

Demarcatie: wie doet wat in de samenwerking?

Bij KPI Solutions werken we samen met klanten, en daarom is het belangrijk om af te spreken wie waarvoor verantwoordelijk is. Ons wie-doet-wat-beleid oftewel de "demarcatie" van de diensten is bedoeld om de samenwerking te verduidelijken. KPI Solutions is ISO27001 en NEN7510 gecertificeerd. Al onze oplossingen worden gehost bij Microsoft Azure in Europa en informatieveiligheid is voor ons van vitaal belang. Deze demarcatie is onderdeel van de voorwaarden.

Algemeen

- Overall waar klant staat, kan dit ook een leverancier zijn van de klant. Bijvoorbeeld de IT-dienstverlener of ontwikkelaar van het bronsysteem. Dit zijn echter altijd leveranciers van de klant, waarmee de **klant** afspraken en contracten heeft.
- Het is uitgangspunt is dat zowel de **klant** als **KPI** elk verantwoordelijk zijn voor alle beveiligingsmaatregelen in de eigen organisatie, eigen systemen en eigen tenant. Een tenant is de naam van een klantomgeving van Microsoft voor een bedrijf.
- **KPI** is verantwoordelijk voor het voldoen aan de eigen verwerkersovereenkomst, certificeringen en verplichtingen uit overeenkomsten. **Klant** is verantwoordelijk voor een eventuele DPIA of leveranciersbeoordeling over KPI, hun certificeringen en verplichtingen uit overeenkomsten.
- **Klant** beoordeelt of het niveau en voorwaarden van dienstverlening van KPI voldoet voor de situatie waar ze het willen gebruiken. **KPI** levert diensten volgens de voorwaarden en afspraken.
- Processen in de tenant van de klant, vallen onder het beheer en verantwoordelijkheid van de **klant**. Hierop wordt geen controle en updates uitgevoerd. Partij die de omgeving host, is verantwoordelijk voor beschikbaarheid, toegang, beheer, updates, capaciteitsmanagement, configuratie, continuïteit, enz. Alle oplossingen in de klantomgeving zijn one-off zonder updates, patches en fixes. Dit geldt voor alle oplossingen op o.a. Microsoft Azure, Fabric en Power Platform in de omgevingen en tenant van de **klant**.
- KPI wordt niet gezien als beheerder van de tenant of werkruimte, zelfs al zijn deze rechten wel toegekend of voert een consultant hierop acties uit. **Klant** is verantwoordelijk voor het beheer van de eigen IT-omgeving.

Bronssystemen & cloudsystemen

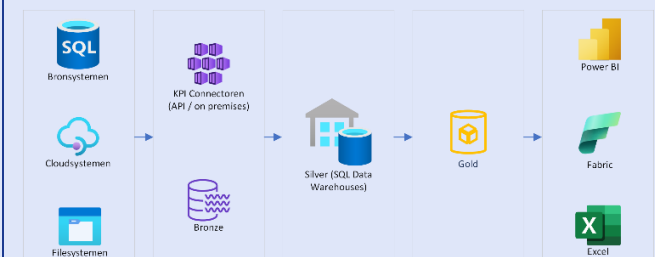
- Bronsystemen zijn de verantwoordelijkheid van **klant**. De klant is verantwoordelijk voor beschikbaarheid, integriteit en vertrouwelijkheid van het bronsysteem en afspraken met hun leveranciers. Als KPI-integratiepartner van het specifieke pakket is zorgt **KPI** voor de samenwerking met het bronsysteem, maar niet namens de klant.
- **KPI** specificeert de mogelijke methoden om de data te ontsluiten. De **klant** is verantwoordelijk voor de juiste toegang tot de data volgens die specificatie, en rechten op het account dat wordt verstrekt dan wel beschikbaar wordt gesteld via de authenticatie.
- **Klant** draagt er zorg voor dat de data die ze delen of toegang toe geven ook met KPI als subverwerker gedeeld mag worden voor het gewenste doel (AVG).
- Bij persoonlijke gezondheidsgegevens is de **klant** altijd zelf verantwoordelijk voor geïnformeerde toestemming van cliënten, informatiedeling, clientrelatie en clientzorg (NEN7510)
- Bij API-bronsystemen dient de API te zorgen voor limieten en capaciteitsbeheer, waardoor het bronsysteem beschikbaar en integer blijft tijdens data-vernieuwing. Het gebruik van API binnen de beperkingen is de verantwoordelijkheid van de dataleverancier en dus de **klant**. Bij een on-premises systeem is dit een samenwerking, maar ook dan ligt de uiteindelijke verantwoordelijkheid hiervoor bij de **klant**.
- **KPI** zorgt dat de verstrekte inloggegevens veilig worden opgeslagen en volgens de afspraken worden gebruikt.

Bronze Layer (SFTP, Blob, SMB, filesystemen)

- Partij die de omgeving (zoals SFTP-server) host, is verantwoordelijk voor beschikbaarheid, toegang, beheer, capaciteitsmanagement, configuratie, continuïteit, enz. Voor de KPI-producten is dit **KPI**, anders is dit de **klant**.
- Partij die de omgeving verzorgt, verzorgt ook een inlog. **Klant** is zelf verantwoordelijk hoe dit in de organisatie wordt gebruikt en verspreid.
- **Klant** is verantwoordelijk voor het juist aanleveren van de bestanden of data. KPI controleert niet of data juist is aangeleverd.

Projectmanagement

- De scope van het project wordt door **KPI** en de **klant** vastgesteld. Dit betreft onder meer de functionele en technische vereisten van de oplossing, en de benodigde tijdsinvestering van beide partijen. Er wordt Agile en flexibel samengewerkt waarbij de scope kan veranderen gedurende het project.
- **KPI** zorgt voor de juiste consultants voor het project en beschikbaarheid van inzet. **Klant** zorgt voor betrokkenheid van "sponsor", "domein-verantwoordelijken", "projectverantwoordelijke" en/of andere beslissingsbevoegden om het project een succes te maken.



KPI Connectoren (API en on-premises)

- Alleen processen op het KPI dataplatform zijn een "KPI Connector". **KPI** is dan verantwoordelijk voor de beschikbaarheid en integriteit, op het niveau zoals beschreven in de voorwaarden en verwerkers-overeenkomst.
- **KPI** controleert of deze processen correct lopen en zorgt voor bugfixes, updates en doorlopende controle. KPI zorgt voor beheer, capaciteitsmanagement, configuratie, continuïteit, enz.
- KPI Connectoren zijn een SaaS-dienst die niet door de klant wordt beheerd en niet kan worden overgenomen. **KPI** verzorgt ontwikkeling, tests, acceptatie en operatie van dit product.
- **Klant** is verantwoordelijk voor de juistheid van de data. Onjuiste en incomplete invoer in het bronsysteem zorgt voor een onjuist en incompleet datawarehouse. Onjuiste aanlevering door de ontwikkelaar van het bronsysteem kan niet door KPI worden beïnvloed, maar door de **klant**. **KPI** spant zich in om de data zo correct mogelijk te repliceren naar het datawarehouse, binnen de randvoorwaarden.

Silver (SQL Datawarehouse) en Gold Layer

- **KPI** verzorgt een inlog tot het datawarehouse. **Klant** krijgt deze inlog voor het DWH, en is zelf verantwoordelijk hoe dit binnen (of buiten) de organisatie wordt gebruikt en verspreid inclusief authenticatie, autorisatie, rechten en rollen.
- Connectoren kunnen ook repliceren naar een externe database. **Klant** verzorgt een inlog met lees- en schrijfrechten tot het datawarehouse voor KPI, en zorgt voor beheer, capaciteitsmanagement, configuratie, continuïteit, enz. **Klant** is zelf verantwoordelijk hoe deze database in de organisatie wordt gebruikt en verspreid.

Microsoft Power Platform en Microsoft Fabric

waaronder Power BI, Power Apps, Power Automate

- Rapportages, dashboards, apps, flows, pipelines, enz. worden samen met de klant beoordeeld op integriteit ("aansluiten"). **Klant** is zelf verantwoordelijk voor acceptatie en gebruik van de oplossingen. Afhankelijk van de wensen en budget van de klant kan een oplossing volledig getest of juist op 'best effort' worden opgeleverd door **KPI**.
- De **klant** mag aanpassingen doen aan oplossingen maar daarmee stopt de officiële ondersteuning door KPI voor de werking hiervan, indien van toepassing.
- Deze oplossingen worden bij voorkeur gepubliceerd in de Microsoft-"tenant" van de klant. De **klant** is zelf verantwoordelijk voor het gebruik van de oplossingen in de organisatie, verder delen van de rapportages en het verzorgen van toegang, authenticatie, autorisatie, rechten, rollen, licenties en andere eisen.
- Bij een "Power BI refresh" monitort **KPI** actief of de processen uitgevoerd worden. **KPI** is verantwoordelijk voor de trigger en monitoring binnen de eigen tenant. De **klant** is verantwoordelijk voor het deel in de eigen tenant en voor de juiste toegang tot de PBI-service. **KPI** voldoet aan alles wat hiervoor is vermeld onder KPI Connectoren.
- **KPI** kan ondersteunen in de toegang voor gebruikers, waaronder met Row Level Security, maar de verantwoordelijkheid hiervoor ligt uiteindelijk bij de **klant**.
- **KPI** krijgt een inlog tot de klantomgeving om de oplossingen te publiceren, of stuurt het als bestand naar de klant. **Klant** zorgt indien gewenst voor een officeaccount met licenties voor Power BI Pro, Outlook en SharePoint licentie voor KPI.
- Bij uitzondering draaien rapportages (zonder persoonlijke gezondheidsgegevens) in de tenant van KPI. **KPI** zorgt dan voor capaciteit, toegang en licenties voor Power BI Pro, Outlook en SharePoint licentie voor KPI. De **klant** krijgt een of meerdere inlogs tot de rapportage, waarbij de licenties tegen kostprijs worden doorbelast aan de klant, maar blijft ook dan zelf verantwoordelijk voor gebruik en toegang binnen de klantorganisatie.

Artificial Intelligence (Machine Learning)

- De **klant** is verantwoordelijk voor het aanleveren van de benodigde data en het waarborgen van een consistente datastructuur. Dit kan ook met voorgenoemde Bronze, Silver (SQL-datawarehouse) en Gold Layer, waarbij **KPI** voldoet aan alles wat hiervoor is vermeld.
- Alle ML-oplossingen worden gehost op het KPI Dataplatform. **KPI** monitort actief of de processen technisch correct verlopen en stelt vervolgens waar nodig de klant op de hoogte.
- Na oplevering monitort KPI niet de inhoudelijke performance van het model. De **klant** is verantwoordelijk voor het bewaken van de modelprestaties en het signaleren van eventuele verslechtering. Indien gewenst kan **KPI** op verzoek ondersteuning bieden bij modelupdates.
- Voor andere AI-oplossingen worden tot op heden maatwerkafspraken gemaakt, maar geldt onverminderd dat zowel de **klant** als **KPI** elk verantwoordelijk zijn voor alle beveiligingsmaatregelen in de eigen organisatie, eigen systemen en eigen tenant.

Verschillen met versie 2026-01

- De uitleg over "Power BI refresh", puntje 4 onder Microsoft Power Platform en Microsoft Fabric, is duidelijker verwoord, zonder inhoudelijke wijziging.
- Het laatste puntje onder Artificial Intelligence is toegevoegd, zonder inhoudelijke wijziging.