SCOPE 4 MATION

Privacy & Security

Toelichting

V0.6

Inhoudsopgave

WIJZIGINGSHISTORIE

Om een duidelijk overzicht van onze diensten te krijgen, hebben we voor de verschillende serviceniveaus servicetypes gedefinieerd. Elk servicetype heeft een beschrijving om (in het algemeen) uit te leggen wat er in elk niveau wordt behandeld.

Versie	Wijziging
n.n.b.[1]	• -
31/10/2024	• ORB Graph rechten (4.6) aangepast n.a.v. optimalisaties in de ORB, MailSend recht.
16/10/2024	• ORB Graph rechten (4.6) aangepast n.a.v. optimalisaties in de ORB • Administratief: Inhoudsopgave en wijzigingshistorie toegevoegd
12/09/2024	• V0.4 van deze supportovereenkomst

[1]Niet inhoudelijke wijzigingen worden alvast opgenomen in de wijzigingshistorie en tenminste 1 keer per jaar gecommuniceerd, of als er een inhoudelijke wijziging plaatsvindt.

INLEIDING

Een belangrijk aspect van onze diensten betreft privacy en veiligheid (security). We verwerken informatie van onze klanten die in goede handen moet zijn. We zijn hier transparant en helder in. Om onszelf te toetsen, werken we conform ISO27001 en laten we ons door een erkende organisatie, TÜV Nederland, auditeren en certificeren. Met deze certificering laten we zien dat we informatiebeveiliging belangrijk vinden, niet alleen bij het ontwikkelen van onze oplossingen, maar ook voor wat betreft de bedrijfsvoering. ISO27001 draait om het controleren en beheersen van risico's, want risico's zijn er altijd. Risico's zijn niet te voorkomen en goed analyseren wat de risico's zijn, hier passende maatregelen voor treffen, hier op toezien (en informeren), dit goed evalueren en zorgen dat deze risico's lager worden, is dan erg belangrijk. Met dit document hebben we alle relevante aspecten benoemd. Omdat ISO27001 draait om continue verbetering komen we graag in contact om het gesprek aan te gaan mocht iets onduidelijk zijn of als er iets ontbreekt.

De volgende onderwerpen worden behandeld:

- Naleving / Informatie
- Qixium
- Outlook Room Booker
  - Verwerken Persoonsgegevens
  - Exchange
    - Notificaties ("Lezen")
    - CRUD ("Schrijven")
    - App-toegang
    - Permissies & Functionaliteit
    - Rechten uitdelen aan ons
  - TOPdesk
    - Lees/schrijf rechten en permissies
  - Proces inrichting
- Ons Statement

1. INFORMATIE

Op de website vind je alle actuele informatie over onze voorwaarden, IB-beleid en opzet, onze EULA en onze verkoopvoorwaarden. Ook vind je hier de meest recente versie van onze DNO (Dienst Nivo Overeenkomst) / SLA (Service Level Agreement).

2. COMPLIANCE

Scope4mation voldoet aan alle wettelijke eisen. Op onze website hebben we beschreven hoe wij dit naleven en ervoor zorgen compliant te zijn.

We hebben de volgende informatie samengevat als startpunt om inzicht te geven in de verschillende aspecten die hier een rol bij spelen:

- ISO27001 Certificaten/ certificering
- Privacy (compliancy statement)
- Bescherming persoonsgegevens
  - Verwerkersovereenkomst
  - Privacyverklaring
  - Cookiebeleid
- Hosting
  - Locatie & beveiliging van data & servers
  - Netwerk & cloud beveiliging
  - Beschikbaarheid en continuïteit
- Integriteit en vertrouwelijkheid
- Incidenten/ datalek of zwakke plekken

3. QIXIUM

Bij het implementeren van oplossingen zijn er altijd risico's aanwezig. Dit geldt ook voor de oplossingen die wij aanbieden. Afhankelijk van de specifieke oplossing kunnen deze risico's variëren in omvang en aard. Het is van essentieel belang om te bepalen of jullie organisatie deze risico's als acceptabel beschouwt en welke maatregelen zijn getroffen om deze risico's te mitigeren of te voorkomen. Er dient een goede balans te zijn tussen de voordelen en besparingen en de bijbehorende risico's. Wij gaan ervan uit dat, indien jullie organisatie besluit gebruik te maken van een van onze diensten deze beslissing reeds is genomen of dat wij zullen samenwerken tijdens een pilotperiode om de oplossing, inclusief de informatiebeveiligingsaspecten, te evalueren.

Dit document dient ter ondersteuning van onze inspanningen op het gebied van informatiebeveiliging. Het geeft inzicht in de maatregelen die Scope4mation heeft genomen om risico's te beperken of te voorkomen. Daarnaast onderstrepen wij hiermee onze expertise. Niet alleen met betrekking tot ons product, maar ook met betrekking tot de processen en inrichting ervan, zodat wij jullie van deskundig advies kunnen voorzien. Het document vormt de basis voor gesprekken met verschillende functionarissen binnen jullie organisatie, zoals Privacy Officers, Chief Information Security Officers (CISO's) en andere relevante rollen, om te bespreken welke oplossingen wij inzetten en hoe wij de risico's beheersen. Zoals eerder aangegeven beschouwen wij dit als een zeer belangrijk aspect van onze dienstverlening. Door dit onderwerp grondig te bespreken kunnen beslissingen weloverwogen worden genomen.

Onze SaaS-dienst Qixium biedt oplossingen voor het extraheren of invoeren van informatie in TOPdesk ten behoeve van jullie operationele applicaties en diensten. Indien de informatiebeveiliging binnen jullie eigen diensten goed is geregeld, ondersteunt en verstrekt dit de samenwerking en integratie met onze oplossingen.

Voor een groot deel van ons portfolio geldt dat we de afspraken dekkend maken door middel van een verwerkersovereenkomst, die in alle gevallen vereist is. Elke oplossing die wij leveren, heeft in meer of mindere mate betrekking op persoonsgegevens. Daarnaast zijn er oplossingen waarvoor in de bron- of doelapplicatie/dienst specifieke rechten nodig zijn. Wij hebben hiervoor een overzicht opgesteld om te verduidelijken waarom deze rechten noodzakelijk zijn, welke maatregelen wij nemen om risico's te beheersen, en wat de mogelijke gevolgen zijn mocht zich toch een incident voordoen.

Wat betreft de veiligheidseisen en de toetsing hiervan voor ons Qixium SaaS-platform en het gebruik daarvan, verwijzen wij graag naar onze website, waar deze aspecten zijn geïntegreerd in onze ISO27001-certificering. Wij bevelen aan om bij het inloggen gebruik te maken van Single Sign-On (SSO) in combinatie met Multi-Factor Authentication (MFA). Wij staan uiteraard open voor vragen en komen graag met je in contact.

4. OUTLOOK ROOM BOOKER [ORB]

Voor de Outlook Room Booker is het belangrijk om “boekingen” te beheren tussen Exchange(Online), lees ook: Outlook en TOPdesk. In beide omgevingen hebben we toegang nodig om dit te doen. Vanuit TOPdesk wordt geboekt op basis van een ruimte, in Exchange is dit op basis van een organisator. De ORB is een geavanceerd systeem dat in veel situaties ondersteuning biedt bij het beheren van boekingen.

Om dit effectief te doen is het noodzakelijk om onder andere de data te analyseren en op basis daarvan een conclusie te trekken om te bepalen wat er moet gebeuren. Denk hierbij bijvoorbeeld aan een herhalende reeks, waarbij 3 boekingen worden uitgesloten en op een andere locatie/ruimte worden geboekt. Of een secretariaat dat namens iemand anders een boeking doet en dat net even anders aanpakt. Deze uiteenlopende scenario’s maken het beheer hiervan al snel complex. Binnen de ORB worden deze processen zo optimaal mogelijk gestructureerd, waarbij alle rechten en instellingen zorgvuldig zijn afgestemd om aan specifieke scenario’s te voldoen.

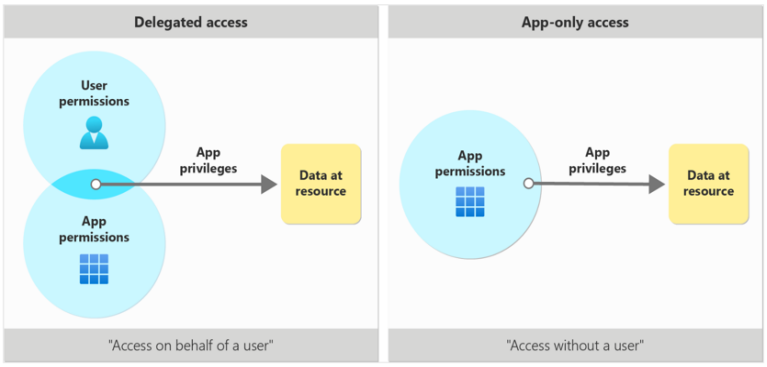
4.1 Verwerken persoonsgegevens

Persoonsgegevens die een rol spelen betreft binnen de ORB uitsluitend het e-mailadres. Dit is in de regel gebaseerd op een combinatie van gegevens, zoals bijvoorbeeld jan.jansen@bedrijf.nl, op basis waarvan een voor- en achternaam van een persoon en de organisatie waarvoor deze werkt afgeleid kan worden. Omdat we persoonsgegevens verwerken is het afsluiten van een verwerkersovereenkomst op basis van de AVG een wettelijke verplichting. We hebben de procedure hiervoor zo eenvoudig mogelijk gemaakt. Meer informatie vind je hier.

4.2 Exchange toegang

Voor toegang maakt de ORB gebruik van de door Microsoft geleverde toegangsmethoden. Dit gaat middels een App Registratie, die door jullie wordt opgezet en beheerd. Via de Graph API krijgt de ORB i.c.m. met de app registratie toegang tot jullie Exchange omgeving.

Omdat de ORB namens de organisator boekingen moet kunnen maken zijn hier de juiste permissies voor nodig.



4.3 Exchange notificaties (“Lezen”)

Omdat de ORB op basis van de zogenaamde “Deamon methode” werkt is de “alleen app-toegang” vereist. Een Daemon is een proces dat in de achtergrond loopt. Het doet in feite niets totdat een ander programma een beroep doet op de Daemon. Exchange bepaalt zo wanneer de ORB wat moet doen en geeft dit door. Dit gebeurt door middel van een “subscriptie” (abonnement). De ORB conformeert zich hierbij aan de verplichte Microsoft spelregels die gehanteerd worden voor het verwerken van zowel geringe als grote aantallen boekingen. Je moet bijvoorbeeld binnen X tijd reageren, omdat er anders problemen kunnen optreden.

Microsoft biedt 3 manieren om verbinding te maken met het notificatie systeem. De ORB maakt gebruik van Rich Notifications, op basis van Webhooks. Hiervoor is een extra security laag geïmplementeerd, die met een certificaat werkt. Dit om ervoor te zorgen dat de verbinding extra beveiligd en versleuteld wordt.

Verder wordt ook de inhoud van een boeking versleuteld en pas binnen de ORB weer leesbaar gemaakt. Beide verwerkingen worden met verschillende certificaten behandeld. De inhoud van de boeking wordt aanvullend met roulerende certificaten beveiligd, zodat deze frequent wijzigen. Uitsluitend de publieke sleutel wordt aan Microsoft doorgegeven en Microsoft versleuteld hier vervolgens alle data van een boeking mee. Per subscriptie wordt een random gegenereerd token meegegeven die op elke binnenkomende notificatie gecontroleerd wordt om te kunnen vaststellen of het bericht onderweg niet is aangepast. Dit principe heet “Anti-tempering” waar de ORB gebruik van

maakt. Voordeel van de notificatiemethode is dat mailboxen en/of kalenders niet door de ORB gescand worden, maar wacht op notificaties die bestemd zijn voor de ORB. Boekingen in een persoonlijke agenda die niet voor afhandeling door de ORB bestemd zijn hoeven en worden hierdoor ook in geen enkel geval door de ORB gelezen. De gegevens van deze boeking worden dus ook niet gescand door de ORB en de ORB heeft ook geen recht om deze te “scannen".

4.4 Exchange CRUD (“Schrijven”)

Boekingen worden teruggeschreven naar Exchange op basis van het CRUD principe. CRUD staat voor Create, Update, Delete. De hoogste standaard die Microsoft Graph levert voor beveiliging is de mogelijkheid van transportbeveiliging op basis van https. Inloggen vindt plaats op basis van de Oauth autorisatie. Dit is een bewezen wereldstandaard voor beveiliging. Om risico’s nog verder te verlagen wordt de toegang gemonitord en alles wat er met deze toegang gebeurd wordt gelogd.

Schrijven van boekingen gebeurt gecontroleerd en uitsluitend gegevens die via de ORB doorgegeven moeten worden, worden verwerkt. In een persoonlijke kalender mogen meerdere boekingen naast elkaar staan. Er hoeft hierdoor niet door de ORB gecontroleerd (uitgelezen) te worden of er op een bepaald moment nog ruimte in een persoonlijke kalender vrij is. ORB beheerd hierdoor uitsluitend de eigen boekingen. Boekingen in de persoonlijke agenda die niet door ORB beheerd worden kunnen hierdoor ook op geen enkele wijze door de ORB benaderd worden.

4.5 Exchange App-toegang

ORB maakt gebruik van **App-toegang**. Onderstaand het verschil tussen app-toegang en gedelegeerde toegang.

Kenmerk	App-toegang	Gedelegeerde toegang
ORB Processor	Ja, is beschikbaar	**Nee, methode kan niet worden gebruikt**
Definitie	Bij toegang met alleen apps roept de app Microsoft Graph aan met een eigen identiteit, zonder een aangemelde gebruiker.	Bij gedelegeerde toegang roept de app Microsoft Graph aan namens een aangemelde gebruiker.
Bedoeld voor	Deamon gebruikers principe, draaien op de achtergrond.	Gebruikers die bijvoorbeeld via een App moeten “doorloggen” als zichzelf binnen Microsoft Graph.
Consent	Toegang tot de kalender wordt op admin/beheerder niveau geregeld voor de gehele organisatie, middels een 1-malige bevestiging.	Toegang wordt op admin/beheerder niveau geregeld voor de gehele organisatie, middels een 1x bevestiging. *Of* Toegang moet individueel worden goedgekeurd, heeft iemand dat niet gedaan, wordt deze geen onderdeel van de informatie richting de Graph API en ontbreekt deze persoon bij de boeking.

Permissie detail toelichting Microsoft delegated & application permissies

Belangrijk om te realiseren is dus dat je op basis van de app-toegang niet als “gebruiker of beheerder” kunt inloggen. Uitsluitend de geregistreerde app heeft toegang. Aanvullend kan doormiddel van IP white-listing gezorgd worden dat er alleen tussen de Exchange klantomgeving en de ORB communicatie kan plaatsvinden. De toegang, zowel op account als IP-niveau, wordt door jullie als klant beheerd en kan op ieder moment afgesloten worden indien daar aanleiding toe zou zijn.

Category	Delegated permissions	Application permissions
Types of apps	Web app / Mobile / Single-page app (SPA)	Web / Daemon
Access context	Get access on behalf of a user	Get access without a user
Who can consent	• Users can consent for their data • Admins can consent for all users	Only admin can consent
Other names	• Scopes • OAuth2 permissions	• App roles • App-only permissions • Direct access permissions
Result of consent	oAuth2PermissionGrant	appRoleAssignment
Supported **signInAudience** types	AzureADMyOrg AzureADMultipleOrgs AzureADandPersonalMicrosoftAccount PersonalMicrosoftAccount	AzureADMyOrg AzureADMultipleOrgs AzureADandPersonalMicrosoftAccount

Extra info: Meer informatie en een uitgebreide toelichting vanuit Microsoft kan je hier vinden.

4.6 Exchange permissies & functionaliteit

De ORB Graph verwerking is opgezet volgens de best-practice regels van Microsoft, o.b.v. “least privilege”. Er wordt hiermee uitsluitend het privilege benut dat noodzakelijk is voor een specifieke actie. En niet (zoals vaak gebeurt) het “hoogste recht”, omdat “daar alles zo gemakkelijk mee kan”. Bij alles wat de ORB doet is het uitgangsprincipe van “least privilege” toegepast.

Bij de Graph Processor zijn de de volgende rechten toegepast. Onderstaand telkens minimaal 1 voorbeeld als toelichting waarom een recht benodigd is:

Graph API Methodes [klik voor details]	Functionaliteit	Configureerbaar	Lees/Schrijf	Voorbeeld
Calendars.ReadWrite	Primaire functie	Nee	Lees + Schrijf	Ophalen en wegschrijven van boeking(en). Ophalen boekingen ruimte, persoonlijke kalender. Tonen van boekingen via de View functionaliteit (weergave i.v.m. analyse boeking)
Mail.Send	Mailen	Ja	*Nvt*	Versturen van een email bij het informeren van gebruikers. Dit is te limiteren tot 1 gebruiker die alleen binnen de organisatie mail kan versturen.
Places.ReadAll List Places Get Place	Ruimten	Nee	Lees	Het recht is Places.ReadAll en we voeren de API-methodes list, get place om uit te lezen welke Ruimtes er zijn.

4.7 Exchange rechten uitdelen aan de ORB

Voor maximale veiligheid wordt het uitdelen van rechten voor de app-toegang die de ORB nodig heeft, evenals de secret-key, door jullie als klant zelf ingesteld en wordt deze versleuteld opgeslagen. Ondanks dat alleen de ORB de app-account kan gebruiken begrijpen wij, zeker als wij elkaar nog maar net kennen, dat weten hoe de omgang met jullie rechten door derden plaatsvindt een belangrijk aandachtspunt is. Uiteraard maken we hier afspraken over, leggen we zaken vast in de verwerkersovereenkomst en werken we conform procedures die geauditeerd worden. Echter het belangrijkste is het onder controle hebben van het proces van het verstrekken van rechten en niet zozeer het uitdelen ervan zelf, dat is een stap verder. Dat dit nodig is moet gezien worden als het gegeven en niet als het issue, wel hoe hiermee omgegaan wordt. Als je samen alles gedaan hebt om maximale veiligheid te waarborgen dan is al het overige gebaseerd op vertrouwen. Een metafoor:

"Stel je voor dat je na grondige screening de sleutel tot een prachtig museum krijgt. Deze sleutel geeft je de mogelijkheid om op elk moment binnen te gaan en toegang te hebben tot alle waardevolle kunstwerken en historische artefacten die daar worden tentoongesteld. Hoewel je de sleutel hebt en in principe op elk moment binnen kunt wandelen, betekent dit niet dat je moet rondlopen en de kunstwerken aan moet raken of mee naar huis moet nemen. De sleutel is je toevertrouwd omdat men erop vertrouwt dat je respectvol met de toegang omgaat.
Deze metafoor benadrukt het verschil tussen de mogelijkheid om iets te doen (je hebt de sleutel) en het juiste gebruik van die mogelijkheid (het museum en zijn kunstwerken respecteren). Het geeft aan dat je verantwoordelijk bent voor hoe je de rechten en toegang gebruikt die je hebt gekregen, en dat je deze rechten niet moet misbruiken."

4.8 TOPdesk lees/schrijf rechten & permissies

Om verbinding te maken met TOPdesk, gebruiken we de API van TOPdesk. Deze wordt op alle aspecten ondersteund. De volgende API methodes worden toegepast:

TOPdesk API Methodes [klik voor details]	Functionaliteit	Configureerbaar	Voorbeeld
Reserverations	Primaire functie	Nee	Voor het inlezen van delta details voor boekingen. Wegschrijven van een boeking
Supporting files (Persons)	Primaire functie	Nee	Ophalen van persoonsinformatie voor een email adres

4.9 ORB Velden

Binnen de ORB wordt gebruikgemaakt van de velden uit Exchange of TOPdesk. Hieronder zijn deze opgesomd en toegelicht. Alle velden die zijn vermeld zijn aan beide zijden beschikbaar. Velden die niet voor het beheer noodzakelijk zijn kunnen worden uitgesloten in de weergave. Deze worden dan voor iedereen uitgesloten en zijn niet zichtbaar. De standaardweergave betreft de velden die voor beheer zichtbaar moeten zijn. Hoewel op basis van onze ervaring niet nodig en niet geadviseerd, kan hiervan door middel van configuratie afgeweken worden.

AGENDA GERELATEERD

Veld	Toelichting	Privacy Opties
Afspraak Type	Enkelvoudig of herhalend.	*Nvt*
Organisator	Organisator van de boeking, o.b.v. het emailadres.	*Nvt*
Locatie	Locatieveld, bevat alle resources.	*Nvt,* wordt verder niet gebruikt, alleen voor inzicht
Ruimte	Ruimte emailadres, waar de boeking in is gemaakt.	*Nvt*
Deelnemers	Deelnemers die zijn gekoppeld aan de boeking.	*Nvt*
Onderwerp	Onderwerp van een boeking.	Ruimte: - Onderwerp

		verbergen op de ruimte zelf ORB: - Onderwerp niet meenemen
Start / Eind Tijd	Start en eindtijd van een boeking.	*Nvt*
Complexiteit Index	Hoe vaak is de boeking gewijzigd? We berekenen dit om te bepalen hoe complex de boeking op de achtergrond is geworden.	Geen, is een cijfer, worden verder geen gegevens verzameld.
Aanmaak datum	Datum dat de boeking is binnengekomen in de ORB.	*Nvt*

SYSTEEM GERELATEERD

Veld	Toelichting	Privacy Opties
ORB Match Id	Sleutel veld, wordt gebruikt om te ondersteunen bij het snel trekken van conclusies.	*Nvt*
Correlatie Id	Referentie veld, voor inzicht. Heeft een relatie met een uitgevoerde run, zodat we dit kunnen gebruiken bij een onderzoek.	*Nvt*
Processor Aangemaakt	Om te weten aan welke kant de boeking aangemaakt is.	*Nvt*
Orginele Organisator	Bij registratie van de boeking wordt dit 1x gevuld.	*Nvt*

STATUS GERELATEERD

Veld	Toelichting	Privacy Opties
Datum/Tijd Laatste bijgewerkt	Timestamp van de laatste verwerking.	*Nvt*
Laatst bijgewerkte Processor	Heeft Exchange of TOPdesk de boeking voor het laatst behandeld?	*Nvt*
Orginele Organisator	De organisator op het moment van aanmaken van de boeking.	*Nvt*
Gefaald Datum Tijd	Timestamp van het moment dat er iets mis is gegaan.	*Nvt*
Gefaalde Processor	Processor waar de fout heeft plaatsgevonden.	*Nvt*
Failed Count	Aantal keren dat het fout is gegaan.	*Nvt*
Aantal x opnieuw geprobeerd	Aantal keren dat het opnieuw is aangeboden aan Exchange of TOPdesk.	*Nvt*
Status: Exchange/TOPdesk processor	Laatst bekend status die teruggegeven is door TOPdesk of Exchange.	*Nvt*

4.10 Proces inrichting

Op basis van onze ervaring en methodiek kunnen we ervoor zorgen dat de ORB inrichten aansluit op de processen binnen jullie organisatie. Op basis van onderstaand overzicht kunnen we jullie ondersteunen om de risico's te verlagen en controleerbaar te maken.

Onderdeel	Aspect	Aanvullende Informatie
Privacy	Wanneer je met de ORB werkt, deel je met de ORB alleen het emailadres. Alle andere informatie kunnen we uitsluiten binnen de ORB. Denk hierbij aan Onderwerp of Inhoud.	ORB Configuratie, wordt tijdens het project doorgenomen als dit opportuun is.
Graph best practice	We werken bij het bepalen van de EXCHANGE PERMISSIES op basis van de best-practice adviezen van Microsoft en hebben die doorgevoerd in de ORB.	https://learn.microsoft.com/en-us/graph/permissions-overview?tabs=http#best-practices-for-using-microsoft-graph-permissions
Scope	Binnen Microsoft Graph kan je geen "scope" (toepassingsgebied) vaststellen bij de "app-toegang". Wat wel kan is dat er mailboxen uitgezonderd worden, waar wij geen toegang toe hebben. Zie ook "Beperken (mailbox) kalender toegang" hierna.	Configuratie en toelichting: https://learn.microsoft.com/en-us/graph/auth-limit-mailbox-access?context=graph%2Fapi%2F1.0&view=graph-rest-1.0
Alleen op een ruimte boeken	Dat willen we graag en vanuit TOPdesk kan dit ook prima. Bij TOPdesk reserveringenbeheer wordt gedacht vanuit een Ruimte. Bij Exchange werkt dit echter niet zo. Het reserveren van een ruimte is onderdeel van een boeking in een persoonlijke agenda. Hierdoor moeten we vanuit de persoonlijke kalender werken en niet vanuit een ruimte. *ORB ondersteund "room only" boeking wel, echter we raden dit sterk af. Een wijziging van een ruimtereservering vanuit TOPdesk werkt in dat geval alleen de ruimte bij in Exchange en niet de agenda van de organisator met de genodigden.*	ORB Configuratie, wordt tijdens het project doorgenomen als dit opportuun is.
Beperken (mailbox) kalender toegang	ORB werkt alleen met kalender lees en schrijf rechten, en heeft alleen toegang tot de kalender van een mailbox en heeft geen verdere toegang tot de mailbox en daarmee uiteraard expliciet ook niet tot mails. We lezen verder geen volledige gebruikerskalenders uit. De ORB maakt boekingen aan in een gebruikerskalender (van de organisator). ORB wijzigt alleen boekingen met een ruimte die door de ORB beheerd worden.	We hebben verder geen toegang tot de kalender.

Veranderd er bij jullie werkwijze nog iets aan de werking van Exchange of Outlook?	Nee, er verandert niks aan de huidige manier van werken op het gebied van privacy. Er zijn ongetwijfeld privacy en boekingsspelregels actief in Outlook, deze worden allemaal gehonoreerd met de ORB en onze manier van werken. Zet je een slotje op een agenda item, dan kunnen wij dit item niet inzien (wel verwerken). Vaak adviseren we ook om bijvoorbeeld een aparte boeking te maken op een ruimte wanneer je zeker wil weten dat er geen privacygevoelige informatie wordt gedeeld. Ook niet in de Ruimte Agenda van Outlook. Dit heeft te maken met het beleid van jullie organisatie. We zien steeds vaker het fenomeen dat er gewerkt wordt met een “Open agenda” beleid. Hierbij staat iedereen vrij te boeken hoe je dat zou willen en op het gebied van privacy wordt ervan uit gegaan dat je de algemene “bedrijfsregels” hanteert. Dit kan worden gedaan om het goed werkbaar te houden.	
Overwegingen/ argumenten	We kunnen ons voorstellen dat de volgende stellingen tijdens dit traject naar boven komen: “Hoe belangrijk is het boeken in of vanuit een persoonlijke agenda? Hoeveel voordeel geeft dit voor de organisatie in relatie tot wat er nodig is om dit te regelen?” “Maar dan kunnen jullie in de inhoud kijken” “Jullie kunnen dan overal bij?” “Wat is het bedrijfsbeleid rondom kalenders en het gebruik hiervan?”	Onze motivatie lees je hieronder bij “Ons statement”

5. Ons Statement

Vanuit Scope4mation vinden we het belangrijk om kwalitatief goede en complete diensten te leveren en daar zo helder mogelijk in te zijn. Bijvoorbeeld in relatie tot de ORB en het lezen en schrijven in een persoonlijke (bedrijfs)kalender van een medewerker; Deze methode kan prima worden gebruikt voor het automatisch synchroniseren van bedrijfsactiviteiten, zoals het boeken van een afspraak in TOPdesk op een ruimte. Voor een kalender van een medewerker moet er dan wel een bepaalde mate van herkenbaarheid zitten in de afspraken die worden gemaakt en het moet niet als een totale verrassing komen dat dit gebeurt. ORB bepaald natuurlijk niet wanneer er wat geboekt wordt, dat komt vanuit de medewerkers zelf. Die spelen de hoofdrol in de synchronisatie. Vanuit privacy oogpunt is het aannemelijk dat individuele medewerkers geen persoonlijke toestemming hoeven te geven voor het synchroniseren van ruimteboekingen tussen Outlook en TOPdesk. Toestemming op bedrijfsniveau is normaalgezien efficiënt en afdoende. Kenbaar maken dat dit proces actief is en dat de efficiency van het boeken van ruimtes bij afspraken hiermee wordt verbetert is zeker een Pré. We blijven echter wel realistisch dat niet iedereen in een organisatie eerst een expliciete consent kan geven alvorens boekingen met ruimtes via de ORB te kunnen laten synchroniseren. Als deze boekingen niet meegenomen zouden worden dan zou dat ook een directe impact hebben op alle andere boekingen.

Tot slot begrijpen we dat toegang tot Exchange een uiterst gevoelig onderwerp is. Door het toepassen van de app-toegang, de “least privilege” methode, IP white-listing, versleutelen en beveiligen van data en de communicatie en de wijze waarop de ORB ontwikkeld is met uitsluitend die functionaliteit en rechten die in dit document beschreven zijn, hebben we alle technische methodes en middelen voor informatiebeveiliging toegepast. Los van deze technische aspecten hebben we ook op organisatieniveau gezorgd dat informatiebeveiliging en de omgang met (privacy) gevoelige data geborgd is. Niet voor niets laten we ons met een zeer brede scope en verklaring van toepasselijkheid auditeren en certificeren op de ISO 27001 norm door een gerenommeerde en geaccrediteerde instantie als TÜV Nederland.

Zijn er nog vragen vanuit jullie organisatie? Dan is het belangrijk dat we met elkaar in contact komen. Dit kan via privacy@scope4mation.com. Je komt dan direct bij mij en ons privacy team terecht. We werken graag samen!

Namens Team Scope4mation hoop ik op een mooie en veilige samenwerking!

Marcel van de Steeg
Privacy Officer