Privacykader govroam

Auteur: Stichting govroam
Versie: 1.0
Datum: December 2018

info@govroam.nl
https://govroam.nl

Inhoudsopgave

1. Inleiding

1.1 govroam

govroam is een voorziening die Nederlandse organisaties in het openbaar bestuur (zoals gemeenten, ministeries, waterschappen, ZBO's, etc.) in staat stelt hun elektronische netwerken (zoals wifi) op confederatieve basis met elkaar te delen zodat iedereen in het openbaar bestuur overal veilig online kan gaan zonder extra kosten. Aan govroam deelnemende organisaties sluiten daartoe een overeenkomst met de Stichting government roaming Nederland (hierna '*Stichting govroam*'), die govroam in Nederland ontwikkelt en beheert.

govroam is een initiatief ván en vóór de overheid. Het is gebaseerd op een vergelijkbare samenwerking in het onderwijs, genaamd eduroam.[1] Stichting govroam streeft ernaar om govroam met een zo hoog mogelijk kwaliteitsniveau te leveren. Een belangrijk aandachtspunt hierbij is de integriteit van de gegevens van de eindgebruiker en de wijze waarop de deelnemende organisaties en Stichting govroam met de persoonsgegevens van de eindgebruiker omgaan. Voor meer informatie over de (technische) werking van govroam zie: *govroam.nl*.

1.2 Doel en scope van dit document

Om govroam mogelijk te maken zijn verschillende partijen betrokken die persoonsgegevens verwerken, zoals de deelnemende organisaties. Deze partijen zullen zich moeten houden aan de huidige en toekomstige privacyregelgeving, waaronder de Algemene Verordening Gegevensbescherming ("**AVG**") die per 25 mei 2018 in werking treedt/is getreden.

Omdat het voor de betrokkenen (eindgebruikers van govroam) duidelijk moet zijn waar zij terecht kunnen met privacyvragen, heeft Stichting govroam dit Privacykader gepubliceerd waarin de rolverdeling van de partijen verder wordt beschreven en waarin nadere informatie wordt verstrekt over de wijze waarop persoonsgegevens worden verwerkt. Hoewel govroam internationaal kan worden gebruikt (op dit moment België), is dit Privacykader primair bedoeld om duidelijk te maken hoe de rolverdeling is tussen de Nederlandse deelnemende partijen binnen govroam.

Dit Privacykader wordt onderdeel van de Gebruiksovereenkomst die de deelnemende organisaties met Stichting govroam sluiten.

[1] Voor meer informatie over eduroam zie: *https://eduroam.nl/*

2. Rolverdeling binnen govroam

2.1 Federatieve opzet

govroam wordt gekenmerkt door een federatieve opzet waarbij de betrokken organisaties hun medewerkers en/of gasten op een veilige manier toegang geven tot elkaars netwerk. De belangrijkste functionaliteit van federatieve authenticatie zoals govroam die biedt, is dat de eindgebruiker met de digitale identiteit die is verkregen bij de eigen thuisorganisatie toegang kan krijgen tot het netwerk van andere deelnemende organisaties (gastorganisaties). In de praktijk wordt het inlogverzoek van de eindgebruiker dus door thuis- en gastorganisatie gezamenlijk afgehandeld. De **authenticatie** vindt plaats bij de eigen thuisorganisatie, terwijl de **autorisatie** plaatsvindt bij de organisatie waar toegang wordt gevraagd, de gastorganisatie.

Een kernonderdeel binnen het govroamstelsel is de RADIUS-server. De RADIUS-server stuurt alle authenticatieverzoeken, en de antwoorden die hierop volgen, door naar de juiste organisaties. De nationale RADIUS-server, waarvoor Stichting govroam als Roaming Operator, verantwoordelijk is, vormt daarmee een centraal knooppunt waarlangs alle authenticatie-verzoeken en antwoorden de juiste kant op worden gestuurd.

In onderstaande tabel zijn de rollen van partijen nader beschreven.

Stichting govroam	**Roaming Operator**; verantwoordelijk voor de (nationale) RADIUS-server die nodig is voor het routeren van het authenticatieverzoek. Stichting govroam heeft het beheer van de RADIUS-server uitbesteed.
Thuisorganisatie	Ook wel **Identity Provider** genoemd; de organisatie die zorgdraagt voor authenticatie van de eindgebruiker voor het gebruik van govroam.
Gastorganisatie	Ook wel **Service Provider** genoemd; de organisatie die zorgdraagt voor autorisatie van de eindgebruiker voor het gebruik van govroam.

2.2 Privacyrollen

Terminologie

De AVG legt de meeste verplichtingen op aan de verwerkingsverantwoordelijke (hierna: '*verantwoordelijke'*). Dat is de partij die, alleen of samen met anderen, het doel (het waarom) van en de middelen (het hoe) voor de verwerking van persoonsgegevens vaststelt. De

verantwoordelijke kan het verwerken van persoonsgegevens uitbesteden aan een verwerker. Dat zijn partijen die ten behoeve van de verantwoordelijke gegevens verwerken zonder onder diens rechtstreeks gezag te staan. Een verwerker heeft geen zeggenschap over de gegevensverwerking, maar handelt uitsluitend naar de instructies en onder verantwoordelijkheid van de verantwoordelijke.

Privacyrollen binnen govroam
De betrokken partijen (Stichting govroam, thuis- en gastorganisaties) kunnen binnen de samenwerkingsketen allen (in)direct invloed uitoefenen op het overkoepelende beleid van govroam en de verwerkingen die daarbinnen plaatsvinden. Binnen het govroam-stelsel kunnen organisaties zowel als Identity als Service Provider optreden. Op macroniveau zijn de verschillende verwerkingen van de betrokken partijen min of meer geïntegreerd met het gezamenlijke doel om toegang tot elkaars netwerk mogelijk te maken door middel van gezamenlijk vastgestelde middelen.

Binnen deze opzet ligt het voor de hand om de Stichting en de thuis- en gastorganisaties als *deelverantwoordelijke* aan te merken. Dat houdt in dat ieder van deze partijen zelfstandig verantwoordelijk is voor zijn eigen deel van de gegevenswerking. Partijen zijn onderling dus geen verwerker van elkaar en hoeven dan ook geen verwerkersovereenkomst met elkaar af te sluiten.

3. De verwerking van (persoons)gegevens binnen govroam

3.1 Wat is het doel van de gegevensverwerking?
In de AVG staat het principe van de doelbinding centraal; persoonsgegevens mogen slechts worden verwerkt voor zover noodzakelijk ter realisatie van een doel. Het doel moet vooraf worden geformuleerd. De wet schrijft voor dat de doeleinden welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn. De persoonsgegevens zullen niet opnieuw worden gebruikt voor een doel dat daarmee niet verenigbaar is.

De verwerking van de benodigde (persoons)gegevens van de eindgebruikers in het kader van govroam heeft tot doel om overheidsmedewerkers binnen Nederland op een veilige en verantwoorde wijze toegang te geven tot elkaars netwerk, zonder daarmee afbreuk te doen aan het gemak en de privacy van de eindgebruikers. Daarnaast is de verwerking nodig om een correcte werking van govroam te waarborgen en om de thuisorganisatie en de eindgebruiker (door de thuisorganisatie) te identificeren in geval van misbruik.

3.2 Wie doet wat binnen govroam?
Stichting govroam (Roaming Operator)
Stichting govroam treedt in deze context op als Roaming Operator voor de deelnemende organisaties. Als Roaming Operator heeft Stichting govroam een coördinerende rol binnen govroam en stelt zij beleid op.

Bovendien is Stichting govroam verantwoordelijk voor de nationale RADIUS-server die nodig is voor de authenticatie binnen govroam. Naast de verwerking van gegevens ten behoeve van de dienstverlening houdt Stichting govroam logbestanden bij van de authenticatieverzoeken ten behoeve van troubleshooting.

De thuisorganisatie (authenticatie)
De thuisorganisatie verzorgt de authenticatie van de eindgebruiker. Concreet betekent dit dat wanneer de eindgebruiker te gast is bij een andere organisatie, de inloggegevens van de eindgebruiker (end-to-end) versleuteld worden verstuurd (via de centrale RADIUSproxy van de Stichting govroam) naar de authenticatieserver van de thuisorganisatie.

De thuisorganisatie controleert of inloggegevens van de eindgebruiker valide zijn bij het eigen Identity Management System (authenticatie) en meldt dit terug aan de gastorganisatie, die op basis daarvan de autorisatie uitvoert.

De gastorganisatie (autorisatie)
Een eindgebruiker bij de gastorganisatie krijgt toegang tot het netwerk door middel van govroam. De gastorganisatie stuurt de versleutelde inloggegevens van de eindgebruiker via de Roaming Operator (Stichting govroam) naar de authenticatieserver van de thuisorganisatie. Nadat de thuisorganisatie gecontroleerd heeft of de inloggegevens van de eindgebruiker valide zijn, meldt de thuisorganisatie dit terug aan de gastorganisatie. De gastorganisatie draagt zorg voor autorisatie van de eindgebruiker voor het gebruik van govroam.

3.3 Welke (persoons)gegevens worden vastgelegd?
In de privacywetgeving wordt aan het verzamelen van gegevens de eis gesteld dat er niet te veel of te gedetailleerde gegevens worden verzameld (niet bovenmatig), dat de gegevens toereikend zijn (zodat er geen verkeerd/onvolledig beeld ontstaat) en ter zake dienend zijn (niet overbodig).

Deelnemende organisaties binnen govroam zullen zich bij het verwerken van persoonsgegevens binnen het govroam-stelsel steeds de vraag moeten stellen of er niet met minder gegevens hetzelfde doel bereikt kan worden. Bovendien moeten de gegevens juist en nauwkeurig zijn. Dat betekent dat de eindgebruiker bij eerste opname van de gegevens bij de thuisorganisatie juist is geïdentificeerd en dat er periodieke (interne) controles nodig zijn om na te gaan of deze gegevens nog juist zijn.

De aard van sommige persoonsgegevens brengt mee dat verwerking ervan een grote inbreuk kan vormen op de privacy van de betrokkene zoals godsdienst, ras, politieke gezindheid, gezondheid en strafrechtelijk verleden. Daarom kent de wet voor deze gegevens een strenger regime, waarbij het uitgangspunt is dat deze zogenaamde ‘bijzondere’ gegevens niet mogen worden verwerkt. Uiteraard kent de wet een aantal

specifieke uitzonderingen voor dit verbod. Voor govroam geldt dat er door alle deelnemers geen bijzondere gegevens zullen worden verwerkt.

Stichting govroam (Roaming Operator)
Stichting govroam verwerkt in haar rol als Roaming Operator de volgende (persoons)gegevens:

- Unieke apparaatgegevens (MAC-adres) van de eindgebruikers.
- Identiteit van de thuisorganisatie en gastorganisatie.
- Tijdstip van het authenticatieverzoek.
- Authenticatiegegevens (gebruikersnaam en wachtwoord).
  NB: wachtwoord wordt altijd geëncrypt verstuurd en kan niet worden ingezien. Gebruikersnaam kan geëncrypt worden verstuurd als dit is geconfigureerd door de gebruiker.

Genoemde gegevens worden tevens opgeslagen in logbestanden.

Thuisorganisatie
Deelnemende organisaties die optreden als thuisorganisaties verwerken in ieder geval de volgende (persoons)gegevens met betrekking tot govroam.

- Unieke apparaatgegevens (MAC-adres) van de eindgebruikers.
- Identiteit van de gastorganisatie.
- Identiteit van het toegangspunt (wifi access point/netwerkswitch).
- Tijdstip van het authenticatieverzoek.
- Authenticatiegegevens (gebruikersnaam en wachtwoord).

Genoemde gegevens worden tevens opgeslagen in logbestanden.

Gastorganisatie
De gastorganisatie verwerkt in het kader van govroam de volgende (persoons)gegevens:

- Unieke apparaatgegevens (MAC-adres) van de eindgebruikers
- Identiteit van de thuisorganisatie.
- Identiteit van het toegangspunt (wifi access point/netwerkswitch).
- Tijdstip van het authenticatieverzoek.
- Authenticatiegegevens (gebruikersnaam en wachtwoord).
  NB: wachtwoord wordt altijd geëncrypt verstuurd en kan niet worden ingezien. Gebruikersnaam kan geëncrypt worden verstuurd als dit is geconfigureerd door de gebruiker.

Genoemde gegevens worden tevens opgeslagen in logbestanden.

Zoals hierboven aangegeven geldt dat het bij een juiste configuratie (te bepalen door de gebruiker) mogelijk is om in te loggen zonder dat de username van de eindgebruiker door de Roaming Operator of gastorganisatie via de logfiles achterhaald of ingezien kan worden. De Roaming Operator en de gastorganisatie zien dan alleen ‘anonymous@organisatie.nl’, de zogenoemde ‘*outer identity*’. De ‘*inner identity*’ wordt

(net als het wachtwoord) geëncrypt en kan alleen worden ingezien door de thuisorganisatie.

3.4 Hoe lang worden de gegevens bewaard?

De AVG schrijft voor dat organisaties persoonsgegevens niet langer mogen bewaren dan noodzakelijk is voor de doeleinden waarvoor ze de gegevens verwerken.
Stichting govroam, de thuis- en gastorganisatie zullen de door hen verwerkte gegevens niet langer bewaren dan 6 maanden na de laatste inlog van de eindgebruiker.

4. De verdeling van verantwoordelijkheden binnen govroam

4.1 Algemeen

In algemene zin geldt dat ieder van de deelnemende organisaties zelfstandig verantwoordelijk is voor zijn eigen deel van de gegevenswerking. Gelet echter op de veelheid van partijen die betrokken zijn binnen govroam, is het belangrijk om duidelijk te maken wie wat doet, zodat het voor de eindgebruiker helder is bij wie hij waarvoor het beste kan aankloppen.

4.2 Transparantie

Een belangrijke doelstelling van de AVG betreft de transparantie. Voor een goede bescherming van de privacy van de eindgebruikers is het noodzakelijk dat de eindgebruiker inzicht heeft in wat er gebeurt met zijn/haar persoonsgegevens. Des te gevoeliger de gegevens over de eindgebruiker zijn, des te meer reden is er om de eindgebruiker gedetailleerd te informeren over de gegevensverwerking.

De verplichting om betrokkenen te informeren over de gegevensverwerking en het voldoen aan verzoeken van betrokkenen die hun rechten op grond van de AVG willen uitoefenen, berust primair bij de verantwoordelijke, aldus artikel 12 e.v. AVG. Dit betekent dat de (deel)verantwoordelijken binnen het govroam -stelsel ieder voor zich verantwoordelijk zijn om de eindgebruikers te informeren en te voldoen aan privacyverzoeken van eindgebruikers. Vanuit praktisch oogpunt spreken partijen in dit verband het volgende af.

Privacy notice

Het eerste logische aanspreekpunt voor eindgebruikers is de thuisorganisatie. Partijen spreken daarom af dat de thuisorganisatie er primair voor zorgdraagt dat de eindgebruiker bij het gebruik van govroam op de hoogte wordt gebracht van de wijze waarop zijn/haar persoonsgegevens worden verwerkt binnen govroam.

Hiervoor kan gebruik worden gemaakt van de door de Stichting govroam opgestelde privacy notice template (**Bijlage 1)**.

Bovenstaande laat onverlet dat iedere partij verantwoordelijk blijft voor het informeren over de eigen gegevensverwerking. Omwille van een consistente informatievoorziening naar de gebruikers, raadt Stichting govroam ook de overige betrokken partijen aan om gebruik te maken van de bovengenoemde privacy notice template.

Wijze van informeren
Via de govroam.nl website zal de Stichting govroam het privacykader govroam openbaar stellen en de eigen privacy notice als Roaming Operator **(Bijlage 2)**. In overleg met de organisaties kan een link worden opgenomen naar de betreffende privacy notices.

4.3 Uitoefenen van rechten door de eindgebruiker

Om een transparante verwerking van persoonsgegevens te waarborgen geeft de AVG diverse rechten aan de eindgebruiker. De eindgebruiker kan deze rechten uitoefenen jegens de verantwoordelijke. Zo heeft de eindgebruiker onder meer recht op inzage, correctie en verwijdering van zijn gegevens.

Indien een eindgebruiker een beroep doet op zijn privacyrechten, kan hij zich het beste wenden tot de ICT-helpdesk van zijn of haar eigen thuisorganisatie. De thuisorganisatie zal vervolgens uiterlijk binnen één maand reageren, tenzij het een complex verzoek betreft. In dat laatste geval zal de organisatie de eindgebruiker binnen één maand na ontvangst van het verzoek in kennis stellen van de verlengde termijn (maximaal twee extra maanden).

4.4 Beveiliging

Deelnemende organisaties en eindgebruikers zijn gebaat bij een veilige online omgeving. Iedere organisatie is zelfstandig verantwoordelijk voor het treffen van passende technische en organisatorische beschermingsmaatregelen om de persoonsgegevens te beschermen. De deelnemende organisaties zijn verplicht om beveiligingsrichtlijnen van Stichting govroam op te volgen, die direct betrekking hebben op de dienst.

Het gebruik van govroam is daarnaast aan bepaalde (technische) randvoorwaarden gebonden waaraan de deelnemende organisaties moeten voldoen. Deze voorwaarden zijn onder meer te vinden op de govroam-webpagina: *https://govroam.nl/ondersteuning/downloads/*

4.5 Beveiligingsincidenten

De AVG bevat een verplichting om onder omstandigheden een inbreuk in verband met persoonsgegevens (een datalek) te melden aan de Autoriteit Persoonsgegevens en de betrokkene. Iedere organisatie is zelfstandig verantwoordelijk voor het op tijd melden van datalekken. Stichting govroam en deelnemende organisaties zijn ieder zelfstandig verantwoordelijk voor het op tijd melden van datalekken.

Overheidsorganisaties kunnen gebruik maken van Nationaal Cyber Security Operations Center ("**NCSOC"**). Het NCSOC opereert 24 uur per dag 7 dagen per week opereert als meldpunt voor cyberincidenten. Voor meer informatie zie: *https://www.ncsc.nl/incident-response/24-uurshulp.html*.

4.6 Centraal contactpunt voor eindgebruikers

Bij algemene vragen over dit Privacykader of overige vragen over de verwerking van persoonsgegeven binnen govroam, kunnen eindgebruikers contact opnemen met het volgende centrale emailadres: privacy@govroam.nl.

Bij specifieke vragen kunnen eindgebruikers het beste contact opnemen met de functionaris voor gegevensbescherming van de thuisorganisatie, dan wel de ICT-helpdesk van de thuisorganisatie.

Bij technische problemen kan contact worden opgenomen met de helpdesk van govroam via het volgende emailadres: helpdesk@govroam.nl.

5. Bijlagen

5.1 Bijlage 1: Template Privacy Policy voor de organisaties

Het meest recente template is on-line te vinden via:
https://www.govroam.nl/.....

5.2 Bijlage 2: Privacy Policy van Roaming Operator Stichting govroam

De actuele privacy policy van Stichting govroam, als Roaming Operator van govroam, is te vinden via:
https://www.govroam.nl/.....