Verwerkersovereenkomst ARBIT-2022

De ondergetekenden:

1. <opdrachtgever.Naam>, gevestigd te <opdrachtgever.Plaats>, te dezen vertegenwoordigd door <opdrachtgever.vertegenwoordiger.naam>, namens deze, <opdrachtgever.namens.naam> <opdrachtgever.namens.functie, opdrachtgever.namens.onderdeel>,
hierna te noemen: **Opdrachtgever**,

en

2. Algemeen Nederlands Persbureau
(statutair) gevestigd te 's-Gravenhage,
te dezen vertegenwoordigd door M.M. Riemsma

hierna te noemen: **Wederpartij**,

hierna gezamenlijk te noemen: '**Partijen**' of afzonderlijk als '**Partij**'.

OVERWEGENDE DAT:

- voor zover Wederpartij Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, kwalificeert Opdrachtgever als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Wederpartij als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Wederpartij wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen
In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in de ARBIT-2022 of de Verordening, met dien verstande dat een aantal begrippen op de Verwerkersovereenkomst zijn toegespitst. Aldus en in aanvulling daarop wordt onder de volgende begrippen, ongeacht of ze in meervoud of enkelvoud, of als werkwoord of zelfstandig naamwoord worden gebruikt, in deze Verwerkersovereenkomst verstaan:

1.1 **ARBIT-2022**: Algemene Rijksvoorwaarden voor IT-overeenkomsten 2022.

1.2 **Betrokkene**: degene op wie een Persoonsgegeven betrekking heeft.

1.3 **EER**: Europese Economische Ruimte, zijnde alle EU-landen plus Liechtenstein, Noorwegen en IJsland.

1.4 **Inbreuk in verband met Persoonsgegevens**: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins Verwerkte gegevens.

1.5 **Ontvanger**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de Persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk Persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als Ontvangers; de Verwerking van die gegevens door die overheidsinstanties

Intern gebruik

strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.

1.6 **Overeenkomst**: de overeenkomst tussen Opdrachtgever en Wederpartij waarop deze verwerkersovereenkomst van toepassing is : <overeenkomst.datum, overeenkomst.kenmerk>

1.7 **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever Verwerkt.

1.8 **Toezichthoudende autoriteit**: een door een lidstaat ingevolge artikel 51 van de Verordening ingestelde onafhankelijke overheidsinstantie.

1.9 **Verordening**: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.10 **Verwerker**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt.

1.11 **Verwerkersovereenkomst**: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.12 **Verwerking**: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking door Wederpartij in het kader van de Overeenkomst en is onlosmakelijk verbonden met de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en Ontvangers zijn in **Bijlage 1** omschreven.

2.3 Wederpartij garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Wederpartij garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt voor zover en nadat Wederpartij alle Persoonsgegevens heeft gewist, terugbezorgd en bestaande kopieën heeft verwijderd met inachtneming van artikel 10 van deze Verwerkersovereenkomst.

3.3 Deze Verwerkersovereenkomst is niet tussentijds opzegbaar.

Artikel 4. Omvang verwerkingsbevoegdheid Wederpartij

4.1 Wederpartij Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever, tenzij een op Wederpartij van toepassing zijnde wettelijk voorschrift hem tot Verwerking verplicht. In dat geval stelt Wederpartij Opdrachtgever voorafgaand aan de Verwerking in kennis van dat wettelijk voorschrift, tenzij dat wettelijk voorschrift deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

4.2 Wederpartij heeft geen zeggenschap over het doel van en de middelen voor de Verwerking als bedoeld in de Verordening.

Artikel 5. Beveiliging van de Verwerking

5.1 Onverminderd artikel 2.3 van deze Verwerkersovereenkomst treft Wederpartij de technische en organisatorische beveiligingsmaatregelen zoals beschreven in **Bijlage 2**.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Wederpartij waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Wederpartij aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Wederpartij Verwerkt Persoonsgegevens niet buiten de EER, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming, zo nodig voorzien van nadere voorwaarden, heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Wederpartij informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Wederpartij verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Wederpartij

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 17.1 van de ARBIT-2022.

6.2 Wederpartij waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 17.2 van de ARBIT-2022.

Artikel 7. Subverwerker

Wanneer Wederpartij, met inachtneming van het bepaalde in artikel 23 van de ARBIT-2022, een andere Verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere Verwerker bij een overeenkomst dezelfde verplichtingen

inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

8.1 Voor zover mogelijk en rekening houdend met de aard van de Verwerking door middel van passende technische en organisatorische maatregelen, verleent Wederpartij Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

8.2 Partijen dragen elk de door henzelf in verband met de in het eerste lid te maken kosten.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Wederpartij informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in **Bijlage 3**.

9.2 Wederpartij informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde Toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, draagt Wederpartij er zorg voor dat hij, naar gelang de keuze van Opdrachtgever, alle Persoonsgegevens wist of terugbezorgt aan Opdrachtgever en bestaande kopieën verwijdert, tenzij opslag van de Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.

In geval van wissen en/of verwijderen van kopieën door Wederpartij informeert hij Opdrachtgever zodra hij dit heeft gedaan.

10.2 Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Wederpartij zorg voor het wissen of terugbezorgen en het verwijderen van kopieën van de betreffende Persoonsgegevens, tenzij opslag van deze Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.

10.3 Wederpartij anonimiseert de Persoonsgegevens binnen 3 maanden na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, bij gebreke waarvan Wederpartij een boete verschuldigd is van €500,- per dag, met een maximum van de opdrachtwaarde. Betaling van de boete laat de verplichting uit dit lid en de gehoudenheid van Wederpartij om de schade die het gevolg is van de schending te vergoeden onverlet.

Artikel 11. Informatieverplichting en audit

Om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst door Wederpartij zijn en worden nagekomen kan Opdrachtgever overeenkomstig artikel 5 van de ARBIT-2022 Wederpartij om informatie verzoeken of een audit laten uitvoeren.

Aldus overeengekomen en ondertekend in tweevoud door:

Plaats:	Plaats: Den Haag
Datum	Datum
<opdrachtgever.vertegenwoordiger.naam>, Opdrachtgever, Namens deze, <opdrachtgever.namens.naam>, <opdrachtgever.namens.functie>, <opdrachtgever.namens.onderdeel>	Wederpartij, <Naam tekeningsbevoegde> <functie>

Bijlage 1. De Verwerking van Persoonsgegevens
In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Overzicht Verwerkingen

Het onderwerp/aard en doel van de Verwerking	**Onderwerp:** De digitale ontvangst en opslag van relatiegegevens (medewerkers van verwerkingsverantwoordelijke) ten behoeve van ANP Raadsradar. **Aard & doel:** Het verwerken van data en beschikbaar stellen voor toegang en gebruik dienst aan opdrachtgever.
Het soort Persoonsgegevens	• Gebruikersnaam (e-mailadres) • Versleutelde wachtwoordgegevens (verwerkt en opgeslagen via Google Identity Platform) • Voornaam • Achternaam
Overige gegevens gekoppeld aan persoon	**Voorkeuren en instellingen:** Opgeslagen thema's, zoek- en signaleringsprofielen, alsmede de toestemmingsvoorkeuren voor analyse. **AI-Chatinteracties:** Prompts ingevoerd in de RAG AI-chatmodule, de door het systeem gegenereerde antwoorden op basis van de beschikbare content, alsmede de bewaarde chatgeschiedenis ter naslag.
Beschrijving categorieën Persoonsgegevens	Gewoon
Beschrijving categorieën Betrokkenen	Gebruikers bij opdrachtgever van ANP raadsradar
Beschrijving categorieën Ontvangers van Persoonsgegevens	Verwerkers
Locatie Verwerking Persoonsgegevens	EU/EER
Bewaartermijn	Anonimiseren na 3 maanden na inactief profiel, verwijdering persoonsgegevens 38 maanden na inactief profiel en op verzoek van de gebruiker

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Uitzondering Publieke Raadsgegevens: Partijen stellen vast dat het scrapen, verzamelen en verwerken van publieke gegevens van het openbaar bestuur (waaronder transcripties, namen, uitspraken en standpunten uit openbare raadsvergaderingen en livestream-bronnen van gemeenten) door ANP geschiedt onder de eigen zelfstandige verwerkingsverantwoordelijkheid van ANP ter bevordering van democratische transparantie en het volgbaar maken van lokaal beleid.

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Wederpartij in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

In te vullen door Opdrachtnemer:

Certificaten	**Organisatieonderdeel / dienst waarop certificaat betrekking heeft**	**Geldigheidsduur certificaat**	**Verklaring van toepasselijkheid**
ISO/IEC-27001:2022	Informatiebeveiliging gerelateerd aan het adviseren, ontwerpen, ontwikkelen, integreren, onderhouden en exploiteren van de SAAS diensten voor Mediamonitoring, Nieuwsvoorziening, Persberichten en datavisualisatie.	10-02-2029	Ja

Overige kwalificaties:

ANP is ISO/IEC-27001:2022 gecertificeerd
De SAAS diensten waar opdrachtgever gebruik van gaat maken draaien in de gecertificeerde Google Cloud omgeving. zie https://cloud.google.com/security?hl=nl

In te vullen door Opdrachtgever:

Aanvullende beveiligingseisen:

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens (waaronder datalekken)

In deze bijlage moeten de afspraken over hoe Wederpartij Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Aanleiding
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de Betrokkenen (de mensen van wie de Persoonsgegevens zijn gelekt).

Aangezien Wederpartij Persoonsgegevens gaat verwerken in het kader van het uitvoeren van de Overeenkomst, heeft Wederpartij de verplichting om bij het constateren van een Inbreuk in verband met Persoonsgegevens (art. 33 lid 2 AVG), zonder onredelijke vertraging, dit te melden aan Opdrachtgever.

Verlenen van medewerking
Opdrachtgever coördineert de afhandeling van het datalek naar en de melding aan de Autoriteit Persoonsgegevens en zo nodig aan Betrokkenen. Wederpartij dient volledige medewerking te verlenen door alle door opdrachtgever gevraagde informatie te verstrekken.

Opdrachtgever zal onder meer de volgende gegevens aan Wederpartij vragen:

1. Gegevens van zijn organisatie (naam organisatie, adres, postcode, vestigingsplaats, registratie beroeps- of handelsregister);
2. Gegevens van de melder (naam, functie, e-mailadres, telefoonnummer(s));
3. Gegevens over het datalek (korte samenvatting van het incident waarbij er een Inbreuk is geweest op de beveiliging van Persoonsgegevens, minimaal en maximaal aantal Betrokkenen waarop de Inbreuk op de Persoonsgegevens betrekking heeft, een omschrijving van de groep Betrokkenen waarop de Inbreuk betrekking heeft, wanneer de Inbreuk heeft plaatsgehad (exacte datum of periode), wanneer de Inbreuk is ontdekt);
4. Gegevens over de aard van de Inbreuk (lezen, kopiëren, veranderen, verwijderen, vernietigen, diefstal);
5. Soort Persoonsgegevens (beschreven in bijlage 1)(NAW-gegevens, telefoonnummers, e-mailadressen of andere adressen voor elektronische communicatie, toegangs- of identificatiegegevens, financiële gegevens, BSN, paspoort of kopieën van andere legitimatiebewijzen, geslacht, geboortedatum en/ leeftijd, bijzondere persoonsgegevens (zoals: etniciteit, politieke opvattingen, levensbeschouwing, lidmaatschap vakbond, genetische gegevens, biometrische identificatie, gezondheid, seksuele leven en strafrechtelijke gegevens);
6. Welke technische en organisatorische maatregelen genomen zijn om het datalek aan te pakken en om verdere Inbreuken te voorkomen?;
7. Technische beschermingsmaatregelen (waren de Persoonsgegevens op het moment van het ontdekken van het datalek (deels) versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? Op welke manier waren de Persoonsgegevens geheel of gedeeltelijk onbegrijpelijk dan wel ontoegankelijk gemaakt?).

Ook indien bovenstaande informatie nog niet bekend is, wordt er direct door Wederpartij contact opgenomen met de contactpersoon/het contactpunt datalekken van Opdrachtgever.

Voorbeelden van datalekken

8. Verlies of diefstal van een laptop, smartphone, USB-stick etc. Ook wanneer sprake is van encrypted data!
9. Per ongeluk openbaar maken van Persoonsgegevens.
10. Het versturen van een e-mail met namen in de CC in plaats van BCC terwijl de geadresseerden niets met elkaar te maken hebben. Of het versturen van een e-mail naar het verkeerde adres.
11. Slachtoffer zijn van een phishing mail of hack.
12. Het illegaal doorgeven van gebruikersnamen/inlogcodes of toegang hebben tot bestanden waarvoor je niet (meer) bent geautoriseerd.
13. Vernietiging van een database met Persoonsgegevens als gevolg van een menselijke fout terwijl een back-up ontbreekt.

In te vullen door Opdrachtgever:

Contactgegevens bij datalekken:
<opdrachtgever.datalekken.contact>
<opdrachtgever.datalekken.email>

In te vullen door Wederpartij:

Contactgegevens bij datalekken:
Privacy Officer ANP
E: privacy@anp.nl

Bijlage 4: Sub-verwerkers

Wederpartij gebruikt de volgende Sub-verwerkers bij de uitvoering van de overeenkomst:

Partij:	Land van verwerking (binnen/buiten EU/EER)	Verwerken persoonsgegevens ja/nee	Het onderwerp/aard en doel van de Verwerking
Google Cloud	EU	Ja	Ten behoeve van hosting en opslag
Twilio Sendgrid	EU	Ja	Ter verzending van nieuwsbrieven via de app

Bijlage 5: Algemene contactgegevens van partijen

Opdrachtgever:

Organisatie	<opdrachtgever.naam>
Contactpersoon	<opdrachtgever.contact.naam>
Contactgegevens	<opdrachtgever.contact.email>

Wederpartij:

Organisatie	Algemeen Nederlands Persbureau
Contactpersoon	Service Desk
Contactgegevens	servicedesk@anp.nl

Bijlage 6: Beveiligingsmaatregelen (Artikel 32 AVG)

Verwerker treft passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking. Deze maatregelen omvatten onder meer:

1. **Identiteits- en Toegangsbeheer:** Het beheer van inloggegevens en wachtwoorden is ondergebracht bij het Google Identity Platform. Wachtwoorden worden uitsluitend versleuteld opgeslagen en zijn voor ANP op geen enkele wijze inzichtelijk.

2. **Encryptie & Transport:** Alle gegevensuitwisseling tussen de gebruiker en de applicatie (https://raadsradar.anp.nl) vindt plaats via beveiligde, versleutelde verbindingen (TLS/HTTPS). Gegevens in rust worden eveneens geëncrypteerd opgeslagen.

3. **Analyse en Anonimisering:** Inzage in en analyse van het gebruik van de applicatie, ingestelde thema's en AI-chatinteracties ten behoeve van verbetering en doorontwikkeling vindt uitsluitend plaats indien de gebruiker hiervoor expliciet toestemming heeft gegeven via de voorkeuren. Gegevens die voor deze doeleinden worden gebruikt, worden strikt geanonimiseerd.

4. **Vertrouwelijkheid en Toegang:** Toegang tot de verwerkte gegevens binnen ANP is beperkt tot geautoriseerde medewerkers die gebonden zijn aan een geheimhoudingsplicht en toegang hebben op basis van het *need-to-know* principe.