# Bijlage D
# Risk, Compliance en Informatieveiligheid

## IWR2026|SMS-gateway

## ICT Werkomgeving Rijk

| | |
|---|---|
| Status: | versie 1.0 |
| Referentie: | IUC 202510087 |

# Inhoud

# 1 Inleiding

Op het gebied van informatiebeveiliging van de informatievoorziening dienen de Hoofdopdrachtgever en de Deelnemers zich te houden aan vastgestelde regels voor de Rijksoverheid. De regels over informatiebeveiliging voor de Rijksoverheid zijn onder meer terug te vinden in:

- Besluit BVA-stelsel Rijksdienst 2021[1];
- Baseline Informatiebeveiliging Overheid (BIO2);
- Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007)[1];
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2025)1;
- Algemene Verordening Gegevensbescherming (AVG)[1];
- Network and Information Security 2-richtlijn (NIS2)/ Cyberbeveiligingswet.

De Prestatie die Opdrachtnemer levert is integraal onderdeel van de informatievoorziening waar de rijksdienst gebruik van maakt. Dit betekent dat de Producten en Diensten van Opdrachtnemer niet strijdig mogen zijn met het beveiligingsbeleid van Hoofdopdrachtgever en/of Deelnemers.

Daarnaast dient de opdracht te voldoen aan de contracteisen Risk, Compliance en Informatieveiligheid. Deze contracteisen worden uitgewerkt in Bijlage 06A en 06B van de opdracht.

## 1.1 Basisbeveiliging Rijksoverheid opdrachten

De regels op het gebied van informatiebeveiliging die gelden voor de Rijksoverheid zijn gebaseerd op de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 normen. Opdrachtnemer dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering.

In deze Bijlage D – Risk, Compliance en Informatieveiligheid zijn de beveiligingsaspecten opgenomen, die van toepassing zijn op de Dienstverleningsovereenkomst[2]. Deze beveiligingsaspecten zijn onder te verdelen in:

- Eisen die gesteld worden aan de methode van Risicomanagement, inclusief Business Continuity Management;
- Eisen die gesteld worden aan de Compliance van de Dienstverlening, Producten en Diensten;
- Eisen die gesteld worden aan de uitvoering van de Dienstverlening, Producten en Diensten inzake het kwaliteitsaspect Informatieveiligheid, uitgewerkt in Informatiebeveiliging en Privacybescherming.

In het Dossier afspraken en procedures (DAP) tussen de Opdrachtnemer en de Deelnemer worden alle specifieke beveiligingsafspraken tussen de Opdrachtnemer en de Deelnemer vastgelegd.

[1] Zie hoofdstuk 5 Bronvermeldingen voor de link naar het document

[2] Zie bijlage 02 'Specificatie van de Prestatie'

Wet- en regelgeving is niet statisch. Opdrachtnemer zal zich conformeren aan de actuele wet- en regelgeving. Uitgangspunt hierbij is dat de scope en reikwijdte van eventuele opvolgers van bestaande wet- en regelgeving niet wezenlijk wijzigen.

## 1.2 Nationale veiligheid

Voor sommige deelnemers is, aan de hand van de Quickscan Nationale veiligheid van de NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid)[3], bepaald dat er in deze opdracht risico's zijn met betrekking tot de Nationale veiligheid (bv. vitale bedrijfsprocessen, datalek).

Hierdoor zullen er extra maatregelen in het kader van Nationale veiligheid getroffen moeten worden in de opdracht. Dit is conform het ABRO Kaderbesluit, artikel 3 Risicomitigatie inkopen en nationale veiligheid[4]. De mitigerende maatregelen worden als eisen in een aanvullende Bijlage 06B – Risk, Compliance en Informatieveiligheid opgenomen bij de aanbestedingsdocumenten.

[3] https://www.nctv.nl/onderwerpen/e/economische-veiligheid/toolbox-veilig-inkopen

[4] https://wetten.overheid.nl/jci1.3:c:BWBR0051910&paragraaf=2&artikel=3&z=2026-01-01&g=2026-01-01

# 2 Eisen voor Riskmanagement

## 2.1 Basisbeveiliging Rijksoverheid opdrachten

De risicoaanpak dient gebaseerd te zijn op de ISO27001 of een vergelijkbare methode. Het vormt ook de basis van de BIO-aanpak binnen de overheid. De risicomanagement processen zijn ontworpen om risico's systematisch te identificeren, beoordelen, beheersen en continu te monitoren. Dit is verder uitgewerkt in de BIO Deel 1, het BIO2-kader.

Een aparte benadering dient gekozen te worden voor de risico's van Business Continuity Management (BCM). Hierin dient gekeken te worden naar de risico's voor bedrijfscontinuïteit en dient invulling gegeven te worden aan crisismanagement. Het bestuur van de Opdrachtnemer dient betrokken te zijn bij de aanpak van BCM.

## 2.2 Nationale veiligheid

Door de Deelnemers waarbij er sprake is van risico's van Nationale Veiligheid is er een aanvullende risicoanalyse gedaan. De risicoaanpak van de Opdrachtnemer dient rekening te houden met en aan te sluiten op deze risicoanalyse van de Deelnemer. De Opdrachtnemer informeert de Deelnemer bij wijzigingen in de risico's en er wordt actief gestuurd op het mitigeren van de risico's.

Aanvullend op de aanpak voor bedrijfscontinuïteit en crisismanagement, dient er rekening gehouden te worden met een crisis van Nationale Veiligheid[5]. Er dient een aanvullend uitwijkplan opgesteld én geoefend te worden waarmee de opdracht voortgezet kan worden op een aangewezen infrastructuur en/of datacenter locatie.

[5] Conform de Nationale Crisisstructuur, zie https://www.nctv.nl/onderwerpen/n/nationale-crisisstructuur

# 3 Eisen voor Compliance

## 3.1 Basisbeveiliging Rijksoverheid opdrachten

De compliance dient gebaseerd te zijn op de ISO27001 of een vergelijkbare methode. Het vormt ook de basis van de BIO-aanpak binnen de overheid. De ISO27001 vereist dat organisaties een Verklaring van Toepasselijkheid (VvT) opstellen, waarin zij de geselecteerde beheersmaatregelen vastleggen en toelichten welke maatregelen zijn geïmplementeerd. Hierbij geldt dat hierin ook de overheidsmaatregelen van de BIO expliciet worden opgenomen. Eventuele afwijkingen of niet-toepasbare beheersmaatregelen worden in een bijlage 'Uitzonderingen op de VvT' opgenomen.

De verantwoording over de compliance vindt standaard plaats door een ISO27001-certificaat op te leveren, met daarbij de VvT als toelichting. Ook dient er transparantie gegeven te worden over de continue verbetering van de compliance. Hiervoor maakt de Opdrachtnemer gebruik van een managementsysteem / ISMS (Information Security Management System).

## 3.2 Nationale veiligheid

Bij opdrachten met risico's voor de Nationale veiligheid, dient de Opdrachtnemer de VvT uit te breiden met een toelichting op de implementatie van de ABRO-maatregelen. Hiervoor levert de Deelnemer een mapping met de ISO27002 beheersmaatregelen op, waarmee de Opdrachtnemer de mapping met de eigen controls/maatregelen kan bepalen.

De verantwoording over de compliance vindt vervolgens plaats door middel van een SOC-2, ISAE 3000A type II assuranceverklaring of (aantoonbaar) gelijkwaardig alternatief, voor de scope van de opdracht. Het aantoonbaar gelijkwaardige alternatief voldoet tenminste aan het opleveren van bewijslast door een onafhankelijk gecertificeerde auditor, aantoonbaarheid welke werkzaamheden daartoe worden uitgevoerd en welke bewijslast beschikbaar zal komen, en zal ook op *werking* (conform type II) toetsen. De verklaring wordt minimaal eenmaal per jaar overlegd aan de Deelnemer. Tijdens de transitiefase kan volstaan worden met een type I verklaring of een andere audit op basis van *opzet* en *bestaan*.

Op basis van de assuranceverklaring zal er vanuit decentraal contractmanagement gestuurd worden op de opdracht. Hiervoor zullen de (materiële) bevindingen van de externe auditor gedeeld worden met de Deelnemer. Onder bevindingen wordt in zulks verstaan mogelijke tekortkomingen en/of aandachtspunten in de processen en techniek. Op basis van de bevindingen zullen Opdrachtnemer en Deelnemer in gesprek gaan over de voorgestelde verbeteringen, acties, aanpak, timing en opvolging daarvan.

# 4 Eisen voor Informatieveiligheid

Het kwaliteitsaspect van Informatieveiligheid wordt gewaarborgd door het toepassen van informatiebeveiliging en privacybescherming. Informatiebeveiliging en privacybescherming omvat het geheel aan maatregelen gericht op een kosteneffectieve beheersing van de risico's met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en data. Deze maatregelen komen voort uit wet- en regelgeving, besluiten en standaarden[6]. In dit hoofdstuk worden de eisen opgenomen voor concrete implementatie van mitigerende maatregelen.

## 4.1 Basisbeveiliging Rijksoverheid opdrachten

De informatiebeveiliging bij Rijksoverheid-opdrachten wordt in de basis geregeld door de BIO. Daarnaast wordt gestuurd op security-by-design, zero-trust, soevereiniteit, open source en open standaarden en ketenveiligheid. Toezicht hierop dient conform de NIS2 / Cyberbeveiligingswet ingericht te worden.

De privacybescherming wordt geregeld vanuit de AVG, met toezicht vanuit de Autoriteit Persoonsgegevens. Voor Rijksoverheid-opdrachten met persoonsgegevens wordt altijd een verwerkersovereenkomst afgesloten binnen het contract. De Opdrachtnemer zal aansluiten op de AVG-procedures van de Deelnemer, zoals bijvoorbeeld het melden van datalekken.

## 4.2 Nationale veiligheid

Conform het ABRO Kaderbesluit dient beoordeeld te worden of er voldoende (aanvullende) maatregelen getroffen kunnen worden om de risico's van Nationale veiligheid te mitigeren. Deze maatregelen zijn voor nu toegelicht in 'Bijlage E SMS-gateway en maatregelen'.

Per Deelnemer kunnen de maatregelen verschillen, afhankelijk van de risico's. Met de uitvraag van deze maatregelen gaan de Deelnemers akkoord met de mate van risicomitigatie om het ABRO-voorschrift niet van toepassing te verklaren. Hierdoor blijft het toezicht op de opdracht uitgevoerd worden door de Opdrachtgever en Deelnemers.

[6] Zie hoofdstuk 5 Bronvermeldingen voor de link naar het document

# 5 Bronvermeldingen

Onderstaand zijn de links opgenomen van de documenten en onderwerpen die in deze Bijlage zijn genoemd. De opgegeven links zijn de geldige links op het moment van publiceren van de marktconsultatie.

Voor de meest actuele versie van deze documenten tijdens de contractfase dient contact opgenomen te worden met Centraal Contractmanagement (CCM).

| Document | Locatie |
|---|---|
| Besluit BVA-stelsel Rijksdienst 2021 | wetten.nl - Regeling - Besluit BVA-stelsel Rijksdienst 2021 - BWBR0044617 (overheid.nl) |
| Baseline Informatiebeveiliging Overheid (BIO) | Producten/diensten - bio-overheid<br>https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/ |
| Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) | https://wetten.overheid.nl/BWBR0022141/2007-07-01 |
| Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI 2025) | https://wetten.overheid.nl/BWBR0051482/2025-09-09 |
| Algemene Verordening Gegevensbescherming (AVG) | https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving |
| Algemene Beveiligingseisen Rijksoverheid Opdrachten (ABRO) | https://www.rijksoverheid.nl/onderwerpen/zakendoen-met-het-rijk/beveiligingseisen-abro |
| Identificatieplicht | https://www.Rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/met-welke-identiteitsbewijzen-kan-ik-mij-identificeren |
| Door het NBV goedgekeurde producten | Geëvalueerde producten \| Informatiebeveiliging \| AIVD |
| Forum Standaardisatie: Pas Toe of Leg Uit | 'Pas toe leg uit' standaarden (verplicht) \| Forum Standaardisatie |
| NCSC: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) 2025-05 | https://www.ncsc.nl/transport-layer-security-tls/richtlijnen2025-05 |