetty ja perusteltu.			
Mistä sen tunnistaa: Näyttönä on luettelo tiedoista, joita palvelu tallentaa sisältötietojen ohella (käyttölokkit, telemetria, diagnostiikkatiedot), tarkoituksineen ja säilytysaikoineen, sekä kuvakaappaus asetuksesta, jolla valinnainen telemetria kytketään pois. Kysymys toimittajalle: mitä käyttö-, telemetria- ja diagnostiikkatietoja keräätte lisäksi, mihin käytätte niitä, ja voimmeko kytkeä keräämisen pois?				
Näyttö / perustelu				

A.5

Tietojen minimointi

2

A.5.1

Henkilötietojen käsittelyssä syntyvät väliaikaiset tiedostot, kuten tilapäiset tallennustilat, välimuistit tai peruutuslokkit, poistetaan turvallisesti määritellyn ajan kuluessa.

Mistä sen tunnistaa: Näyttönä on käyttö- tai poistomenettely, jossa väliaikaisille tiedoille on ilmoitettu säilytysaika ja jota tukee järjestelmän konfiguraatio, esimerkiksi välimuistin elinaika (TTL) tai ajastettu siivoustyö suorituslokeineen. Kysymys toimittajalle: minkä ajan kuluttua välimuistit, väliaikaiset tiedostot ja välitilat poistetaan, ja miten sitä seurataan?

Näyttö / perustelu

8.11

Aina kun käyttö, testaus tai tuki ei edellytä tuotantotietoja, henkilötiedot peitetään, pseudonymisoidaan tai anonymisoidaan. Käsiteltävien tietojen määrä pysyy rajattuna siihen, mitä palvelu tosiasiaassa tarvitsee.

Mistä sen tunnistaa: Näyttönä on linjaus siitä, mitkä ympäristöt saavat nähdä tuotantotietoja, sekä kuvakaappaukset tai skriptit testi- ja kehitysjärjestelmissä käytetystä peittämisestä. Kysymys toimittajalle: työskentelevätkö tuki- ja kehitystiiminne tuotantotiedoilla, ja jos työskentelevät, minkä suojausten alaisena? Pienelle yritykselle riittää sääntö, jonka mukaan testijärjestelmät toimivat yksinomaan tuotetuilla esimerkkitiedoilla.

Näyttö / perustelu

A.6 Käytön, säilytyksen ja luovuttamisen rajoittaminen				3
A.6.1	Jos tarjoaja saa oikeudellisesti sitovan pyynnön luovuttaa henkilötietoja, esimerkiksi viranomaiselta, se ilmoittaa siitä pilvipalvelun asiakkaalle etukäteen siltä osin kuin laki sen sallii.			
Mistä sen tunnistaa: Näyttönä on sopimuksen ilmoitusehto ja sisäinen prosessi viranomaispyyntöjä varten nimettyine vastuuhenkilöineen. Kysymys toimittajalle: ilmoitatteko meille ennen tietojen luovuttamista, ja julkaisetteko avoimuusraportin viranomaispyynnöistä? Ajantasainen avoimuusraportti on vahva näyttö.				
Näyttö / perustelu				

A.6.2	Jos tarjoaja luovuttaa henkilötietoja kolmansille osapuolille, se kirjaa tapahtuman jäljitettävästi: kuka tiedot sai, milloin se tapahtui, mitä tietoja luovutus koski ja mihin perusteeseen se nojaa.				Asiakirja
	Mistä sen tunnistaa: Näyttönä on luovutusrekisteri tai tikketihistoria, jossa nämä kentät ovat, vaikka merkintöjä ei olisi yhtään. Tyhjä mutta ylläpidetty rekisteri on hyväksyttävissä ja on pienelle yritykselle käytännöllinen tapa. Kysymys toimittajalle: pidätkö rekisteriä tietojen luovutuksista, ja saammeko siitä otteita?				
	Avoim	Kesken	Täytetty	Ei koske	
Näyttö / perustelu					

8.10	Henkilötiedot poistetaan, kun sovittu säilytysaika päättyy tai sopimus päättyy, mukaan lukien varmuuskopioissa olevat kopiot niiden kiertosyklin jälkeen.				
	Mistä sen tunnistaa: Näyttönä on poistokonsepti, jossa on säilytysajat tietoryhmittäin, varmuuskopioiden säilytysaika sekä poistoloki tai poistovahvistus. Kysymys toimittajalle: kuinka kauan tietomme säilyvät varmuuskopioissanne sopimuksen päättymisen jälkeen, ja saammeko kirjallisen vahvistuksen niiden poistamisesta?				
	Avoim	Kesken	Täytetty	Ei koske	
Näyttö / perustelu					

A.7 Täsmällisyys ja laatu

2

A.7 (Grund)	Tarjoaja ei muuta sille uskottuja henkilötietoja oma-aloitteisesti. Korjaukset ja päivitykset tehdään yksinomaan pilvipalvelun asiakkaan ohjeesta tai toiminnoilla, joita asiakas käyttää itse.				
	Mistä sen tunnistaa: Näyttönä ovat palvelun muokkaustoiminnot muutoshistorioineen sekä käsittelysopimuksen ohjeistusehto. Kysymys toimittajalle: voimmeko korjata tallenteita itse, ja kirjataanko jokainen muutos jäljitettävästi?				
	Avoim	Kesken	Täytetty	Ei koske	
Näyttö / perustelu					
8.13	Henkilötietojen eheys on suojattu tallennuksessa, siirrossa ja palautuksessa. Varmuuskopiot ovat olemassa ja niiden palautettavuus on testattu.				
	Mistä sen tunnistaa: Näyttönä ovat varmuuskopioinnin konfiguraatio, tarkistussumma- tai eheysmekanismi ja vähintään yksi dokumentoitu palautustesti vuodessa päiväyksineen ja tuloksineen. Kysymys toimittajalle: kuinka usein testaatte palautuksia, ja mihin palautumisaikaan sitoudutte palvelutasossa?				
	Avoim	Kesken	Täytetty	Ei koske	
Näyttö / perustelu					

A.8 Avoimuus, läpinäkyvyys ja tiedottaminen

2

A.8.1	Henkilötietoja käsittelevien alihankkijoiden käyttö kerrotaan ennen sopimuksen tekemistä. Luettelon muutoksista ilmoitetaan asiakkaalle hyvissä ajoin, jotta asiakas voi vastustaa niitä tai irtisanoa sopimuksen.				Asiakirja
	Mistä sen tunnistaa: Näyttönä on ajantasainen luettelo alikäsittelijöistä, julkaistuna tai sopimuksessa saataville annettuna, sisältäen nimen, maan ja käsittelyn tarkoituksen, sekä ilmoitussääntö GDPR:n artiklan 28 kohdan 2 mukaisesti. Kysymys toimittajalle: mistä löydämme alikäsittelijäluettelonne, kuinka paljon etukäteen ilmoitatte muutoksista, ja miten voimme vastustaa niitä?				
	Avoim	Kesken	Täytetty	Ei koske	
Näyttö / perustelu					
A.8 (Grund)	Ennen sopimuksen tekemistä tarjoaja antaa saataville ymmärrettävää tietoa siitä, miten henkilötietoja käsitellään, mitä suojauksia on käytössä ja millä lainkäyttöalueilla käsittely tapahtuu.				
	Mistä sen tunnistaa: Näyttönä ovat tietosuojaseloste, tietoturvakuvauus, luottamuskeskuksen sivu ja käsittelysopimus, jonka liitteenä ovat tekniset ja organisatoriset toimenpiteet. Kysymys toimittajalle: toimittakaa ajantasainen luettelo teknisistä ja organisatorisista toimenpiteistä sopimusliitteenä, ei pelkkää markkinointiaineistoa.				
	Avoim	Kesken	Täytetty	Ei koske	
Näyttö / perustelu					

A.9 Yksilön osallistuminen ja tiedonsaanti

2

A.9 (Grund) Palvelu antaa pilvipalvelun asiakkaalle tekniset keinot hoitaa rekisteröityjen tarkastus-, oikaisu- ja poistopyynnöt itse, esimerkiksi vienti-, haku- ja poistotoiminnoilla.

Mistä sen tunnistaa: Näyttönä on vienti- ja poistotoimintojen tuotedokumentaatio, jota tukee sisäinen koeajo: yksi tarkastuspyyntö käydään läpi alusta loppuun ja kirjataan, kauanko siihen kuluu. Kysymys toimittajalle: voimmeko löytää, viedä ja poistaa yhtä henkilöä koskevat tiedot ilman tukeanne?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

5.34 Jos asiakas ei voi hoitaa rekisteröidyn pyyntöä itse, tarjoaja avustaa sovitun ajan kuluessa. Pyynnöt, jotka rekisteröidyt lähettävät suoraan tarjoajalle, välitetään asiakkaalle sen sijaan, että tarjoaja vastaisi niihin.

Mistä sen tunnistaa: Näyttönä on käsittelysopimuksen vastaava ehto konkreettisine vastausmääräaikoineen sekä tukitietojen historia todellisena esimerkkinä. Kysymys toimittajalle: mihin määräaikaan sitoudutte rekisteröityjen oikeuksien avustamisessa, ja mitä se maksaa?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.10 Vastuuvollisuus

4

A.10.1 Henkilötietoihin kohdistuvista loukkauksista ilmoitetaan pilvipalvelun asiakkaalle ilman aiheetonta viivytystä, ja ilmoituksessa kerrotaan laajuus, kohteena olevat tiedot, syy ja tehdyt toimenpiteet. Ilmoitusprosessi vastuineen ja määräaikoineen on määritelty.[Asiakirja](#)

Mistä sen tunnistaa: Näyttönä ovat tapahtumien käsittelysuunnitelma eskalointiketjuineen, sopimuksessa sovittu ilmoitusmääräaika (käytännössä toimiva määräaika on 24 tunnista 48 tuntiin, jotta asiakas ehtii vielä GDPR:n artiklan 33 mukaiseen 72 tunnin määräaikaan) ja tallenteet aiemmista tapahtumista tai harjoituksesta. Kysymys toimittajalle: minkä ajan kuluessa ilmoitatte tapahtumasta, mitä kanavaa pitkin, ja mitä tietoja annatte sen mukana?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.10.2 Tietoturvapoliitikat, toimintamenettelyt ja niihin liittyvät tallenteet säilytetään määritellyn ajan, jotta käsittely voidaan jälkikäteen selvittää.[Asiakirja](#)

Mistä sen tunnistaa: Näyttönä on säilytysääntö sekä politiikkojen versiohistoria, esimerkiksi asiakirjarekisterin tai versionhallintajärjestelmän kautta hyväksymispäivineen. Kysymys toimittajalle: kuinka kauan säilytätte politiikkojen versiot ja niihin liittyvät tallenteet, ja saammeko niihin pääsyn auditoinnin yhteydessä?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.10.3 Henkilötietojen palauttamisesta, siirtämisestä ja tuhoamisesta sopimuksen päättyessä on määritelty järjestely, jossa nimetään muodot, määräajat ja kopioiden käsittely.[Asiakirja](#)

Mistä sen tunnistaa: Näyttönä on käsittelysopimuksen päättymisehto sekä poistovahvistus sopimuksen päättyttyä. Kysymys toimittajalle: missä muodossa ja minkä ajan kuluessa saamme tietomme takaisin, milloin kaikki kopiot tuhotaan, ja saammeko siitä kirjallisen vahvistuksen?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

5.35 Suojausten vaikuttavuus katselmoidaan riippumattomasti määräajoin, esimerkiksi sisäisillä auditoinneilla, tunkeutumistesteillä tai kolmannen osapuolen varmennusraporteilla. Tulokset annetaan pilvipalvelun asiakkaan saataville sopivassa muodossa.

Mistä sen tunnistaa: Näyttönä on standardin ISO/IEC 27001 mukainen sertifikaatti, jonka soveltuvuuslausunto sisältää standardin ISO/IEC 27018 hallintakeinot, tai SOC 2 -raportti, yhdessä ajantasaisten tunkeutumistestien yhteenvetojen kanssa. Kysymys toimittajalle: toimittakaa sertifikaatti, sen soveltamisala ja vahvistus siitä, että ISO/IEC 27018 näkyy soveltuvuuslausunnossa. Kannattaa tarkistaa, kattaako soveltamisala todella käytössä olevan palvelun.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.11 Tietoturvaluuusu					13
A.11.1	Jokainen, jolla on pääsy henkilötietoihin, on salassapitovelvollinen riippumatta siitä, onko hän suoraan palkattu vai ulkopuolinen.				Asiakirja
Mistä sen tunnistaa: Näyttönä ovat allekirjoitetut salassapitosopimukset tai sitoumukset, jotka pysyvät voimassa tehtävän päätyttyä. Kysymys toimittajalle: onko koko henkilöstö ja kaikki palveluntarjoajat, joilla on pääsy tietoihin, velvoitettu kirjallisesti salassapitoon?					
Näyttö / perustelu					
A.11.2	Henkilötietoja sisältäviä tulosteita ja muita paperikopioita tehdään vain silloin, kun se on ehdottoman välttämätöntä. Sallitusta laajuudesta on sääntö.				
Mistä sen tunnistaa: Näyttönä on tulosteiden käsittelyä koskeva sääntö, joka konesaleissa on tyypillisesti täydellinen tulostuskielto alueilla, joilla on asiakastietoja. Kysymys toimittajalle: tulostetaanko asiakastietoja lainkaan toiminnassanne, ja jos tulostetaan, millä ehdoilla?					
Näyttö / perustelu					
A.11.3	Palautukset varmuuskopioista hyväksytään etukäteen ja kirjataan lokiin, mukaan lukien palautuksen käynnistänyt henkilö ja tiedot, joita palautus koski.				Asiakirja
Mistä sen tunnistaa: Näyttönä on palautusloki aikaleimoinen, aloittajineen ja laajuuksineen, jonka varmuuskopiointityökalu yleensä tuottaa automaattisesti. Kysymys toimittajalle: kirjaatko jokaisen palautuksen lokiin, ja voimmeko tarkastella näitä lokeja auditoinnin yhteydessä?					
Näyttö / perustelu					
A.11.4	Henkilötietoja sisältävät tallennusvälineet, jotka viedään toimitilojen ulkopuolelle, on suojattu luvattomalta pääsylvä ja katoamiselta, pääsääntöisesti salauksella ja kuljetuksen kirjauksella.				
Mistä sen tunnistaa: Näyttönä ovat osoitus salauksesta (koko tallennusvälineen salaus), kuljetus- ja luovutuskirjaukset sekä tallennusvälineiden luettelo. Kysymys toimittajalle: viedäänkö asiakastietoja sisältäviä tallennusvälineitä koskaan toimipaikkojenne ulkopuolelle, esimerkiksi varmuuskopioita varten, ja miten ne suojataan kuljetuksen aikana?					
Näyttö / perustelu					
A.11.5	Salaamattomien siirrettävien tallennusvälineiden ja laitteiden käyttö henkilötietoihin on kielletty tai rajattu perusteltuihin poikkeuksiin, joilla on dokumentoitu hyväksyntä.				
Mistä sen tunnistaa: Näyttönä on siirrettäviä tallennusvälineitä koskeva politiikka sekä sen tekninen pakottaminen, esimerkiksi pakotettu laitesalaus tai laitehallinnan kautta estetyt USB-portit. Kysymys toimittajalle: voiko henkilöstö kopioida asiakastietoja salaamattomiin laitteisiin, ja mikä estää sen teknisesti?					
Näyttö / perustelu					
A.11.6	Julkisissa verkoissa siirrettävät henkilötiedot salataan. Käytössä olevat mekanismit vastaavat nykyistä tekniikan tasoa.				
Mistä sen tunnistaa: Näyttönä ovat TLS-konfiguraatio (ajantasainen protokollaversio, ei vanhentuneita salausmenetelmiä) ja ulkoinen konfiguraatiotesti raporttina. Pienelle yritykselle käytännöllistä: maksuton TLS-tarkistus ajetaan kerran vuodessa ja tulos arkistoidaan. Kysymys toimittajalle: minkä siirtosalauksen pakotatte, ja onko levossa olevan tiedon salaus käytössä?					
Näyttö / perustelu					
A.11.7	Henkilötietoja sisältävät paperiset tallenteet tuhotaan tavalla, joka sulkee pois niiden palauttamisen.				
Mistä sen tunnistaa: Näyttönä ovat riittävän turvallisuuatason silppurit tai tuhoamistodistukset palveluntarjoajalta, joka toimii standardin DIN 66399 tai vastaavan mukaisesti. Kysymys toimittajalle: miten tuhoatte asiakkaisiin liittyvät paperiset tallenteet, ja ovatko tuhoamistodistukset tallessa?					
Näyttö / perustelu					

A.11.8 Käyttäjätunnukset on annettu yksilöllisesti yhdelle henkilölle, eikä niitä anneta uudelleen tai jaeta. Jaettuja tunnuksia on vain perustelluissa poikkeuksissa, ja niihin liittyy lisäjäljitettävyys.

Mistä sen tunnistaa: Näyttönä on identiteettijärjestelmän käyttäjäluettelo ilman ryhmätunnuksia sekä sääntö, jonka mukaan ylläpitotyö tehdään henkilökohtaisella tunnuksella. Kysymys toimittajalle: työskenteleekö käyttöhenkilöstönne henkilökohtaisilla tunnuksilla, ja onko monivaiheinen tunnistautuminen pakollinen?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.11.9 Tarjoaja pystyy milloin tahansa kertomaan, mitkä henkilöt tai roolit saavat pääsyn henkilötietoihin, ja tämä yleiskuva on ajan tasalla.[Asiakirja](#)

Mistä sen tunnistaa: Näyttönä on rooleittain jäsennetty käyttöoikeuksien yleiskuva, jota tukee toistuva käyttöoikeuksien katselmointi päiväyksineen ja tuloksineen. Pienelle yritykselle riittää puolivuositainen käyttäjäluettelon vienti hyväksyntämerkintöineen. Kysymys toimittajalle: kuinka moni henkilöstöstänne pääsee tietoihinne, ja kuinka usein katselmoitte sen?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.11.10 Käyttäjätunnuksia hallitaan koko niiden elinkaaren ajan: luonti, muutos ja viivytyksetön poistaminen käytöstä, kun joku lähtee tai vaihtaa tehtävää.

Mistä sen tunnistaa: Näyttönä on perehdytys- ja lähtömenettely tarkistuslistoineen sekä lokit käytöstä poistetuista tunnuksista aikaleimoineen. Kysymys toimittajalle: minkä ajan kuluessa poistatte pääsyn lähteviltä työntekijöiltä, ja miten osoitatte sen?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.11.11 Tarjoajan tietoturva- ja tietosuojavelvoitteet on sovittu sopimuksessa, mukaan lukien tekniset ja organisatoriset toimenpiteet, asiakkaan ohjeiden sitovuus ja asiakkaan auditointioikeus.[Asiakirja](#)

Mistä sen tunnistaa: Näyttönä on allekirjoitettu GDPR:n artiklan 28 mukainen käsittelysopimus toimenpideliitteineen sekä auditointi- tai tiedonsaantioikeus. Kysymys toimittajalle: toimittakaa allekirjoitettu käsittelysopimus liitteineen, ei pelkkää viittausta yleisiin palveluehtoihin.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.11.12 Henkilötietoja käsittelevillä alihankkijoilla on vähintään samat velvoitteet kuin tarjoajalla itsellään. Niiden valinta ja jatkuva seuranta perustuu määriteltyyn prosessiin.

Mistä sen tunnistaa: Näyttönä on velvoitteiden siirtyminen alihankkijoiden sopimukseen (GDPR:n artiklan 28 kohta 4) ja päivätty toimittaja-arviointi. Kysymys toimittajalle: miten arvioitte alihankkijanne, ja mitä näyttöä vaaditte heiltä?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.11.13 Ennen tallennustilan uudelleenkäyttöä on varmistettu, ettei aiempien käyttäjien tietoja jää saataville, ei fyysisillä tallennusvälineillä eikä virtualisoiduissa ympäristöissä.

Mistä sen tunnistaa: Näyttönä ovat tallennustilan vapauttamisessa käytettävä tyhjennys- tai ylikirjoitusmenettely, tallennusvälineiden tuhoamisen tallenteet ja arkkitehtuuridokumentissa kuvattu asiakkaiden erottelu. Kysymys toimittajalle: miten varmistatte, ettei uudelleen käytettävässä tallennustilassa ole muiden asiakkaiden jäännöstietoja?

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

A.12 Tietosuojan vaatimustenmukaisuus

3

A.12.1 Maat, joissa henkilötietoja säilytetään ja käsitellään, on nimetty ja ne ovat pilvipalvelun asiakkaan tiedossa. Säilytyspaikkojen muutoksista ilmoitetaan.[Asiakirja](#)

Mistä sen tunnistaa: Näyttönä on tarjoajan yleiskuva toimipaikoista ja alueista sopimuksessa tai dokumentaatiossa sekä kuvakaappaus käytössä olevan palvelun alueasetuksesta. Kysymys toimittajalle: missä maissa tietomme ovat levossa, mistä maista niihin on pääsy esimerkiksi tuessa, ja voimmeko kiinnittää alueen?

Avoim Kesken Täytetty Ei koske

Näyttö / perustelu

A.12.2 Henkilötietojen siirrot kolmansiin maihin ovat tiedossa, perusteltuja ja asianmukaisten suojatoimien kattamia.[Asiakirja](#)

Mistä sen tunnistaa: Näyttönä ovat vakiosopimuslausekkeet tai riittävyyspäättös, joita tukee siirtovaikutusten arviointi, joka voi pienessä yrityksessä olla lyhyt: kohteena olevat tietoryhmät, kohdamaa, riski ja tehdyt lisätoimenpiteet. Kysymys toimittajalle: millä oikeusperusteella siirrätte tietoja kolmansiin maihin, ja mitä täydentäviä toimenpiteitä sovellatte?

Avoim Kesken Täytetty Ei koske

Näyttö / perustelu

5.31 Henkilötietojen käsittelyyn sovellettavat lakisääteiset ja sopimusperusteiset vaatimukset on tunnistettu ja pidetään ajan tasalla oikeustilan muuttuessa. Ristiriitaiset lainkäyttöalueet on arvioitu.

Mistä sen tunnistaa: Näyttönä on yleiskuva sovellettavista vaatimuksista (GDPR, kansalliset säännökset, toimialakohtaiset velvoitteet) vastuuhenkilöineen ja katselmointipäivineen. Pienessä yrityksessä riittää yhden sivun luettelo, joka katselmoidaan vuosittain. Kysymys toimittajalle: koskevatko teitä tai alihankkijoitanne lainkäyttöalueet, jotka sallivat viranomaisten pääsyn tietoihimme, ja miten käsittelette sen?

Avoim Kesken Täytetty Ei koske

Näyttö / perustelu