

CHECKLIST TECHNISCHE VOORWAARDEN EN RFP-EISEN DIGITALE BESLUITVORMING

Dit document is geschreven naar aanleiding van het document Implementatie digitaal besluiten van VNG Realisatie en is opgesteld door de informatiebeveiligingsdienst voor gemeenten (IBD) van de VNG www.ibdgemeenten.nl. Dit document geeft antwoord op de eisen die gesteld kunnen worden vanuit informatiebeveiligings- en privacy perspectief aan tooling die gebruikt kan worden om het online vergaderen en besluitvorming van gemeenteraden te ondersteunen. Dit document dient in samenhang met een aantal andere documenten te worden beschouwd:

- ◆ Veilig digitaal vergaderen voor Raadsleden (IBD)
- ◆ Implementatieplan Digitaal besluiten (VNG-R)
- ◆ Adviesdocument voor Griffiers (Lokale Democratie i.s.m. vereniging van Griffiers)
- ◆ Stappenplan digitale besluitvorming (punt 2.7)
- ◆ <https://www.informatiebeveiligingsdienst.nl/nieuws/vragen-over-videoconferencingtools/> (IBD) met bijlage:
- ◆ <https://www.informatiebeveiligingsdienst.nl/product/quicksan-videoconferencing-tools/> (IBD)

ALGEMENE CONTEXT

Er moet worden opgemerkt dat Raad vergaderen al ondersteund wordt door diverse Raadsinformatiesysteem (RIS)-leveranciers, met tal van tools. Het enige dat nu verandert is dat raadsvergaderingen vanuit huis worden gevoerd en dus dat alle deelnemers aan de vergadering niet meer in het gemeentehuis aanwezig zijn in een raadszaal en dat alle automatisering en video-oplossingen nu vanuit andere locaties gebruikt worden. In principe is het hele proces uitgekristalliseerd, alleen de locatie van uitvoeren is veranderd. Dit betekent onder andere dat er gebruikt gemaakt gaat worden van een veelheid van apparaten en dat de kwaliteit van de verbindingen, het beeld en het geluid goed moeten zijn. De manier van werken als het gaat om besluitvorming is niet wezenlijk anders, sprekers kunnen zich nog steeds melden bij de Griffier en zij kunnen nog steeds deelnemen aan de vergadering, als ze in het bezit zijn van een goede verbinding en een apparaat waarmee beeld en geluid kan worden opgenomen

JURIDISCHE CONTEXT (PRIVACY)

Het in beeld brengen van personen en het via internet ter beschikking stellen van beelden van raadsvergaderingen zijn verwerkingen van persoonsgegevens die vallen onder de werking van de AVG. Artikel 23 Gemeentewet bepaalt dat raadsvergaderingen in het openbaar moeten worden gehouden. Een uitvloeisel daarvan is dat gemeenteraadsvergaderingen worden opgenomen en live worden uitgezonden of achteraf via internet zijn te zien. Dat is iets wat nu al gebruikelijk is. De grondslag hiervoor is het uitvoeren van een wettelijke verplichting (art. 23 Gemeentewet en artikel 6.1(c) AVG). Het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) voegt geen additionele inzichten toe. Gemeenten hebben ook maatregelen genomen om iedereen te informeren die aanwezig is bij een raadsvergadering dat die wordt opgenomen. Een digitale raadsvergadering gebaseerd op de Tijdelijke wet digitale beraadslaging en besluitvorming gemeenten is wat dat betreft in het kader van de AVG niets nieuws.

CONTEXT INFORMATIEBEVEILIGING

Er zijn informatiebeveiligings- en privacy-eisen van toepassing die gelden voor systemen voor digitale vergadering en -besluitvorming. Veelal zal gebruik worden gemaakt van een bestaand systeem waarmee voor de tijdelijke wet digitale beraadslaging en besluitvorming ook werd gewerkt. Verreweg de meeste systemen zullen Cloud gebaseerd zijn en daarom zijn de eisen vooral gebaseerd op die omstandigheid. Zie voor meer informatie ook de handleiding en factsheet cloud computing en privacy van de IBD.¹ Gemeenten wordt aangeraden voor selectie in contact te treden met hun CISO en FG voor ondersteuning.

Uitgangspunten / randvoorwaarden:

1. De leverancier is transparant over de technische inrichting van de oplossing, dat wil zeggen dat ze inzichtelijk maakt welke beveiligingsmaatregelen er toegepast worden en in hoeverre deze aansluiten bij geldende Nederlandse wet- en regelgeving. In het bijzonder gelden hier de BIO, de AVG en de Archiefwet. In het bijzonder, maar niet uitsluitend, volgens het lijstje van de IBD: <https://www.informatiebeveiligingsdienst.nl/nieuws/vragen-over-videoconferencingtools/>
2. De leverancier is transparant over de gebruikte technologie, sub-verwerkers en -leveranciers en locatie van verwerking.
3. De leverancier toont aan hoe de veiligheid van de actieve (raadsleden) en passieve (toeschouwers) deelnemers gewaarborgd is.
4. De leverancier toont aan hoe de functionele eisen uit hoofdstuk 2 van het adviesdocument voor griffiers werken, dan wel ingericht kunnen worden.
5. De leverancier levert een duidelijke (technische) configuratie en gebruikers handleiding die voor iedereen in begrijpelijke taal opgesteld is.
6. De leverancier levert ook support of is beschikbaar op de momenten waarop raadsvergaderingen plaatsvinden.

Concreet betekent dit dat de gekozen oplossing (in aanvulling op de reeds bestaande RIS-oplossing aan de volgende eisen moet voldoen:

- ◆ De videostream moet encryptie hebben om manipulatie van de stream te voorkomen.
- ◆ De interactieve gebruikers moeten kunnen inloggen zodat zeker is dat de gebruiker de gebruiker is.
- ◆ De video service geeft per vergadering een unieke vergader-id.
- ◆ De video service is per vergadering af te schermen met een wachtwoord.
- ◆ De video service leverancier heeft een duidelijk privacy statement waaruit af te leiden is hoe de leverancier omgaat met privacy.
- ◆ De video service is bij voorkeur gehost en verwerkt binnen de EER, of de leverancier doet mee met de EU-U.S. privacy shield.
- ◆ De videoservice leverancier is bij voorkeur gecertificeerd voor de ISO 27001 of bezit een ISEA 3402 type 2 of een SOC 2 type 2 verklaring.
- ◆ De videoservice is te gebruiken met een APP of via een webbrowser. Het wordt afgeraden om deelnemers te laten inbellen via een telefoon.

¹ <https://www.informatiebeveiligingsdienst.nl/?s=cloud>

PROCESMATIGE CONTEXT

Het vergaderen via verschillende videokanalen is niet wezenlijk anders dan via de normale manier. Waar op gelet moet worden bij besluitvormende raadsvergaderingen is dat de Griffier de vergadering moet kunnen sturen, dat wil zeggen dat de Griffier moet kunnen bepalen wie het woord krijgt, maar ook wie het woord niet krijgt. De volgende procesmatige zaken zijn van belang voor de raadsvergadering:

Voraf:

- ◆ Doet de live stream het bij alle interactieve deelnemers, inclusief hen die spreekrecht krijgen?
- ◆ Is er een voldoende stabiele internetverbinding?
- ◆ Is de verlichting bij de interactieve deelnemers goed?
- ◆ Is er een neutrale achtergrond waar de deelnemer voor zit of kan deze ingesteld worden?
- ◆ Is het geluid goed, zijn alle interactieve deelnemers verstaanbaar?
- ◆ Is er een aparte (tijdelijke) chatgroep voor communicatie met de griffier via een ander kanaal?
- ◆ Hebben alle interactieve deelnemers de juiste link naar de vergadering en het wachtwoord op een veilige manier gekregen?
- ◆ Is de publieke link beschikbaar voor toehoorders?
- ◆ Zijn de bedienaars vertrouwd met de omgeving?
- ◆ Is de vergaderdiscipline uitgewerkt?
- ◆ Werkt de opname?

Tijdens:

- ◆ Is iedere interactieve deelnemer zichtbaar en hoorbaar herkenbaar op een manier dat de identiteit kan worden vastgesteld (art. 2.3 tijdelijke afwijking gemeentewet)
- ◆ Een stem zonder zichtbare en herkenbare deelnemer dient als ongeldig te worden beschouwd.
- ◆ Kunnen alle deelnemers en toeschouwers het beeld en geluid volgen?
- ◆ Kan men extra spreekverzoeken indienen bij de VZ / Griffie?
- ◆ Is zichtbaar of niet meer dan het gewenste aantal interactieve deelnemers online aanwezig is?
- ◆ Kunnen stemmingen (tenzij anoniem) zichtbaar gemaakt worden voor alle deelnemers? (via stream of via RIS applicatie)
- ◆ Blijft de Griffie in control en kan de vergadering gestuurd worden?
- ◆ Zijn er geen vertrouwelijke documenten en informatie te zien?

<https://www.informatiebeveiligingsdienst.nl/product/cloud-computing/>

De IBD heeft dit advies opgesteld in afstemming met NCSC (Nationaal Cyber Security Centrum).