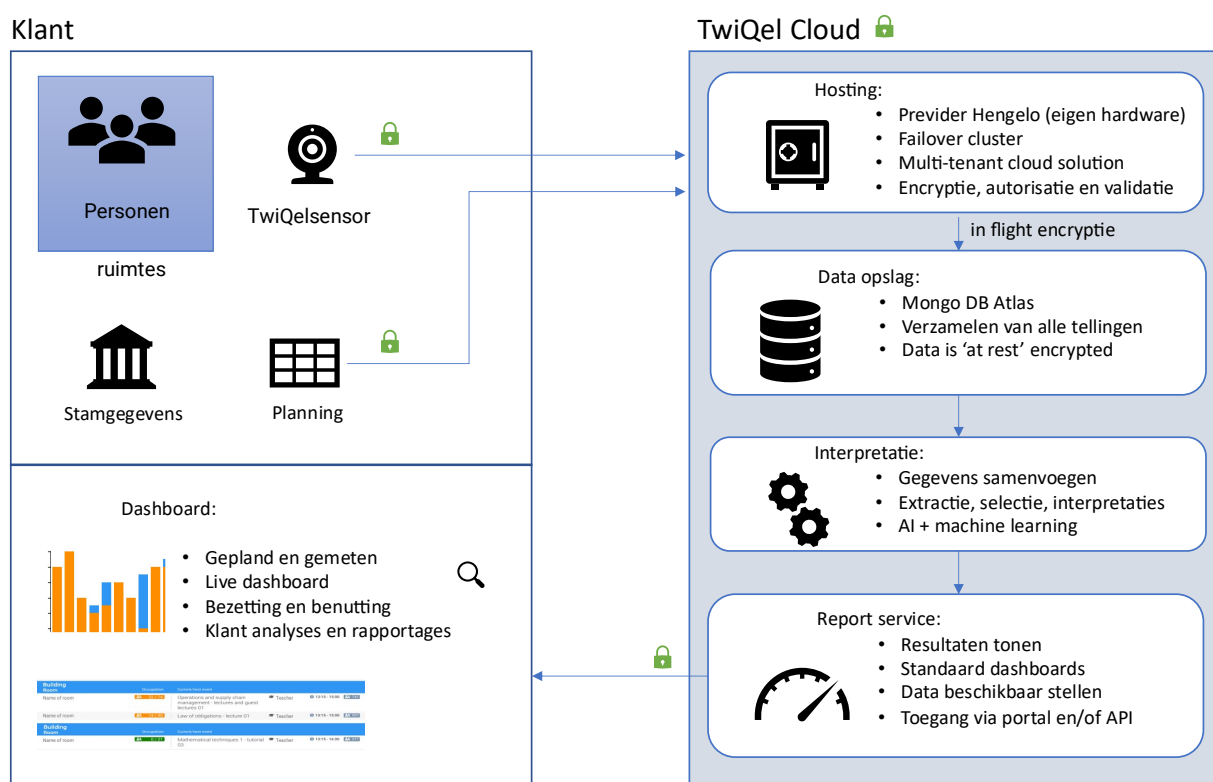


Privacy paper Twiqel BV

Twiqel werkt volgens het principe van privacy-by-design. Er wordt gestreefd naar het zo min mogelijk gebruiken van persoonsgegevens (privacy gevoelige data). Indien toch persoonsgegevens noodzakelijk zijn dan worden beveiligingsmaatregelen genomen zoals anonimiseren, pseudonimiseren, data minimalisatie, beveiliging van transport, encryptie en access control.

Tijdens de installatie wordt toegewerkt naar een technische inrichting van dataverwerking die overeenkomt met onderstaand technisch ontwerp van de datastromen tussen klant en Twiqel.

Technisch ontwerp datastromen:



Hieronder wordt beschreven welke privacygevoelige data wordt opgeslagen, verwerkt en getransporteerd binnen de bovenstaande keten. De beschrijving is per deelsysteem. Dit zijn:

1. Sensoren en overige brondata
2. De Twiqel Cloud omgeving

Niet privacy-gerelateerde data wordt buiten beschouwing gelaten.

Per deelsysteem wordt onderstaande beschrijving gehanteerd:

- Uitleg deelsysteem
- Welke data, welke verwerking
- Hoe wordt getransporteerd
- Waar gaat de data naartoe

1. Sensoren en overige brondata

Deze sectie beschrijft de inzet van de verschillende typen sensoren die data collecteren met als doel het tellen van aanwezige personen in die ruimte op elk moment, evenals stamdata en roosterdata.

- **Twiqelteller**
Personen die één van de ruimtes binnenlopen waarin wordt gemeten, worden gezien met de sensor die werkt op basis van beeldherkenning. Hiervoor worden door Twiqel zelf ontworpen sensoren gebruikt, genaamd Twiqeltellers. Deze intelligente meetcomputers verwerken hun informatie op de sensor zelf, en sturen gegevens over de getelde aantallen mensen door aan de Twiqel Cloud. Die aantallen worden in de Twiqel Cloud ontvangen met een Id van de sensor en een timestamp. De data is beveiligd door een VPN verbinding, bij voorkeur over een afgeschermd deel van het klant-netwerk (VLAN), rechtstreeks naar het IP-adres van de Twiqel Cloud. Ieder beeld dat de sensor maakt wordt alleen in het ram-geheugen van de sensoren verwerkt, waarna het volgende beeld wordt gemaakt en verwerkt. Er wordt dus geen beeld opgeslagen op medium of anderszins bewaard.
- **Stamgegevens**
Bij het opstarten van de metingen wordt informatie verzameld over de te meten ruimtes, waaronder de gebouwnaam, de kamernummers, de namen van de ruimtes, en de door de klant toegewezen IP-adressen op het afgeschermd gedeelte van het netwerk.
- **Roosterdata**
Door middel van een API wordt roosterdata uit de roosterapplicatie opgevraagd en verstuurd naar de Twiqel Cloud. De gegevens die worden opgevraagd bevatten informatie over de ruimtes: datum, gebouw, ruimte, event naam, start event, einde event, en indien gewenst de naam van de persoon die de ruimte heeft geboekt.

Standaard worden alleen metingen met de Twiqelteller uitgevoerd op doordeweekse dagen en tussen 7.00 en 22.00 uur. In overleg kan hiervan worden afgeweken.

2. Twiqel Cloud omgeving

De Twiqel Cloud omgeving zorgt voor validatie en autorisatie van toegang en hosting van de data. De data van de Twiqel Cloudomgeving wordt achter de schermen gehost bij MongoDB met 'database as a service' genaamd MongoDB Atlas. Dit betreft een high secure omgeving die alleen toegankelijk is via de Twiqel Cloud, die wordt gehost bij hostingbedrijf Previder in Hengelo. Deze wordt beheerd door PCA, het partnerbedrijf van Twiqel, namens Twiqel. Data tussen de Twiqel Cloud en MongoDB wordt "in flight" versleuteld via een rechtstreekse verbinding. Data in de Twiqel database wordt (in flight) versleuteld ontvangen en staat "at rest" versleuteld. Mongo heeft het hoofdkantoor in Dublin, Ierland. De veiligheid hiervan wordt gezien als extreem hoog. MongoDB Atlas wordt bijvoorbeeld ook gebruikt door bedrijven zoals KPMG en door de Europese Commissie vanwege de veiligheid, schaalbaarheid en snelheid. Zoals beschreven staan in de Twiqel Cloud database geen persoonsgegevens van klanten, maar alleen de tellingen per ruimte met timestamps en de sensor-Id's, samen met de beschreven roosterdata.

Meer over de Privacy policy van MongoDB: <https://www.mongodb.com/legal/privacy-policy>

Meer informatie over GDPR bij MongoDB: <https://www.mongodb.com/Cloud/trust/compliance/gdpr>

Verwerking

Met behulp van de tellingen van het aantal personen via de sensoren, wordt in de TwiQel Cloud de data omgezet naar informatie over bezetting en benutting van de ruimtes. De data wordt verwerkt door het combineren en integreren van de verschillende datastromen, het verzamelen van stamdata, roosterdata en gemeten data, plus de interpretatie ervan op basis van slimme algoritmes. Roosterdata wordt opgevraagd met behulp van een API waarvoor de klant een key (token) ter beschikking stelt. Deze data wordt meestal eens per dag opgevraagd en opgeslagen in de TwiQel Cloud omgeving voor de matching met de gemeten data. Het bevat geen persoonsgegevens, behalve als namen van bijvoorbeeld docenten mogen worden opgevraagd.

Autorisatie

Toegang tot de TwiQel Cloud is voorbehouden aan door TwiQel geautoriseerde medewerkers. Alle gebruikers krijgen een persoonlijke gebruikersnaam en wachtwoord. Verantwoordelijke is in staat om de rechten van elke gebruiker aan te passen aan de rol die de gebruiker heeft met de daarbij behorende rechten die deze gebruiker in de systemen van Verwerker daarom zou moeten krijgen.

Dashboard

In de TwiQel portal worden de geplande en gemeten bezetting en benutting van de ruimtes weergegeven. Er is geen privacy gevoelige informatie aan toegevoegd. Mogelijk staan hier wel de namen van docenten getoond, als die mogen worden opgevraagd uit de roosterdata. De informatie wordt in een dashboard gepresenteerd door middel van grafieken en/of tabellen, met daarin overzichten van de bezetting en benutting per zaal, zowel gemeten als gepland, per tijdseenheid. De data kan ook ter beschikking worden gesteld door een export op te vragen in csv formaat. Alleen geautoriseerde medewerkers van TwiQel en de klant krijgen toegang tot de portal. De data van bezetting en benutting mag door TwiQel worden gebruikt om de dienstverlening in het algemeen te verbeteren en voor promotiedoeleinden.

Samenvatting beveiligingsmaatregelen

- De systemen en daarmee de data zijn enkel te benaderen via software met sterke encryptie.
- Verwerking tot telling van personen gebeurt op de sensor zelf. Er worden geen beelden opgeslagen op opslagmedia.
- Persoonsgegevens worden niet opgeslagen of getransporteerd naar de TwiQel Cloud.
- Gebruik van HTTPS en VPN verbindingen verzorgen encryptie van het dataverkeer.
- Toegang tot TwiQel Cloud is voorgehouden aan geautoriseerde klant-medewerkers en TwiQel-medewerkers.
- Alle gebruikers van Verantwoordelijke krijgen een persoonlijke gebruikersnaam en wachtwoord.
- Elke gebruiker heeft eigen, specifieke autorisatie. Verantwoordelijke is in staat om de rechten van elke gebruiker aan te passen aan de rol die de gebruiker heeft en de daarbij behorende rechten die deze gebruiker in de systemen van Verwerker daarom zou moeten krijgen.
- Data van bezetting en benutting blijft beschikbaar voor onderzoek en promotiedoeleinden.
- TwiQel zal deze beveiligingsmaatregelen gedurende de looptijd van de pilot in stand houden.