ISO 27018 security standaard

# Wat is ISO 27018

In augustus 2014 heeft International Organization for Standardization’ (ISO), in samenwerking met Electrotechnical Commssion’ (IEC), ISO 27018 vastegesteld doelend op privacy voor public Cloud service providers in de rol van een bewerker.

# Wat is de bijdrage van ISO 27018 aan Cloud Governance?

Deze standaard is gericht op publieke cloud levernanciers dat functioneert als verwerker van persoonsgegevens. De belangrijkste voordelen van ISO 27018 zijn dat het richtlijnen biedt voor de bescherming van persoonsgegevens in de Cloud en organisaties kan helpen aantonen dat zij voldoen aan de regelgeving omtrent gegevensbescherming. Het kan ook helpen de veiligheid van clouddiensten te verbeteren en vertrouwen op te bouwen tussen organisaties en hun klanten (ISO 27017 and ISO 27018 , 2022).

Omveilig om te gaan met persoonsgegevens in de cloud is het belangrijke om de volgende zaken goed geregeld te hebben in de Cloud:

1. **Voer een sterk wachtwoordbeleiden in**

Zorg ervoor dat het bedrijf alleen sterke wachtwoorden toestaat en dat deze niet worden hergebruikt. Deze best practice voorkomt dat iemand toegang krijgt tot de persoonsgegevens in de Cloud.

1. **Encrypt de data**

Encryptie is een belangrijke stap om de persoonsgegevens te beveiligen. Gebruik aanbevolen encryptie-algoritmen en robuust sleutelbeheer bijvoorbeeld sha-256, sha-512.

1. **Tokeniseer persoonsgegevens**

Dit werkt door de persoonsgegevens te koppelen aan een token (dat bijvoorbeeld een special unieke tekenreeks) dat op niets betekent. Deze token sla je op in plaats van de gegevens. Als de token uitlekt, moet de aanvaller zijn deel, de persoonsgegevens, zien te bemachtigen. De daadwerkelijke informatie wordt echter meestal opgeslagen in een tokenbeheerder die de gegevens alleen bekendmaakt aan bevoegden.

1. **Bewaar alleen noodzakelijke informatie**

Een andere voor de hand liggende manier om gegevens geheim te houden is ze gewoon niet op te slaan. Zorg ervoor dat er geen niet-belangrijke persoonsgegevens bewaard worden en voer ze correct af.

1. **Wees compliant met de ‘The Least Privilege’ principe**

Zorg ervoor dat geen enkele werknemer meer rechten heeft dan nodig is. Dit helpt de te voorkomen dat persoonsgegevens door iedereen gezien kan worden en beperkt zicht tot een minimum. Hierrdoor de veiligheid vergroot je de veiligheid. (Lupsan, 2022)

# Is het compleet, dat wil zeggen: Worden alle aspecten die met Governance te maken hebben afgedekt?

Nee, niet alle aspecten van Cloud governance worden hiermee afgedekt. De ISO standaard 27018 valt onder de categorie beveiliging van het van Governance model. Wat er precies word beveiligd zijn persoonsgegevens van klanten die in de Cloud werken. Het is daarom zeer belangrijk om zorgvuldig om te gaan met deze informatie. Het aantonen van uitgebreide gegevensbescherming (door te werken met cloudserviceproviders die ISO 27018 volgen), zullen zij eerder geneigd zijn zaken met je te doen.

(Nunn, 2021) Voor cloud service providers kun je gemakkelijker deals sluiten met potentiële klanten omdat je kan zeggen: "Wij volgen de meest uitgebreide gegevenscontroles."

# Wat zijn de sterke punten en wat is minder goed?

## Versterkt vertrouwen van de klant

De sterke punten zijn dat je kan aantonen naar klanten dat je zorgvuldig en vertrouwd omgaat met persoonsgegevens. Dit creert vetrouwensrelaties op tussen consument en aanbieder. klanten doen dan meer zaken met jou als aanbieder. dit kan leiden tot meer innovatie, meer focus op businessdoelen en meer service leveren aan klanten.

Een ander voordeel van deze standaar is dat hij wereldwijd erkent is.

## Verbeterde wereldwijde partnerschap

Door aan te tonen dat je ISO 27018 compliant bent, vergroot je de kans om zaken te doen met het buitenland. Dit komt omdat de meeste landen ook compliant zijn met deze standaard, waardoor het makkelijker is om contracten te tekenen.

## Betere beveiliging en rechtsbescherming

Het voldoen aan 27018 vormt een basisbeveiliging voor elk bedrijf dat gegevens in de cloud verwerkt. Bovendien zijn de controles bestand tegen audits, klantonderzoeken en overheidsbeoordelingen. Met deze normen kunnen beveiligingsrisico's ingeperkt worden en het bedrijf beschermen tegen beschuldigingen van nalatigheid of roekeloosheid als zich een inbreuk voordoet.

Op beschuldigingen van nalatigheid staan zware straffen. Maar bedrijven die aantonen dat zij een op risico's gebaseerd kader hebben en beveiligingscontroles volgen, kunnen dat gebruiken als bewijs in een rechtszaak. Helaas zijn inbreuken altijd mogelijk. Door 27018 te volgen, is de kans dat het gebeurt kleiner en de schade meer beperkt als het toch gebeurt.

Voor bedrijven die clouddiensten gebruiken, laat het werken met een gecertificeerd bedrijf zien dat er essentiële stappen genomen worden om de gegevens van gebruikers te beschermen. (ISO 27018: How to protect PII in public clouds, 2023)

## Wat is minder goed.

Er moet wel rekening worden gehouden dat het bedrijf verantwoordelijk blijft voor de beveiliging van de persoonsgegevens die identificeert worden.

Verlaat niet meteen de cloud provider omdat deze nog geen compliance certificaat heeft. Een cloud provider kan aan de meeste of alle bepalingen van ISO 27018 voldoen in overeenkomst met hen en nog niet formeel zijn geaudit. (Gibson, 2015)

# Wat doen de grote public cloud providers eigenlijk met deze standaard/framework? Conformeren zij zich hieraan?

De bekende Public Cloud providers voldoen aan deze standaard. Ze zijn natuurlijk wereldwijk actief en willen hun diensten zoveel mogelijk spreiden en veel klanten binnenhalen. Het is dan vanzelfsprekend dat de grote Cloudproviders (Amazon AWS, Microsoft Azure en Google Cloud Platform) ISO 27018 compliant zijn.

De providers worden regelmatig gecontroleerd of ze voldoen aan de wet en regelgeving m.b.t. de standaard. Onafhankelijke partijen beoordeelt een provider en bepaald op deze manier of zij compliant is of niet.

(ISO/IEC 27018:2019 Compliance, 2023) EY CertifyPoint. Dit is een ISO-certificeerder die is geaccrediteerd door de Raad voor Accreditatie, lid van het International Accreditation Forum (IAF). Certificaten uitgegeven door EY CertifyPoint worden erkend als geldige certificaten in alle landen met een IAF-lid.