

ISO/IEC 27018:2025, Informatiebeveiliging, cybersecurity en privacybescherming:  
Richtlijnen voor de bescherming van persoonsgegevens (PII) in publieke clouds die  
optreden als PII-verwerker (3e editie, 2025-08)

Bescherming van persoonsgegevens in de publieke cloud

36 eisen. Voor deze norm bestaat geen geaccrediteerd certificaat. Versie van 07/2026.

ISO/IEC 27018 is geen managementsysteemnorm, maar een verzameling richtlijnen met aanvullende beheersmaatregelen bovenop ISO/IEC 27002:2022. Er bestaat geen zelfstandig geaccrediteerd certificaat voor ISO/IEC 27018. De beheersmaatregelen worden opgenomen in de Verklaring van Toepasselijkheid van een ISO/IEC 27001-systeem, en het certificaat wordt vervolgens afgegeven op basis van ISO/IEC 27001 met een verwijzing naar ISO/IEC 27018. De norm richt zich op de aanbieder van een publieke clouddienst die persoonsgegevens verwerkt namens de klanten van die clouddienst. Een organisatie die uitsluitend clouddiensten afneemt, vervult die rol niet en doet er verstandig aan de eisen te toetsen aan haar leveranciers, niet aan zichzelf. Voor Leanshift is deze checklist daarom vooral een beoordelingskader voor leveranciers. Elk punt kan als vraag aan de leverancier worden voorgelegd en worden geborgd via de verwerkersovereenkomst op grond van artikel 28 AVG. Het resultaat van een dergelijke beoordeling is een intern conformiteitsdossier of een beoordelingsprofiel van de leverancier, geen certificaat. Over de nummering: de paragrafen A.2 tot en met A.12 volgen de privacybeginselen uit bijlage A van de norm, punten genummerd zoals A.11.6 zijn de daar genoemde aanvullende beheersmaatregelen. Punten genummerd zoals 8.10 of 5.34 verwijzen naar beheersmaatregelen uit ISO/IEC 27002:2022 die de norm specifiek maakt voor de cloud. Punten met de toevoeging "(Grundsatz)", wat beginsel betekent, zijn afgeleid van het beginsel van de paragraaf zelf, in gevallen waarin bijlage A geen aparte aanvullende beheersmaatregel bevat.

Bedrijf

Datum

Opgesteld door

A.2 Toestemming en keuze

2

Document

A.2.1

**De aanbieder van de clouddienst ondersteunt de klant van de clouddienst bij het nakomen van de rechten van betrokkenen, zoals inzage, rectificatie, verwijdering en bezwaar. Verantwoordelijkheden en termijnen zijn contractueel vastgelegd.**

Waarvan je het vaststelt: Als bewijs geldt de verwerkersovereenkomst op grond van artikel 28 AVG met een clause over bijstand bij de rechten van betrokkenen, samen met de technische middelen binnen de dienst zelf: functies voor export, correctie en verwijdering, of een gedocumenteerde ondersteuningsprocedure met een reactietermijn. Vraag aan de leverancier: welke functie of procedure biedt u aan zodat wij een verzoek om inzage of verwijdering binnen een maand kunnen afhandelen?

Open

In behandeling

Voldaan

Niet van toepassing

Bewijs / onderbouwing

A.2 (Grundsatz)

**Persoonsgegevens van klanten van de clouddienst worden uitsluitend verwerkt op basis van de gedocumenteerde instructies van de klant. Het verkrijgen van toestemming van betrokkenen blijft de taak van de klant als verwerkingsverantwoordelijke, en de leverancier loopt daar niet op vooruit.**

Waarvan je het vaststelt: Als bewijs geldt de instructieclause in de verwerkersovereenkomst plus het bewijs dat de leverancier geen secundair gebruik maakt van de gegevens, bijvoorbeeld de privacyverklaring van de dienst en de productdocumentatie. Vraag aan de leverancier: verwerkt u onze klantgegevens op enige wijze buiten onze instructies om, bijvoorbeeld voor productverbetering of het trainen van modellen?

Open

In behandeling

Voldaan

Niet van toepassing

Bewijs / onderbouwing

A.3 Rechtmatigheid en specificatie van het doel

2

Document

A.3.1

**Het doel waarvoor de leverancier persoonsgegevens verwerkt, is beperkt tot het leveren van de overeengekomen dienst en is in het contract vastgelegd. Er vindt geen verwerking plaats voor eigen doeleinden van de leverancier.**

Waarvan je het vaststelt: Als bewijs geldt de verwerkersovereenkomst waarin onderwerp, aard, doel en duur van de verwerking zijn vastgelegd, evenals de categorieën betrokkenen conform artikel 28 lid 3 AVG. Vraag aan de leverancier: lever de contractbijlage aan die het verwerkingsdoel uitputtend beschrijft. Voor kleine organisaties volstaat de standaard verwerkersbijlage van de leverancier, mits deze informatie erin staat.

Open

In behandeling

Voldaan

Niet van toepassing

Bewijs / onderbouwing

**A.3.2 Persoonsgegevens die aan de leverancier zijn toevertrouwd, worden niet gebruikt voor reclame, marketing of andere commerciële doeleinden van de leverancier zonder voorafgaande uitdrukkelijke toestemming. De levering van de dienst wordt niet afhankelijk gemaakt van die toestemming.**

Waarom je het vaststelt: Als bewijs geldt een expliciete contractclausule die commercieel secundair gebruik uitsluit, samen met de servicevoorwaarden. Vraag aan de leverancier: bevestig schriftelijk dat klantgegevens niet worden gebruikt voor reclame, profilering of het trainen van AI-modellen. Ontbreekt die toezegging, dan is de dienst ongeschikt voor persoonsgegevens.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.4 Beperking van de verzameling****1****A.4 (Grondslagen) Naast de gegevens die de klant in de dienst invoert, verzamelt de leverancier geen aanvullende persoonsgegevens voor eigen doeleinden, zoals telemetrie, gebruiksprofielen of contentanalyse. Operationele gegevens en metagegevens die worden verzameld, zijn benoemd en onderbouwd.**

Waarom je het vaststelt: Als bewijs geldt een lijst van de gegevens die de dienst naast de inhoudelijke gegevens vastlegt (toegangslogs, telemetrie, diagnostische gegevens) met doel en bewaartermijn, plus een schermafbeelding van de instelling waarmee optionele telemetrie kan worden uitgeschakeld. Vraag aan de leverancier: welke gebruiks-, telemetrie- en diagnostische gegevens verzamelt u daarnaast, waarvoor gebruikt u ze, en kunnen wij die verzameling uitschakelen?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.5 Minimalisatie van gegevens****2****A.5.1 Tijdelijke bestanden die tijdens de verwerking van persoonsgegevens ontstaan, zoals tijdelijke opslag, caches of rollbacklogboeken, worden binnen een vastgestelde termijn veilig verwijderd.**

Waarom je het vaststelt: Als bewijs geldt een operationele of verwijderingsprocedure met een vastgelegde bewaartermijn voor tijdelijke gegevens, onderbouwd door de systeemconfiguratie, bijvoorbeeld een cache-TTL of een geplande opschoontask met bijbehorend uitvoeringslogboek. Vraag aan de leverancier: na welke termijn worden caches, tijdelijke bestanden en tussentoestanden verwijderd, en hoe wordt dit gecontroleerd?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**8.11 Overal waar operaties, testen of ondersteuning geen live gegevens vereisen, worden persoonsgegevens gemaskeerd, gepseudonimiseerd of geanonimiseerd. De hoeveelheid verwerkte gegevens blijft beperkt tot wat de dienst daadwerkelijk nodig heeft.**

Waarom je het vaststelt: Als bewijs geldt een vastgelegde regel over welke omgevingen live gegevens mogen zien, plus schermafbeeldingen of scripts van de maskering die in test- en ontwikkelsystemen wordt toegepast. Vraag aan de leverancier: werken uw ondersteunings- en ontwikkelteams met productiegegevens en, zo ja, onder welke waarborgen? Voor kleine organisaties volstaat een regel dat testsystemen uitsluitend draaien op gegenereerde voorbeeldgegevens.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.6 Beperking van gebruik, bewaring en verstrekking****3****A.6.1 Wanneer de leverancier een juridisch bindend verzoek ontvangt om persoonsgegevens te verstrekken, bijvoorbeeld van een overheidsinstantie, informeert hij de klant van de clouddienst vooraf, voor zover de wet dit toestaat.**

Waarom je het vaststelt: Als bewijs geldt een contractuele kennisgevingsclausule en een intern proces voor verzoeken van instanties met een aangewezen eigenaar. Vraag aan de leverancier: informeert u ons voordat gegevens worden overgedragen, en publiceert u een transparantierapport over verzoeken van instanties? Een actueel transparantierapport is een sterk bewijs.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

## A.6.2 Wanneer de leverancier persoonsgegevens aan derden verstrekt, legt hij dit vast zodat het traceerbaar is: wie de gegevens heeft ontvangen, wanneer dit gebeurde, om welke gegevens het ging en op welke grondslag de verstrekking berust. Document

Waarvan je het vaststelt: Als bewijs geldt een verstrektingsregister of ticketgeschiedenis met die velden, ook als het geen vermeldingen bevat. Een leeg maar bijgehouden register is aanvaardbaar en is de praktische route voor kleine organisaties. Vraag aan de leverancier: houdt u een register van gegevensverstrekkingen bij, en kunnen wij daar uittreksels van krijgen?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

## 8.10 Persoonsgegevens worden verwijderd zodra de overeengekomen bewaartermijn verstrijkt of het contract eindigt, met inbegrip van kopieën in back-ups na hun rotatiecyclus.

Waarvan je het vaststelt: Als bewijs geldt een verwijderingsconcept met bewaartermijnen per gegevenscategorie, de bewaartermijn van back-ups en een verwijderingslogboek of verwijderingsbevestiging. Vraag aan de leverancier: hoe lang blijven onze gegevens in uw back-ups bestaan na beëindiging, en ontvangen wij een schriftelijke bevestiging van de verwijdering?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

## A.7 Juistheid en kwaliteit

2

### A.7 (Grondslagen) De leverancier wijzigt de aan hem toevertrouwde persoonsgegevens niet op eigen initiatief. Correcties en updates worden uitsluitend uitgevoerd op instructie van de klant van de clouddienst of via functies die de klant zelf bedient.

Waarvan je het vaststelt: Als bewijs gelden de bewerkingfuncties van de dienst samen met de bijbehorende wijzigingsgeschiedenis, plus de instructieclausule in de verwerkersovereenkomst. Vraag aan de leverancier: kunnen wij records zelf corrigeren, en wordt elke wijziging vastgelegd zodat deze traceerbaar is?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

## 8.13 De integriteit van persoonsgegevens is beschermd tijdens opslag, verzending en herstel. Er zijn back-ups aanwezig en de herstelbaarheid daarvan is getest.

Waarvan je het vaststelt: Als bewijs gelden de back-upconfiguratie, checksum- of integriteitsmechanismen, en ten minste één gedocumenteerde hersteltest per jaar met datum en resultaat. Vraag aan de leverancier: hoe vaak test u herstelacties, en welke hersteltijd garandeert u in het serviceniveau?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

## A.8 Openheid, transparantie en kennisgeving

2

### A.8.1 Het inzetten van subverwerkers die persoonsgegevens verwerken, wordt bekendgemaakt voordat het contract wordt gesloten. Wijzigingen in de lijst worden tijdig aan de klant gemeld, zodat de klant bezwaar kan maken of het contract kan beëindigen. Document

Waarvan je het vaststelt: Als bewijs geldt een actuele lijst van subverwerkers, gepubliceerd of contractueel beschikbaar gesteld, met naam, land en verwerkingsdoel, plus een kennisgevingsregel conform artikel 28 lid 2 AVG. Vraag aan de leverancier: waar vinden wij uw lijst van subverwerkers, hoeveel tijd van tevoren meldt u wijzigingen, en hoe kunnen wij bezwaar maken?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

### A.8 (Grondslagen) Vooraf dat het contract wordt gesloten, stelt de leverancier begrijpelijke informatie beschikbaar over hoe persoonsgegevens worden verwerkt, welke waarborgen aanwezig zijn en in welke rechtsgebieden de verwerking plaatsvindt.

Waarvan je het vaststelt: Als bewijs gelden de privacyverklaring, een whitepaper over beveiliging, een trustcenter-pagina en de verwerkersovereenkomst met de technische en organisatorische maatregelen als bijlage. Vraag aan de leverancier: lever de actuele lijst van technische en organisatorische maatregelen aan als contractbijlage, niet alleen als marketingmateriaal.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.9 Participatie en toegang van de betrokkene**

2

**A.9 (Grondslagen) De dienst biedt de klant van de clouddienst de technische middelen om verzoeken om inzage, rectificatie en verwijdering van betrokkenen zelfstandig af te handelen, bijvoorbeeld via functies voor export, zoeken en verwijderen.**

Waarvan je het vaststelt: Als bewijs geldt de productdocumentatie van de export- en verwijderfuncties, onderbouwd door een interne proefdoorloop: werk een verzoek om inzage volledig af en noteer hoe lang dit duurt. Vraag aan de leverancier: kunnen wij alle gegevens over één individuele persoon vinden, exporteren en verwijderen zonder uw ondersteuning?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**5.34 Wanneer de klant een verzoek van een betrokkene niet zelf kan afhandelen, verleent de leverancier binnen een overeengekomen termijn bijstand. Verzoeken die betrokkenen rechtstreeks naar de leverancier sturen, worden doorgestuurd naar de klant in plaats van door de leverancier te worden beantwoord.**

Waarvan je het vaststelt: Als bewijs geldt de betreffende clausule in de verwerkersovereenkomst met een concrete reactietermijn, plus een geschiedenis van supporttickets als praktijkvoorbeeld. Vraag aan de leverancier: welke termijn garandeert u voor bijstand bij de rechten van betrokkenen, en wat kost dit?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**A.10 Verantwoordingsplicht**

4

**A.10.1 Inbreuken in verband met persoonsgegevens worden zonder onnodige vertraging gemeld aan de klant van de clouddienst, met vermelding van de omvang, de betrokken gegevens, de oorzaak en de genomen maatregelen. Er is een meldproces vastgesteld met verantwoordelijkheden en termijnen.**[Document](#)

Waarvan je het vaststelt: Als bewijs gelden het incidentresponsplan met de escalatieketen, de contractuele meldtermijn (24 tot 48 uur werkt in de praktijk goed, zodat de klant nog kan voldoen aan de termijn van 72 uur uit artikel 33 AVG) en registraties van eerdere incidenten of van een oefening. Vraag aan de leverancier: binnen welke termijn meldt u een incident, via welk kanaal, en welke informatie levert u daarbij aan?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**A.10.2 Beveiligingsbeleid, operationele procedures en de bijbehorende registraties worden gedurende een vastgestelde termijn bewaard, zodat de verwerking achteraf kan worden gereconstrueerd.**[Document](#)

Waarvan je het vaststelt: Als bewijs geldt een bewaarregel met de versiegeschiedenis van het beleid, bijvoorbeeld via een documentenregister of een versiebeheersysteem met de goedkeuringsdatum. Vraag aan de leverancier: hoe lang bewaart u beleidsversies en de bijbehorende registraties, en krijgen wij daar toegang toe bij een audit?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**A.10.3 Er bestaat een vastgestelde regeling voor de teruggave, overdracht en vernietiging van persoonsgegevens bij het einde van het contract, met vermelding van formaten, termijnen en de behandeling van kopieën.**[Document](#)

Waarvan je het vaststelt: Als bewijs geldt de exitclausule in de verwerkersovereenkomst plus een verwijderingsbevestiging na afloop van het contract. Vraag aan de leverancier: in welk formaat en binnen welke termijn krijgen wij onze gegevens terug, wanneer worden alle kopieën vernietigd, en ontvangen wij een schriftelijke bevestiging?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**5.35 De effectiviteit van de waarborgen wordt op gezette tijden onafhankelijk beoordeeld, bijvoorbeeld via interne audits, penetratietests of assurancerapporten van derden. De resultaten worden in een geschikte vorm ter beschikking gesteld aan de klant van de clouddienst.**

Waaraan je het vaststelt: Als bewijs geldt een ISO/IEC 27001-certificaat met een Verklaring van Toepasselijkheid waarin de beheersmaatregelen van ISO/IEC 27018 zijn opgenomen, of een SOC 2-rapport, samen met actuele samenvattingen van penetratietests. Vraag aan de leverancier: lever het certificaat, de reikwijdte ervan en de bevestiging dat ISO/IEC 27018 is verwerkt in de Verklaring van Toepasselijkheid. Controleer of de reikwijdte daadwerkelijk de gebruikte dienst omvat.

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

## A.11 Informatiebeveiliging

13

**A.11.1 Iedereen met toegang tot persoonsgegevens is gebonden aan geheimhouding, ongeacht of het gaat om eigen personeel of extern ingehuurd krachten.**

[Document](#)

Waaraan je het vaststelt: Als bewijs gelden ondertekende geheimhoudingsovereenkomsten of -verklaringen die van kracht blijven na afloop van de werkkrelatie. Vraag aan de leverancier: zijn alle medewerkers en dienstverleners met toegang tot gegevens schriftelijk gebonden aan geheimhouding?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**A.11.2 Afdrukken en andere papieren kopieën met persoonsgegevens worden alleen gemaakt wanneer dat strikt noodzakelijk is. De toegestane omvang is vastgelegd in een regel.**

Waaraan je het vaststelt: Als bewijs geldt een regel over de omgang met afdrukken, wat in datacenters doorgaans neerkomt op een algeheel afdrukverbod in ruimtes waar klantgegevens worden verwerkt. Vraag aan de leverancier: worden klantgegevens in uw bedrijfsvoering überhaupt afgedrukt, en zo ja, onder welke voorwaarden?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**A.11.3 Herstelacties vanuit back-ups worden vooraf geautoriseerd en vastgelegd, met vermelding van de persoon die het herstel heeft geïnitieerd en de betrokken gegevens.**

[Document](#)

Waaraan je het vaststelt: Als bewijs geldt het herstellogboek met tijdstempel, initiatiefnemer en omvang, doorgaans automatisch gegenereerd door de back-uptool. Vraag aan de leverancier: legt u elke herstelactie vast, en kunnen wij die logboeken inzien bij een audit?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**A.11.4 Gegevensdragers met persoonsgegevens die de locatie verlaten, zijn beschermd tegen ongeautoriseerde toegang en verlies, doorgaans via versleuteling en een transportregistratie.**

Waaraan je het vaststelt: Als bewijs gelden het bewijs van versleuteling (volledige versleuteling van de drager), transport- en overdrachtsregistraties, en een inventaris van gegevensdragers. Vraag aan de leverancier: verlaten gegevensdragers met klantgegevens ooit uw locaties, bijvoorbeeld voor back-ups, en hoe worden ze tijdens transport beschermd?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**A.11.5 Het gebruik van onversleutelde draagbare gegevensdragers en apparaten voor persoonsgegevens is verboden of beperkt tot gerechtvaardigde uitzonderingen met gedocumenteerde goedkeuring.**

Waaraan je het vaststelt: Als bewijs geldt een beleid voor verwisselbare gegevensdragers plus technische afdwinging, bijvoorbeeld verplichte apparaatversleuteling of geblokkeerde USB-poorten via devicebeheer. Vraag aan de leverancier: kan personeel klantgegevens kopiëren naar onversleutelde apparaten, en wat voorkomt dit technisch?

Open      In behandeling      Voldaan      Niet van toepassing

Bewijs / onderbouwing

**A.11.6 Persoonsgegevens die over openbare netwerken worden verzonden, zijn versleuteld. De gebruikte mechanismen weerspiegelen de actuele stand van de techniek.**

Waaraan je het vaststelt: Als bewijs gelden de TLS-configuratie (actuele protocolversie, geen verouderde ciphers) en een verslag van een externe configuratietest. Praktisch voor kleine organisaties: voer eenmaal per jaar een gratis TLS-scan uit en bewaar het resultaat. Vraag aan de leverancier: welke transportversleuteling schrijft u verplicht voor, en is versleuteling in rust actief?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.11.7 Papieren documenten met persoonsgegevens worden op een zodanige manier vernietigd dat reconstructie is uitgesloten.**

Waaraan je het vaststelt: Als bewijs gelden papiervernietigers met een passend beveiligingsniveau of vernietigingscertificaten van een dienstverlener die werkt volgens DIN 66399 of een gelijkwaardige norm. Vraag aan de leverancier: hoe vernietigt u papieren documenten met betrekking tot klanten, en worden vernietigingscertificaten bewaard?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.11.8 Gebruikers-ID's worden uniek aan één persoon toegekend en worden niet opnieuw uitgegeven of gedeeld. Gedeelde accounts bestaan alleen in gerechtvaardigde uitzonderingen en met aanvullende traceerbaarheid.**

Waaraan je het vaststelt: Als bewijs geldt een gebruikerslijst uit het identiteitssysteem zonder groepsaccounts, samen met de regel dat administratief werk wordt uitgevoerd onder een persoonlijk account. Vraag aan de leverancier: werkt uw operationeel personeel met persoonlijke accounts, en is multifactorauthenticatie verplicht?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.11.9 De leverancier kan te allen tijde aangeven welke personen of rollen toegang mogen hebben tot persoonsgegevens, en houdt dat overzicht actueel.**

Document

Waaraan je het vaststelt: Als bewijs geldt een overzicht van toegangsrechten per rol, onderbouwd door een periodieke toegangsbeoordeling met datum en resultaat. Voor kleine organisaties volstaat een halfjaarlijkse, geaccordeerde export van de gebruikerslijst. Vraag aan de leverancier: hoeveel van uw medewerkers hebben toegang tot onze gegevens, en hoe vaak beoordeelt u dit?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.11.10 Gebruikersaccounts worden beheerd over hun volledige levenscyclus: aanmaak, wijziging en directe deactivering wanneer iemand vertrekt of van functie verandert.**

Waaraan je het vaststelt: Als bewijs gelden een in- en uitdientstredingsprocedure met checklist, plus logbestanden van gedeactiveerde accounts met tijdstempels. Vraag aan de leverancier: binnen welke termijn trekt u de toegang in bij medewerkers die vertrekken, en hoe onderbouwt u dat?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.11.11 De beveiligings- en privacyverplichtingen van de leverancier zijn contractueel vastgelegd, met inbegrip van de technische en organisatorische maatregelen, de bindende werking van de instructies van de klant en het auditrecht van de klant.**

Document

Waaraan je het vaststelt: Als bewijs geldt de ondertekende verwerkersovereenkomst op grond van artikel 28 AVG met de bijlage met maatregelen en een audit- of informatierecht. Vraag aan de leverancier: lever de ondertekende verwerkersovereenkomst inclusief bijlagen aan, niet slechts een verwijzing naar algemene servicevoorwaarden.

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.11.12 Subverwerkers die persoonsgegevens verwerken, zijn ten minste onderworpen aan dezelfde verplichtingen als de leverancier zelf. Hun selectie en doorlopende monitoring verlopen volgens een vastgesteld proces.**

Waaraan je het vaststelt: Als bewijs geldt de doorwerking van verplichtingen in de contracten met subverwerkers (artikel 28 lid 4 AVG) en een leveranciersbeoordeling met datum. Vraag aan de leverancier: hoe beoordeelt u uw subverwerkers, en welk bewijs eist u van hen?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.11.13 Voordat opslagruimte opnieuw wordt gebruikt, wordt gewaarborgd dat er geen gegevens van eerdere gebruikers toegankelijk blijven, noch op fysieke gegevensdragers, noch in gevirtualiseerde omgevingen.**

Waaraan je het vaststelt: Als bewijs gelden de sanitisatie- of overschrijfprocedure die wordt toegepast bij het vrijgeven van opslag, registraties van vernietiging van gegevensdragers, en de scheiding tussen tenants zoals beschreven in het architectuurdokument. Vraag aan de leverancier: hoe waarborgt u dat hergebruikte opslag geen restgegevens van andere klanten bevat?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.12 Naleving op het gebied van privacy****3****A.12.1 De landen waarin persoonsgegevens worden opgeslagen en verwerkt, zijn benoemd en bekend bij de klant van de clouddienst. Wijzigingen in de opslaglocaties worden gemeld.**[Document](#)

Waaraan je het vaststelt: Als bewijs geldt het overzicht van locaties en regio's van de leverancier, in het contract of in de documentatie, plus een schermafbeelding van de regio-instelling van de gebruikte dienst. Vraag aan de leverancier: in welke landen staan onze gegevens in rust, vanuit welke landen wordt toegang verkregen, bijvoorbeeld bij support, en kunnen wij de regio vastleggen?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**A.12.2 Doorgiften van persoonsgegevens naar derde landen zijn bekend, onderbouwd en gedekt door passende waarborgen.**[Document](#)

Waaraan je het vaststelt: Als bewijs gelden standaardcontractbepalingen of een adequaatheidsbesluit, onderbouwd door een beoordeling van de gevolgen van de doorgifte, die voor kleine organisaties kort kan zijn: betrokken gegevenscategorieën, land van bestemming, risico, genomen aanvullende maatregelen. Vraag aan de leverancier: op welke rechtsgrondslag baseert u de doorgifte van gegevens naar derde landen, en welke aanvullende maatregelen past u toe?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing

**5.31 De wettelijke en contractuele eisen die van toepassing zijn op de verwerking van persoonsgegevens zijn geïdentificeerd en worden actueel gehouden naarmate de wettelijke situatie verandert. Conflicterende rechtsgebieden worden beoordeeld.**

Waaraan je het vaststelt: Als bewijs geldt een overzicht van de toepasselijke eisen (AVG, nationale regelgeving, sectorspecifieke verplichtingen) met een eigenaar en een beoordelingsdatum. In een kleine organisatie volstaat een eenvoudige, jaarlijks beoordeelde lijst van een pagina. Vraag aan de leverancier: bent u of uw subverwerkers onderworpen aan rechtsgebieden die instanties toegang tot onze gegevens geven, en hoe gaat u daarmee om?

Open In behandeling Voldaan Niet van toepassing

Bewijs / onderbouwing