ISO 27017 en de 27018

Organisaties die clouddiensten aanbieden (Infrastructuur- of Platform- of Software als een Service) én de afnemers van deze clouddiensten, willen steeds meer aanvullende garanties dat hun gegevens echt goed beveiligd zijn. Met de ISO 27017 en ISO 27018 certificeringen van de partners van 12secure-U kunnen bedrijven exact dat aantonen. De beide normen zijn bedoeld voor clouddiensten, waarmee aangetoond wordt dat de beveiliging van informatie in de cloud goed is geborgd.

Context

De ISO 27001 beschrijft de eisen van een managementsysteem voor informatiebeveiliging. In deze norm wordt verwezen naar de Annex A beheersmaatregelen. Deze zijn verder uitgewerkt in de ISO 27002. De ISO 27017 en ISO 27018 zijn gebaseerd op de ISO 27002. De normen zijn echter verschillend en hebben een andere bedoeling. De normen zorgen er niet alleen voor dat de Cloud Service Providers de data van de klanten goed beschermen, maar geven ook belangrijke verplichtingen om te communiceren met de klanten in het geval van problemen. Daarnaast moet er een contract aanwezig zijn waarin vastgesteld wordt dat de data beveiligd blijft en de provider alleen met toestemming van de klant toegang kan krijgen tot die data.

ISO 27017 – Cloud beveiliging

De ISO 27017 stelt eisen aan de cloud-leveranciers maar ook aan de afnemers van deze clouddiensten. De norm bevat cloud-specifieke beheersmaatregelen, waarbij het niet uitmaakt wat voor soort gegevens er wordt verwerkt. De norm spreekt over “Cloud service customer” en over “Cloud service provider”. Er zijn specifieke- en generieke eisen voor de klant én provider vastgesteld. De ISO 27017 heeft 37 eisen aanvullend op de ISO27002 beheersmaatregelen en nog eens zeven extra maatregelen vastgesteld.

ISO 27018 – Privacy bescherming

De ISO 27018 is alleen bedoeld voor cloud aanbieders die persoonsgegevens verwerken (de norm noemt dit Personally Identifiable Information, PII) en richt zich op de beveiliging en behandeling van deze gegevens. Denk aan persoonlijke gegevens van klanten, gezondheids- en patiëntinformatie of informatie over burgers. Voor veel afnemers geeft een ISO27018 certificering van de clouddienst aanbieder extra zekerheid dat deze gevoelige data niet in verkeerde handen komt. De norm is ook gebaseerd op de ISO 27002, maar heeft een aanvullende set van beheersmaatregelen specifiek gericht op het beschermen van persoonsgegevens. Denk daarbij aan toestemming, gegevensminimalisatie en privacy klachten. Geheel in lijn met de eisen uit de AVG.

Voor welke norm certificeren?

De ISO27001 is de meest bekende en gevraagde norm waartegen wordt geaudit en gecertificeert onder accreditatie. Daarom wordt in contracten en aanbestedingen veelal naar de ISO 27001 gevraagd en niet naar de ISO 270017 of ISO 27018. Tóch zijn deze normen belangrijk voor organisaties die diensten in de cloud aanbieden en eindgebruikers van deze diensten. Meestal kiezen organisaties met clouddiensten een combinatie van ISO 27001 en ISO 27017. Organisaties die daarnaast ook veel persoonlijke gegevens verwerken kiezen meestal voor alle drie de normen. Omdat de beide normen gebaseerd zijn op de ISO 27002, is de stap om gecertificeerd te worden conform de ISO27017 en/of ISO27018 vrij klein voor organisaties die al ISO 27001 zijn gecertificeerd. Het overgrote deel van de extra maatregelen zijn al geïmplementeerd, onder meer via hostingcontracten en verwerkersovereenkomsten, maar moeten worden aangescherpt.