

PROTOCOL VOOR DE ELEKTRONISCHE MEDEDELING VAN PERSOONSGEGEVENS VAN
DE STAD ANTWERPEN NAAR ATLAS, INTEGRATIE & INBURGERING ANTWERPEN

in het kader van de koppeling tussen JCC en Azure AD

Dit protocol wordt gesloten conform artikel 8, §1, van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

TUSSEN

Stad Antwerpen met zetel te Grote Markt 1, 2000 Antwerpen vertegenwoordigd door het college van burgemeester en schepenen, voor wie tekenen: Bart De Wever, Burgemeester en Sven Cauwelier, de Algemeen Directeur

hierna: "INSTANTIE 1";

EN

Atlas, Integratie en Inburgering Antwerpen met zetel te Carnotstraat 110, 2060 Antwerpen, vertegenwoordigd door de leidend ambtenaar van Atlas, Integratie en Inburgering Antwerpen, Sandy Peeters, Algemeen Directeur

hierna: "INSTANTIE 2";

[INSTANTIE 1] en [INSTANTIE 2] worden hieronder ook wel afzonderlijk aangeduid als een "partij" of gezamenlijk als de "partijen";

NA TE HEBBEN UITEENGEZET

- A. [INSTANTIE 1] is een lokale overheid;
- B. [INSTANTIE 2] is een extern verzelfstandigd agentschap (EVA) in de vorm van een vzw. Atlas voert namens de stad Antwerpen het Vlaams inburgerings- en integratiebeleid uit conform het Decreet betreffende het Vlaams integratie- en inburgeringsbeleid.
- C. **C1.** [INSTANTIE 2] heeft de gegevens nodig van [INSTANTIE 1] om de beschikbare momenten in de agenda's van gebruikers bij Atlas te raadplegen en afspraken in te boeken via de koppeling tussen JCC met Azure AD.
C2. Toepassing JCC heeft toegang tot Microsoft Entra ID (Azure AD) en haalt dat de afgesproken security groepen en zijn leden op. Vervolgens gaat hij van deze leden toegang tot de agenda's verschaffen. JCC kan alle agenda's uitlezen van de leden in de

security groep, alsook nieuwe items aanmaken in naam van de gebruiker.

In de afsprakenagenda's binnen JCC worden vervolgens tijdsblokken aangeboden als er in de Microsoft O365 agenda van een medewerker geen afspraak staat of een afspraak de status "beschikbaar" heeft. Naast de beschikbaarheid wordt er geen andere informatie door JCC-afspraken opgevraagd. De JCC-gebruiker plant vervolgens in JCC-afspraken de afspraak in bij de medewerker. Daarbij worden standaard afspraakgegevens vermeldt, zoals naam, voornaam, e-mail en/of telefoonnummer, alsook eventueel de reden van de afspraak. De afspraak wordt vervolgens automatisch doorgeschreven in de Microsoft O365 agenda van de medewerker.

C3. De gegevensstroom verloopt via Microsoft en JCC Software. Beide zijn Cloud toepassingen.

- D. De partijen wensen overeenkomstig artikel 8, §1, van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer een protocol te sluiten met betrekking tot de elektronische mededeling van persoonsgegevens. Dat protocol wordt bekendgemaakt op de website van beide partijen.
- F. De functionaris voor gegevensbescherming van [INSTANTIE 1] heeft op 22/09/2023 advies met betrekking tot een ontwerp van dit protocol gegeven.
- G. De functionaris voor gegevensbescherming van [INSTANTIE 2] heeft op 26/09/2023 advies met betrekking tot een ontwerp van dit protocol gegeven.

WORDT OVEREENGEKOMEN WAT VOLGT:

Artikel 1: Onderwerp

In dit protocol worden de voorwaarden en modaliteiten van de elektronische mededeling van de persoonsgegevens zoals omschreven in artikel 3 door [INSTANTIE 1] aan [INSTANTIE 2] uiteengezet.

Artikel 2: Rechtvaardigingsgronden van zowel de mededeling als de inzameling van de persoonsgegevens

De beoogde gegevensverwerking door [INSTANTIE 2] gebeurt op grond van de noodzaak voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag

[INSTANTIE 1] heeft de opgevraagde gegevens oorspronkelijk verzameld voor volgende doeleinden:

- Het maken en afhandelen van afspraken met een medewerker. De afspraken die geboekt en afgehandeld worden bij de stad komen op naam van de medewerker te staan. De gegevens van een gemaakte afspraak worden opgeslagen om afspraken te kunnen afhandelen en opzoeken.

[INSTANTIE 2] zal de opgevraagde gegevens verwerken voor volgende doeleinde:

- De beschikbare momenten in de agenda van gebruikers bij Atlas raadplegen en inboeken via de koppeling tussen JCC met Azure AD. Zo kunnen afspraken worden ingepland voor klanten van Atlas bij de beoogde medewerker van Atlas. De verwerking zal gebeuren op basis van een taak van algemeen belang.

Het doeleinde van de verdere verwerking van deze persoonsgegevens door [INSTANTIE 2] is verenigbaar met de doeleinden waarvoor [INSTANTIE 1] de gegevens oorspronkelijk heeft verzameld, gezien het doeleinde van de verwerking verenigbaar is met de aanvankelijke verwerking.

Artikel 3: De gevraagde persoonsgegevens en de categorieën en omvang van de gevraagde persoonsgegevens conform het proportionaliteitsbeginsel

In onderstaande tabel wordt een overzicht gegeven van de verschillende persoonsgegevens die worden meegedeeld, alsook de verantwoording van de proportionaliteit en de bewaartermijn van de gegevens.

Het betreft geen persoonsgegevens als vermeld in artikel 9 en/of 10 van de algemene verordening gegevensbescherming. Indien dat wel het geval is, wordt dit gespecificeerd in onderstaande tabel.

De gegevens worden opgevraagd op basis van de koppeling van JCC met Azure AD.

<p>Gegeven 1</p> <p><i>het concrete gegeven dat wordt meegedeeld. Als er veel gegevens zijn, kunnen ze in clusters worden vermeld.</i></p>	<p>JCC toont de tijdsblokken dat er in de Microsoft 0365 agenda geen afspraak staat, of wanneer een afspraak de status "beschikbaar" heeft. Verder wordt er geen andere informatie door JCC-Afspraken opgevraagd. Binnen JCC-Afspraken is via de rollen en gebruikers in te stellen of gebruikers afspraken voor zichzelf en/of andere mogen maken, en zo dus de beschikbaarheid in de Microsoft 0365 agenda indirect kunnen opvragen. Als een gebruiker afspraken voor anderen mag maken, dan is</p>
--	---

	<p>ook instelbaar voor welke gebruikers zij dit mogen.</p> <p>Verder schrijft JCC afspraakgegevens naar de Microsoft 0365 agenda, zoals naam, voornaam, datum, uur en type afspraak.</p>
<p>Verantwoording proportionaliteit waarom elk gegeven noodzakelijk is voor het gevraagde doel. Als in artikel 1 en 2 verschillende doelen zijn opgegeven, aangeven voor welk doel het gegeven wordt meegedeeld</p>	<p>Op basis van de beschikbare momenten kunnen afspraken worden ingeboekt tussen enerzijds de klant van Atlas en anderzijds de relevante medewerker van Atlas.</p>

De meegedeelde gegevens zullen door [INSTANTIE 2] bewaard worden. Deze bewaartermijn kan worden verantwoord gezien de klantgegevens automatisch door JCC worden geanonimiseerd na 365 dagen. De afspraken op zich blijven bestaan.

Artikel 4: De categorieën van ontvangers en derden die mogelijk de gegevens eveneens verkrijgen

Elke eventuele mededeling van de gevraagde persoonsgegevens door [INSTANTIE 2] moet voorafgaandelijk aan [INSTANTIE 1] worden gemeld en moet uiteraard in overeenstemming zijn met de relevante wet- en regelgeving inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens. Dat betekent onder meer dat [INSTANTIE 2] waar vereist een protocol sluit voor de mededeling van de gevraagde gegevens.

Artikel 5. Periodiciteit van de mededeling en de duur van de mededeling

De persoonsgegevens zullen PERMANENT worden opgevraagd omdat permanente doorgifte noodzakelijk is om de actuele toestand van de agenda's van de medewerkers van Atlas in te zien.

De mededeling van de persoonsgegevens gebeurt VOOR ONBEPAAALDE DUUR omdat de doorgifte noodzakelijk is om de actuele toestand van de agenda's van de medewerkers van Atlas in te zien.

Artikel 6: Beveiligingsmaatregelen

Volgende maatregelen worden getroffen ter beveiliging van de mededeling van de persoonsgegevens, vermeld in artikel 2:

- Microsoft Entra ID:
 - Gegevens worden omsloten via een App Registration en Enterprise Application. Deze is beveiligd met een secret dat enkel gedeeld is met JCC. Deze secret moet jaarlijks vernieuwd worden.
 - Toegang tot de Exchange omgeving (databron voor de agenda's) wordt beperkt tot een securitygroep, enkel leden van deze groep zijn uit te lezen door de toepassing. De rest van de omgeving blijft zo afgeschermd.
 - (Optioneel) conditionele toegang policy waardoor de gegevens enkel aanspreekbaar zijn vanuit het Digipolis-netwerk.
- JCC
 - De Outlook koppeling vraagt enkel de beschikbaarheid in Outlook op voor de geselecteerde medewerker. Naast de beschikbaarheid wordt er geen andere informatie door JCC-Afspraken opgevraagd.
 - Binnen JCC-Afspraken is via de rollen en gebruikers in te stellen of gebruikers afspraken voor zichzelf en/of anderen mogen maken en via die weg dus de beschikbaarheid in Outlook indirect kunnen opvragen. Als een gebruiker afspraken voor anderen mag maken dan is ook instelbaar voor welke gebruikers zij dit mogen
 - Aanroepen naar Outlook worden niet expliciet gelogd; in JCC-Afspraken wordt wel vastgelegd welke gebruiker een afspraak heeft gemaakt, gewijzigd of geannuleerd. Dus zodoende is dit wel achteraf inzichtelijk.
 - Toegangsbeheer tot de applicatie is een manueel proces. Dit wordt ondersteund door een aanvraagflow waarna deze nog steeds manueel moet worden overgezet door een beheerder.

[INSTANTIE 2] treft ten minste volgende organisatorische en technische beveiligingsmaatregelen ter beveiliging van de ontvangen persoonsgegevens bij verdere verwerking:

ALGEMEEN	Verantwoordelijke voor informatie beveiliging:
BEVEILIGINGSBELEID EN ORGANISATIE VAN INFORMATIEBEVEILIGING	Atlas heeft informatieveiligheidsconsulent aangesteld die verantwoordelijk is voor de data beveiliging

		⇒ contactgegevens: dpo.atlas@apogado.com
		<p>Verantwoordelijke voor gegevensbescherming:</p> <p>Atlas heeft een Data Protection Security Officer aangewezen die verantwoordelijk is voor het coördineren, opvolgen en controleren van de beveiligingsregels en -procedures.</p> <p>⇒ Contactgegevens: dpo.atlas@apogado.com</p>
		<p>Verantwoordelijkheden op vlak van informatiebeveiliging en gegevensbescherming:</p> <p>De verantwoordelijkheden van de medewerkers van Atlas zijn formeel gedocumenteerd en gepubliceerd in een privacy- en security policy</p>
		<p>Risico analyse, beheer en controle: Atlas voert periodiek risicoanalyses uit van de genomen beveiligingsmaatregelen en doet controles voor wat betreft de naleving van de verschillende verschillende informatiebeveiligingsprocedures</p>

PERSONEEL

VEILIG PERSONEELSBELEID		<p>Training over belang van beveiliging en omgang met persoonsgegevens:</p> <p>Atlas voorziet opleidingen om alle medewerkers te sensibiliseren voor wat betreft de beveiligingsrichtlijnen- en beveiligingsprocedures en hun rol daarbij.</p>
		<p>Toegangsautorisatie:</p> <p>Atlas implementeert en handhaaft een autorisatiebeheersysteem dat de toegang controleert tot systemen die persoonsgegevens bevatten.</p>
		<p>Segregatie:</p>

	Atlas heeft een segregatie ingevoerd om te vermijden dat personen toegang krijgen tot gegevens waarvoor ze geen toegang nodig hebben voor de uitoefening van hun taak.
--	--

GEBOUW	
FYSIEKE BEVEILIGING	<p>Fysieke toegang tot productie- en bureauruimtes:</p> <p>Atlas beperkt de toegang tot haar ruimtes waar persoonsgegevens verwerkt worden in kader van haar opdracht, strikt tot geïdentificeerde en geautoriseerde personen.</p> <p>Hiervoor werden badge-lezers geïnstalleerd, werd de lift uitgerust met codes en werden sloten voorzien op deuren waar nog nodig, dit alles om ongeoorloofde toegang te vermijden.</p>
	<p>Beveiliging van de omgeving:</p> <p>Naast badge-lezers is het volledige gebouw uitgerust met camerabewaking</p>
BESCHERMING TEGEN ONGEREGELDHEDEN, PANNES EN INCIDENTEN	<p>Firewall:</p> <p>Atlas is uitgerust met een geavanceerde firewall en controlemechanismen die zijn interne netwerk op gepaste wijze beschermt tegen ongeoorloofde toegang tot zijn interne netwerk.</p>

DATA	
DIGITALE GEGEVENS	
	<p>Anti-virus en beveiligingsupdates:</p> <p>Atlas voorziet al zijn systemen van de laatste updates. Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens haar patchmanagementproces</p>
	<p>Kwaadaardige Software:</p> <p>Atlas voert anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige</p>

		software ongeautoriseerde toegang tot klantengegevens krijgt.
COMMUNICATIE		
BEVEILIGDE VERBINDINGEN		<p>Versleuteling van verbindingen:</p> <p>Atlas maakt gebruik van beveiligde verbindingen voor de toegang tot haar gegevens in het datacenter. Alle data die verzonden wordt over publieke netwerken gebeurt dan ook aan de hand van encryptie mechanismen.</p> <p>⇒ HTTPS</p>
INFORMATIESYSTEMEN		
ONDERHOUD EN EVOLUTIE VAN INFORMATIESYSTEMEN		<p>Controle over systeem updates en evoluties:</p> <p>Atlas heeft een formeel wijzigingsbeheerproces geïmplementeerd om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze.</p>
		<p>Beveiligingsvereisten:</p> <p>De vereisten voor de bescherming van gegevens en systemen worden geanalyseerd en gespecificeerd in samenwerking met onze IT leverancier(s).</p>
INCIDENTEN		<p>Incident response: Atlas houdt een register van beveiligingsinbreuken bij met een beschrijving van de inbreuk, het tijdstip, de gevolgen van de inbreuk, de naam van de melder en van degene aan wie de inbreuk werd gemeld.</p>
		<p>Notificatie van incidenten:</p> <p>In geval van een gegevensbeveiligingsincident dat impact heeft op de vertrouwelijkheid of integriteit van persoonsgegevens van klanten, zal Atlas, zonder onredelijke vertraging, de verwerkingsverantwoordelijke hiervan informeren.</p>

[INSTANTIE 2] moet kunnen aantonen dat de in dit artikel opgesomde maatregelen werden getroffen. Op eenvoudig verzoek van [INSTANTIE 1] moet [INSTANTIE 2] hiervan aan [INSTANTIE 1] het bewijs overmaken.

In het geval [INSTANTIE 2] voor de verwerking van persoonsgegevens die het voorwerp zijn van voorliggend protocol, beroep doet op een verwerker (of meerdere verwerkers), doet de [INSTANTIE 2] uitsluitend beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van de algemene verordening gegevensbescherming voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. [INSTANTIE 2] sluit in voorkomend geval met alle verwerkers een verwerkerovereenkomst in overeenstemming met artikel 28 van de algemene verordening gegevensbescherming. Partijen bezorgen elkaar een overzicht van de verwerkers die de gevraagde gegevens verwerken, en actualiseren dit overzicht zo nodig.

Artikel 7: Kwaliteit van de persoonsgegevens

Zodra [INSTANTIE 2] één of meerdere foutieve, onnauwkeurige, onvolledige, ontbrekende, verouderde of overtollige gegevens in de persoonsgegevens, vermeld in artikel 3, vaststelt (al dan niet op basis van een mededeling van de betrokkene, meldt zij dat onmiddellijk aan [INSTANTIE 1] die na onderzoek binnen een redelijke termijn van de voornoemde vaststellingen de gepaste maatregelen binnen een redelijke termijn treft en [INSTANTIE 2] daarvan vervolgens op de hoogte brengt.

Artikel 8: Sanctie bij niet-naleving

Onverminderd haar recht om een schadevergoeding te vorderen en in afwijking van artikel 5, 2°, kan [INSTANTIE 1] dit protocol middels eenvoudige kennisgeving en zonder voorafgaandelijke ingebrekestelling eenzijdig beëindigen indien [INSTANTIE 2] deze persoonsgegevens verwerkt in strijd met hetgeen bepaald is in dit protocol, met de algemene verordening gegevensbescherming of met andere relevante wet- of regelgeving inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens.

Artikel 9: Meldingsplichten

Partijen engageren zich in het licht van artikel 33 van de algemene verordening gegevensbescherming om elkaar [via de functionarissen voor gegevensbescherming] zonder onredelijke vertraging op de hoogte te stellen van elk gegevenslek dat zich voordoet betreffende de meegedeelde gegevens met impact op beide partijen en in voorkomend geval onmiddellijk gezamenlijk te overleggen teneinde alle maatregelen te nemen om de gevolgen van het gegevenslek te beperken en te

herstellen. De partijen verschaffen elkaar alle informatie die ze nuttig of nodig achten om de beveiligingsmaatregelen te optimaliseren.

[Instantie 2] brengt [instantie 1] onmiddellijk op de hoogte van wijzigingen van wetgeving met impact op voorliggend protocol, zoals de finaliteit, proportionaliteit, frequentie, duurtijd enz. en in voorkomend geval van wijzigingen omtrent de verwerkers.

Artikel 10: Toepasselijk recht en geschillenbeslechting

Dit protocol wordt beheerst door het Belgisch recht.

Alle geschillen die voortvloeien uit of verband houden met dit protocol worden beslecht door de bevoegde rechtbank in Antwerpen.

Artikel 11: Inwerkingtreding en opzegging

Dit protocol treedt in werking op 13/10/2023.

Partijen kunnen dit protocol schriftelijk opzeggen mits inachtneming van een opzegtermijn van 3 maanden.

Het protocol eindigt van rechtswege na afloop van de in artikel 5 van dit protocol bedoelde termijn van mededeling. Het protocol eindigt tevens van rechtswege wanneer er geen rechtsgrond meer bestaat voor de gevraagde doorgifte van persoonsgegevens.

Opgemaakt te Antwerpen, op 13/10/2023. Aangezien deze overeenkomst digitaal wordt ondertekend, wordt in overeenstemming met artikel 8.20 NBW slechts één (digitaal) exemplaar van deze overeenkomst opgemaakt.

voor de stad Antwerpen

namens het college van burgemeester en schepenen

de algemeen directeur

Sven Cauwelier

de burgemeester

Bart de Wever

Voor Atlas

De Algemeen Directeur

Sandy Peeters