

Van: [REDACTED]@minvws.nl
Aan: Groep VWS medewerkers kern
Onderwerp: Dagelijkse update SG
Datum: vrijdag 20 maart 2020 17:34:53

Beste collega,

buiten reikwijdte

[REDACTED]

Dossiervorming

Nu veel collega's thuiswerken is het onverminderd belangrijk om documenten goed op te slaan en te archiveren. Waar normaal gesproken een verslag van een overleg wordt gemaakt geldt dat het ook belangrijk kan zijn om van conference calls verslagen te maken. Gezien de omstandigheden zullen besluiten mogelijk ook op andere manieren worden genomen, bijvoorbeeld via Whatsapp. Het is de bedoeling dat je ook van deze relevante besluitvormende zaken notities maakt en opslaat.

buiten reikwijdte

[REDACTED]

buiten reikwijdte

[REDACTED]

5.1.2.e

[REDACTED]



Bewaren van chatberichten

Handreiking voor de Rijksoverheid



Wijzigingshistorie

10 maart 2020	Oplevering eerste concept-iteratie (v.0.1)
26 maart 2020	Verwerking feedback op eerste concept
16 april 2020	Oplevering tweede concept-iteratie (v.0.9.8)
19 mei 2020	Oplevering derde concept-iteratie (v0.9.9)
26 mei 2020	Oplevering definitieve versie (v1.0) (ter review)
16 juni 2020	Definitieve versie

Inhoud

Wijzigingshistorie	2
1 Inleiding	4
Aanleiding	4
Doel	4
Scope	4
Opbouw	5
2 Kaders voor berichtenapps	6
2.1 Juridische kaders	6
2.2 Beleidskaders	9
3 Bewaren van chatberichten	11
3.1 Welke berichten bewaren?	11
3.2 Wiens berichten bewaren?	11
3.3 Wie bewaart?	12
3.4 Hoe bewaren?	12
3.5 Waar bewaren?	16
3.6 Wanneer bewaren?	17
3.7 Verwijderen?	18
4 Proces van bewaren	19
4.1 Procesoverzicht	20
4.2 Actoren	20
4.3 Toelichting processtappen	21
Bijlage 1 - Doelgroep, Definities en referentiedocumenten	23
Bijlage 2 - Rijksbrede beleidslijn (CIO-beraad)	25
Bijlage 3 - Beleidsadvies en aanpak berichtenapps	26
Bijlage 4 - Instructie bewaren chatberichten	29
Bijlage 5 - Componenten: overzicht en richtlijnen	31
Bijlage 6 - Annotatie uitspraak Raad van State	32

1 Inleiding

Aanleiding

Het gebruik van berichtenapps binnen de overheid is snel toegenomen door de laagdrempeligheid en gebruiksvriendelijkheid van het medium om snel informatie uit te wisselen in chatberichten. Sinds de uitspraak van de Raad van State¹ in maart van 2019 staat vast dat deze chatberichten kunnen worden opgevraagd met een Wob-verzoek. Dit betekent een nieuwe uitdaging voor de Rijksoverheid om de informatie uit chatberichten op te slaan en te beheren.²

Om hier invulling aan te geven is rijksbreed beleid vastgesteld voor het gebruik van berichtenapps:

Rijksbreed beleid “Omgang met berichtenapps”

- Berichtenapps worden zo min mogelijk gebruikt voor werkgerelateerde communicatie.
- Voor bestuurlijke besluitvorming wordt het gebruik van berichtenapps ontraden.

Gebeurt dit toch? Dan moeten de chatberichten die van belang zijn voor de verantwoording en reconstructie van bestuurlijke besluitvorming worden opgeslagen in het Document Management Systeem.

Doel

De handreiking Berichtenapps is ontwikkeld voor iedereen die binnen de Rijksoverheid³ betrokken is bij het bewaren van chatberichten. De handreiking is bedoeld om hen richtlijnen te bieden om het veiligstellen, opslaan en duurzaam toegankelijk maken van berichten, zo in te richten dat:

- Veiligstellen en opslaan efficiënt gebeurt;
- Veiligstellen en opslaan gebeurt binnen de geldende juridische en beleidsmatige kaders;
- Het rijksbrede beleid zo uniform mogelijk wordt uitgevoerd.
- Het waarborgen van een duurzaam toegankelijke informatiehuishouding binnen de Rijksoverheid.

LET OP - Het is uiteindelijk aan de Rijksorganisaties zelf om het beleid rondom berichtenapps in te voeren en daarin keuzes te maken aan de hand van de inzichten en richtlijnen die in deze handreiking worden toegelicht. Uitgangspunt blijft dat het gebruik van berichtenapps voor bestuurlijke besluitvorming wordt ontraden.

Scope

De handreiking is bedoeld voor rijksorganisaties en toepasbaar op:

- Alle typen berichtenapps (WhatsApp, Signal, SMS, etc);
- Alle soorten chatconversaties (zowel appgroepen als één-op-één gesprekken).

¹ Uitspraak van 20 maart 2019 (ECLI:NL:RVS:2019:899) van de Afdeling bestuursrechtspraak van de Raad van State: WhatsApp en SMS-berichten op zowel zakelijke als privételefoons van bestuurders en ambtenaren vallen onder de Wet openbaarheid van bestuur (Wob), als deze in het kader van het werk zijn verstuurd.

² Informatie kent vele vormen, bijvoorbeeld een in- of uitgaand poststuk, Word, Pdf, e-mail, maar ook sms en WhatsApp via de telefoon of tablet. Het gebruik van berichtenapps voor (formeel) zakelijke of bestuurlijke communicatie middels chatberichten is hierin een niet beheerde informatie- en communicatiestroom die veelal ongestructureerd en contextarm tussen functionarissen binnen en buiten rijksorganisaties plaatsvindt.

³ Zie bijlage 1 voor een nadere duiding van de Rijksoverheid en Rijksorganisaties.

Opbouw

De handreiking bevat drie onderwerpen:

Kaders voor berichtenapps P6	Samenvatting van het beleid en de geldende juridische kaders voor het gebruik van berichtenapps en het bewaren van chatberichten.
Bewaren van chatberichten P11	Handreikingen en richtlijnen voor het uniform en efficiënt bewaren van chatberichten bij rijksorganisaties.
Proces van bewaren P18	Beschrijving van de stappen voor het duurzaam toegankelijk bewaren van chatberichten, inclusief handvatten hoe dit vorm te geven.

Voor meer informatie over de specifieke doelgroepen, definities en referentiedocumenten bij deze handreiking, zie bijlage 1.

2 Kaders voor berichtenapps

Dit hoofdstuk biedt een overzicht van de beleidsmatige en juridische kaders die gelden voor het gebruik van berichtenapps en opslaan van chatberichten bij de rijksorganisaties.

Samengevat geldt het volgende kader:

Beperk het gebruik	Het gebruik van berichtenapps voor formeel zakelijke communicatie wordt zoveel mogelijk beperkt. Voor bestuurlijke aangelegenheden wordt het gebruik ontraden.
Bewaar relevante berichten	Chatberichten die relevant zijn voor de reconstructie van bestuurlijke besluitvorming, moeten worden bewaard.
Niet toegestaan	Het is vanuit het gestelde kader niet toegestaan om persoonsgegevens, vertrouwelijke of gerubriceerde informatie te delen via berichtenapps, behalve in specifieke in de wet benoemde situaties.

In dit hoofdstuk wordt dieper ingegaan op de geldende kaders. De lezer van deze handreiking kan:

- Zich verder verdiepen in het **juridisch kader** voor het gebruik van berichtenapps;
- Zich verder verdiepen in het **beleidskader**;
- De verdieping van de kaders overslaan en verder gaan met de modules '**Bewaren van chatberichten**' of '**Proces van bewaren**'.

2.1 Juridisch kader

Voor het gebruik van berichtenapps en het bewaren van chatberichten binnen de Rijksoverheid gelden een aantal wetten en regels die in deze paragraaf worden behandeld:



Uitspraak Raad van State

In maart 2019 heeft de Afdeling bestuursrechtspraak van de Raad van State bepaald dat WhatsApp-berichten, sms'jes en gelijksoortige chatberichten documenten zijn in de zin van de Wet openbaarheid van bestuur (Wob)⁴. Dit betekent dat dergelijke chatberichten, wanneer deze in het kader van het werk zijn verstuurd, onderdeel kunnen uitmaken van de informatie die beschikbaar wordt gesteld bij een Wob-verzoek.

De uitspraak heeft betrekking op alle vormen van elektronische berichtendragers, dus naast WhatsApp en SMS ook Signal, Facebook Messenger, etc.. Het maakt daarbij niet uit of de berichten via een privé of zakelijke telefoon zijn verstuurd.

Wet openbaarheid van bestuur (Wob)

In artikel 3 lid 1 van de Wob staat dat ieder bestuursorgaan (in de zin van de Algemene wet bestuursrecht) verzocht kan worden om informatie uit documenten die te maken heeft met bestuurlijke aangelegenheden openbaar te maken. De wet en de rechtspraak leggen bestuurlijke aangelegenheid uit als informatie die betrekking heeft op de voorbereiding, besluitvorming en uitvoering van beleid binnen het op openbaar bestuur in al zijn facetten.⁵

De Wob bevat geen bewaarplicht: in de wet staat niet precies welke documenten wel en welke niet moeten worden bewaard. Het gaat er bij de Wob om dat documenten (waaronder chatberichten) kunnen worden opgevraagd die op dat moment feitelijk en juridisch bij het bestuursorgaan 'berusten'.

Voor een juridisch houdbare omgang met chatberichten, zijn noodzakelijk:

- a. een uitgevaardigde beleidslijn ten aanzien van bewaren en verwijderen(schiften);
- b. een aantoonbare uitvoering daarvan.

Enkel op basis van bovenstaande voorwaarden kan de bestuursrechter overtuigd worden van het feit dat:

- Alle voor het Wob verzoek relevante chatberichten zijn verzameld zodat het bestuursorgaan niet wordt opgedragen alle informatiebronnen te raadplegen; en dat
- De berichten die niet meer bij het bestuursorgaan berusten terecht zijn verwijderd of vernietigd zodat het bestuursorgaan niet wordt opgedragen berichten bij derden op te vragen.

LET OP - Gedurende een Wob-traject, inclusief vervolgpcedures, gelden bijzondere eisen ten aanzien van het bewaren van documenten (dus ook chatberichten)⁶. Berichten mogen op dat moment bijvoorbeeld niet meer verwijderd worden.

4 De definitie van het begrip document in de Wob: 'een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat'. De rechtspraak leert dat het begrip 'document' ruim moet worden uitgelegd. Naast de 'normale' documenten en e-mails moet hier ook onder worden verstaan foto's, videobanden, geluidsbanden etc. en nu dus ook chatberichten.

5 Zie voor (recente) rechtspraak rond dit onderwerp: ABRvS 9 maart 2016, ECLI:NL:RVS:2016:659; ABRvS 31 augustus 2016, ECLI:NL:RVS:2016:2375, AB 2016/361 en ABRvS 30 augustus 2017, ECLI:NL:RVS:2017:2334, JB 2017/169

6 Als eenmaal een Wob-verzoek is binnengekomen moeten documenten worden bewaard tot het proces is afgerond. Dit is inclusief eventuele (buiten)gerechtelijke procedures, dus tot het besluit juridisch onaantastbaar/onherroepelijk is geworden. Daarbij mag ook niet tot vernietiging worden overgegaan van documenten als een andere wet dit voorschrijft (zoals de Archiefwet 1995).

Archiefwet 1995

De Archiefwet en selectielijsten⁷ bevatten op zichzelf geen aanknopingspunten voor microselectie bij chatberichten, maar vormen daartoe ook geen belemmering. De archiefwet bevat voor overheidsorganen een zorgplicht voor een goed geordende en toegankelijke staat van archiefbescheiden. Dit impliceert dat enige vorm van schifting ('het opruimen van het bureau') is toegestaan zodat tenminste de 'belangrijke' berichten worden bewaard.

LET OP - Er valt helaas geen omschrijving op microniveau te geven welke berichten er precies voor bewaring in aanmerking komen (microselectie); deze inschatting is aan de deelnemers aan het gesprek. Doorgaans kunnen zij het belang van het bewaren van de berichten het beste duiden binnen de context van het dossier. Er moet in ieder geval stil worden gestaan bij het belang van het bewaren van berichten. Vervolgens moet een bewuste risico-inschatting worden gemaakt, ook met oog op potentiële toekomstige ontwikkelingen.

AVG

Chatberichten vallen onder de Algemene verordening gegevensbescherming (AVG). Dat betekent dat rijksorganisaties integer en vertrouwelijk om moeten gaan met persoonsgegevens in chatberichten. Bij gebruik van berichtenapps en bewaren van chatberichten is er sprake van het verwerken van persoonsgegevens, omdat de berichtverwerking ook persoonsgegevens van identificeerbare levende natuurlijke personen omvat.

Eventuele verwerking moet voldoen aan de volgende principes:

- Ze is rechtmatig, behoorlijk en transparant;
- Er is een duidelijk verband met het doel van de verwerking;
- Er worden niet meer gegevens gebruikt dan noodzakelijk;
- De gegevens zijn correct;
- De gegevens worden een beperkte tijd opgeslagen;
- Er wordt integer en vertrouwelijk met gegevens omgegaan.

In Bijlage 6 is een deel van een annotatie op de uitspraak van de Raad van State toegevoegd, die inzicht kan geven in de implicaties van de AVG op het gebruik van berichtenapps en het opslaan van chatberichten.

LET OP - Voordat een rijksorganisatie overgaat op het exporteren en veiligstellen van chatberichten is het noodzakelijk om eerst een Privacy Impact Assessment uit te voeren. Op deze manier wordt inzichtelijk welke privacy risico's er zijn en welke noodzakelijke maatregelen moeten worden getroffen om de verwerking van persoonsgegevens in re richten conform de AVG.

Artikel 68 Grondwet

Uit artikel 68 van de Grondwet volgt een inlichtingenplicht die ministers en staatssecretarissen verplicht de Kamers zo tijdig en volledig mogelijk te informeren, zowel op verzoek als uit eigen beweging. Uitgangspunt is dat er inlichtingen worden verschaft: Gewoonlijk gebeurt dit per brief of nota. Documenten worden alleen verschaft wanneer de minister dit zelf nodig acht. Vervolgens is het aan de Kamer om te beslissen of zij zich voldoende geïnformeerd acht. Als de Kamer van oordeel is dat dit niet het geval is, kan zij verzoeken om nadere inlichtingen, eventueel in de vorm van documenten (dus ook chatberichten). De bewindsman zal dan in goed overleg met de Kamer bezien hoe aan de informatiebehoefte kan worden voldaan. Chatberichten kunnen dus een rol spelen bij dit inlichtingenproces, maar of ze moeten worden bewaard, daar gaat artikel 68 van de Grondwet niet over.

⁷ Een selectielijst is een beschrijving van categorieën procesgebonden informatieobjecten die voor blijvende bewaring dan wel voor vernietiging in aanmerking komen, voorafgegaan door een verantwoording. Daarin staan de termijnen na het verstrijken waarvan de vernietiging wel of niet mag plaatsvinden.

2.2 Beleidskaders

Binnen de Rijksoverheid wordt gewerkt aan een uniforme werkwijze om relevante chatberichten duurzaam toegankelijk te maken. Hiervoor is rijksbreed beleid vastgesteld in verschillende kaders, die in deze paragraaf worden toegelicht:



Rijksbrede beleidslijn (CIO-beraad)

Nog voor de uitspraak van de Raad van State heeft het CIO-Beraad op 7 februari 2018, een rijksbrede beleidslijn vastgesteld. Zie de volledige tekst in bijlage 2.

Deze lijn komt erop neer dat het gebruik van berichtenapps wordt ontraden voor communicatie over bestuurlijke aangelegenheden. Wordt een berichtenapp hier toch voor gebruikt, dan gelden de 'gangbare eisen van archivering en openbaarheid'. Daarnaast is bepaald dat:

- Integer en vertrouwelijk om moet worden gegaan met persoonsgegevens;
- De inhoud van chatberichten geen gevoelige of gerubriceerde informatie mag bevatten.

Voorkeursaanpak Ministerraad

In de Ministerraad van 18 april 2019 is naar aanleiding van de uitspraak van de Raad van State een voorkeursaanpak afgesproken: alle individuele medewerkers van de rijksoverheid schiften voortaan op periodieke basis hun chatberichten, en exporteren handmatig en op stuksniveau de belangrijke berichten.

Wat relevante berichten zijn en hoe dit technisch moet plaatsvinden is in de voorkeursaanpak niet verder uitgewerkt. Aan de ministeries van BZK en OCW is gevraagd om dit nader uit te werken. (Zie hiervoor de Technische exportinstructie en de Instructie bewaren chatberichten (bijlage 4).

Rijksbeleid inzake gebruik en opslag van berichtenapps

Op 3 juli 2019 is in het SG-overleg aanvullend beleid vastgesteld voor het gebruik berichtenapps en bewaren van chatberichten binnen het Rijk. Zie de volledige tekst in bijlage 3.

Dit beleid omvat de volgende drie speerpunten:

- Het gebruik van berichtenapps voor formeel zakelijke communicatie wordt zoveel mogelijk beperkt;
- Het gebruik van berichtenapps voor bestuurlijke aangelegenheden wordt ontraden;
- Het berichtenverkeer dat toch plaatsvindt, wordt periodiek geschikt. Archiefwaardige berichten worden handmatig geëxporteerd en veiliggesteld.

Technische exportinstructie

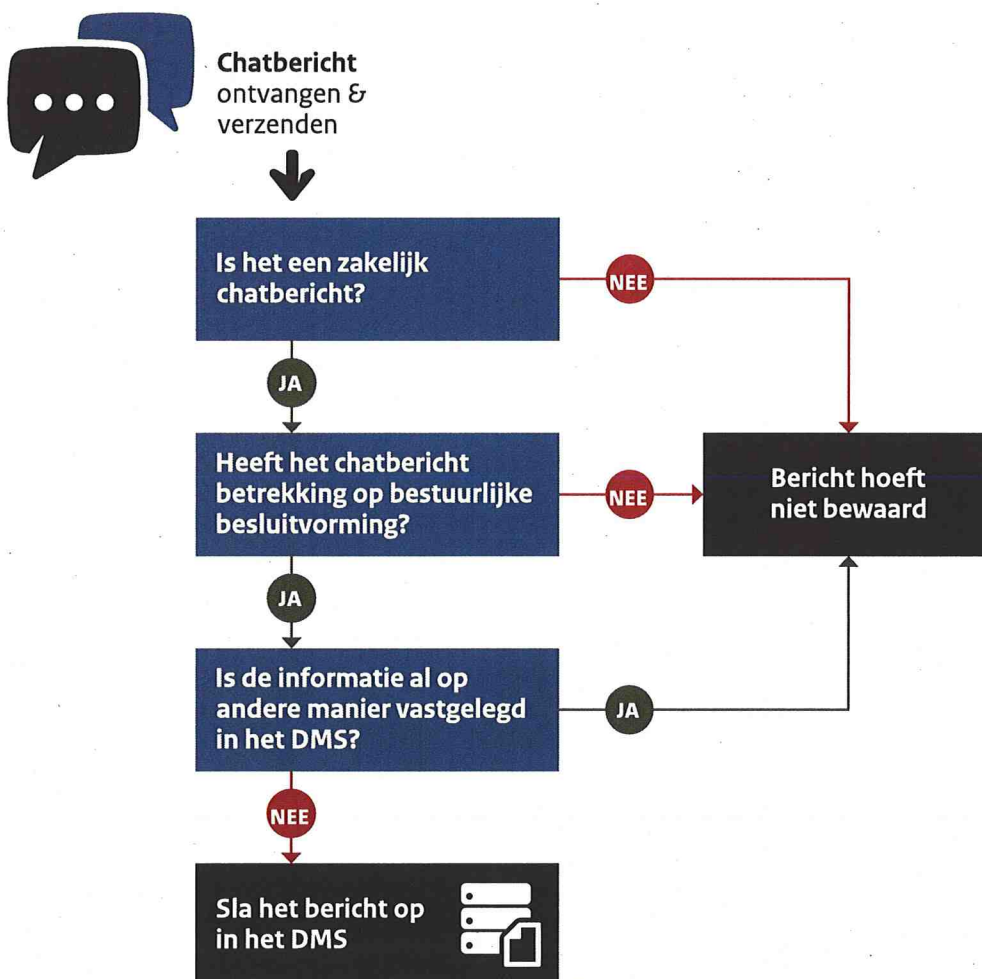
Op 3 juli is door RDDI en het ministerie BZK (CIO Rijk) aan het SG-overleg een technische handleiding opgeleverd voor het (handmatig) exporteren van chatberichten bij de Rijksoverheid. De instructie beschrijft hoe chatberichten veiliggesteld kunnen worden en ondersteunt gebruikers bij het exporteren van chatberichten uit mobiele telefoons en de opslag in DMS.

Instructie bewaren chatberichten

Op 6 december 2019 is in het SG-overleg een rijksbrede instructie voor het bewaren van chatberichten vastgesteld. Deze instructie beschrijft op inhoud welke berichten in ieder geval moeten worden opgeslagen (en verwijderd) conform het rijksbeleid.

- Berichten die betrekking hebben op 'bestuurlijke besluitvorming'⁸ moeten worden bewaard;
- Als de informatie uit het bericht al in een ander document zoals een nota of een e-mail is vastgelegd en opgeslagen, hoeft het niet te worden bewaard;
- Niet iedereen hoeft alle berichten te bewaren; hierover kunnen afspraken worden gemaakt.

Zie de figuur op deze pagina voor een schematische weergave van de instructie. De volledige tekst is terug te lezen in bijlage 4.



⁸ Bestuurlijke besluitvorming valt onder het begrip 'bestuurlijke aangelegenheden' uit de Wob. In de instructie is gekozen voor bestuurlijke besluitvorming, zodat met een kleinere beheerslast, er recht gedaan wordt aan het belang dat gediend wordt met het bewaren van de overheidsinformatie, namelijk ter publieke controle en verantwoording.

3 Bewaren van chatberichten

Dit hoofdstuk biedt handvatten en richtlijnen voor het bewaren van chatberichten bij rijksorganisaties. Deze richtlijnen zijn onderverdeeld in zeven vragen die van belang zijn om chatberichten te bewaren binnen de geldende kaders:



3.1 Welke berichten bewaren?

Alle chatberichten die van belang zijn voor de reconstructie van bestuurlijke besluitvorming moeten worden opslagen, tenzij de inhoud van het bericht al op een andere manier is vastgelegd. Van deze chatberichten moet minimaal de volgende informatie worden bewaard:

- Het bericht met het besluit zelf;
- De berichten die duidelijk maken waarover een besluit wordt genomen;
- De berichten die duidelijk maken wat de onderbouwing is van het besluit;
- Relevante informatie die aan het besluit voorafging en die aanleiding kan zijn voor het besluit;
- De ontvanger en verzender van het bericht;
- Het tijdstip waarop het bericht is verzonden of ontvangen.

In deze handreiking wordt onder bestuurlijke besluitvorming verstaan:

Berichten die onderdeel uitmaken van (de toekomstige reconstructie) van besluitvorming in zaken/ dossiers met maatschappelijke, politiek-bestuurlijke, financiële, juridische en of organisatorische consequenties die voortvloeien uit overheidshandelen.

3.2 Wiens berichten bewaren?

Bestuurlijke besluitvorming kan op ieder niveau plaatsvinden. Van de minister of staatssecretaris die besluit in een ingewikkeld dossier tot een directeur die in een crisissituatie zijn besluit doorgeeft of een projectmanager die via WhatsApp afspraken maakt met leveranciers. In principe geldt dus:

Uitgangspunt

Berichten van alle rijksmedewerkers moeten worden opgeslagen, als ze over bestuurlijke besluitvorming gaan.

Voor de politieke en ambtelijke top is extra aandacht nodig. Gezien de aard van hun functie is de kans bij hen het grootst dat er informatie over bestuurlijke besluitvorming in hun berichten voorkomt. RDDI adviseert rijksorganisaties om voor deze doelgroep extra maatregelen te treffen, bijvoorbeeld in de vorm van aanvullende persoonlijke of technische ondersteuning, Wob- en informatiebeheer adviseurs of specifieke instructies en handleidingen.

3.3 Wie bewaart?

De *Instructie bewaren chatberichten* (bijlage 4) belegt de verantwoordelijkheid voor het bewaren van relevante chatberichten bij de inhoudelijk verantwoordelijke dossierhouder. Voor de situatie waarin de dossiereigenaar niet zelf betrokken is bij de chatconversatie is bepaald dat rijksorganisaties hier zelf afspraken over moeten maken.⁹

Wanneer de dossierhouder zelf niet betrokken is bij de chatconversatie, geldt de volgende richtlijn:

- Iedere rijksmedewerker is zelf verantwoordelijk voor het opslaan van relevante chatberichten;
- In een chatgesprek met meerdere deelnemers ligt de verantwoordelijkheid voor het opslaan bij de deelnemer die binnen de organisatie hiërarchisch gezien het laagst in rang is. De deelnemers moeten hier onderling afspraken over maken;
- Bewindspersonen hoeven alleen berichten te bewaren die niemand anders in de organisatie heeft, bijvoorbeeld omdat er met een extern iemand is gechat.

De medewerker is als deelnemer aan de chatconversatie als enige in staat om goed in te schatten welke berichten bij de reconstructie van bestuurlijke besluitvorming van belang zijn en dus bewaard moeten worden. Het beleggen van deze verantwoordelijkheid bij anderen¹⁰ brengt het risico met zich mee dat er teveel of te weinig wordt gearchiveerd.

3.4 Hoe bewaren?

Er zijn verschillende manieren om chatberichten op te slaan: via screenshots, een export of met behulp van een "mobile archiver". Alle drie deze opties worden in deze paragraaf toegelicht, zodat rijksorganisaties zelf kunnen kiezen welke variant voor hen het beste werkt¹¹.

Het *Informatieblad archiveren chatberichten* van het Nationaal Archief biedt meer informatie over de verschillende werkwijzen en methoden¹² voor het bewaren van chatberichten.

Criteria methoden	Screenshot	Export	Mobile Archiver
Bestandstypen	.JPG	.TXT	XRY, XML, PDF
Bijlages	Nee	Ja	Ja
Methode geschikt voor	Alle berichtenapps	• WhatsApp (Iphone en Android) • Signal (Android)	Alle berichtenapps
Mate van arbeidsintensie opslaan	Medium	Laag	Afhankelijk van volledig uitlezen / selectie maken
Mate van arbeidsintensie beheer (Wob)	Hoog	Laag	Laag

⁹ Waar het uiteindelijk om gaat is dat de inhoudelijke verantwoordelijke dossierhouder kennis heeft van (de inhoud van) de chatsessie inzake de bestuurlijke besluitvorming en dat deze informatie geborgd is binnen de organisatie.

¹⁰ In de praktijk zullen specifieke groepen functionarissen de taak voor het bewaren van de chatberichten bij iemand anders kunnen beleggen vanwege de tijd die het in beslag neemt en de benodigde expertise. Bijvoorbeeld bij het secretariaat, een ondersteunende dienst zoals DIV/DIM of IV of een combinatie hiervan.

¹¹ Een aantal berichtenapps bieden aanvullende "enterprise" functionaliteit voor het centraal beheren van gegevens. Dit alternatief is in deze handreiking niet uitgewerkt omdat het onderzoek hiernaar nog loopt.

¹² Per ict-dienstverlener kan het verschillen of de voorgestelde methode ook daadwerkelijk in deze vorm kan worden uitgevoerd.

Criteria methoden	Screenshot	Export	Mobile Archiver
Kansen	• Privé en werk te scheiden • Redelijk eenvoudige instructie • Niet eenvoudig aan te passen wat ten goede komt van authenticiteit	• Eenvoudige instructie • Eenvoudig deelbaar • Metadata wordt meegeleverd • TXT formaat is te indexeren en dus ook doorzoekbaar in het DMS	• Veel verschillende functionaliteiten • Veel mogelijkheden voor ondersteuning en inbedding binnen de organisatie • Gemakkelijk duurzaam en toegankelijk op te slaan
Risico's	• Arbeidsintensief bij lange conversaties • Formaat is niet automatisch te indexeren en dus slecht doorzoekbaar in het DMS • Contextinformatie moeilijk te linken • Mogelijk gebruik van "nicknames" • Bijlages ontbreken	• Arbeidsintensief bij korte conversaties (Met name het opschonen) • Niet mogelijk bij Signal (IOS) / Threema • Mogelijk gebruik van "nicknames" • TXT-bestanden zijn gemakkelijk aanpasbaar.	• Locatieafhankelijk • Nog niet beproefd • Kosten voor aanschaf en beheer.

LET OP - Vanwege de aard van het communicatiemiddel (berichtenapps) en de te bewaren informatie (chatberichten) geldt dat alle drie de opties risico's met zich meebrengen op het gebied van privacy en beveiliging.

Optie 1 - Screenshot

Met de telefoon kun je eenvoudig screenshots maken van chatberichten, die de dossierhouder op kan slaan in het DMS. De screenshots worden via de e-mail naar het e-mailadres van de gegevensverantwoordelijke of (indien bekend) verantwoordelijke dossierhouder verzonden om vervolgens te worden geregistreerd en opgeslagen in het DMS onder het desbetreffende dossier.



Voordelen	Nadelen
Het is eenvoudig en kan met elke telefoon en voor elke app.	Bij langere chatconversaties zijn veel screenshots nodig en het samenhangend opslaan daarvan is veel werk.
De weergave van een screenshot is vergelijkbaar met de weergave op de telefoon waardoor aanvullende gegevens zoals emoticons en leesbevestigingen ook veilig gesteld worden.	Berichten zijn niet (automatisch) geïndexeerd en dus niet doorzoekbaar in het DMS.
	Metadata zoals de gegevenseigenaar moet handmatig worden toegevoegd, omdat alleen de gegevens van de gesprekspartner zichtbaar is in de screenshot.
	Selectie van de berichten wordt aan het oordeel van de gegevenshouder overgelaten waardoor de volledigheid en authenticiteit van een chatgesprek achteraf moeilijk na te gaan is.
	Bijlagen (aanvullende media) uit chatconversaties moeten separaat worden veiliggesteld.

Optie 2 - Export

In WhatsApp en Signal (alleen bij Android) kun je chats exporteren, inclusief de bijlagen. Het resultaat is een TXT-bestand, dat in een pdf kan worden omgezet. Ook kunnen op deze manier eventuele bijlagen worden veiliggesteld. Na ontvangst moet de gebruiker het zipbestand uitpakken, de berichten die niet relevant zijn verwijderen uit het TXT-bestand, vervolgens het TXT-bestand omzetten naar een PDF en deze samen met de bijlagen opslaan in het DMS.



Voordelen	Nadelen
Opschonen van de chatconversatie is mogelijk waardoor alleen relevante chatberichten worden opgeslagen in DMS	Arbeidsintensief bij korte chatconversaties.
Aanvullende metadata komt mee, waaronder de gegevens van geveenseigenaar en van de gesprekspartner.	Niet mogelijk bij Signal (IOS) en Threema.
Exports zijn eenvoudig te indexeren en dus ook doorzoekbaar in het DMS.	Export is TXT-bestand en gemakkelijk aanpasbaar. Risico voor de betrouwbaarheid en authenticiteit in het gedrang komt.
	Berichten moeten handmatig worden geselecteerd en verwijderd.
	Exportfunctie werkt niet met alle mailapplicaties, waardoor het niet mogelijk is om een export te verzenden via sommige mobiele werkomgevingen bij de Rijksoverheid.
	Niet alle informatieobjecten kunnen veiliggesteld worden. Bepaalde emoticons, audiobestanden, en ontvangst-of leesbevestigingen worden bijvoorbeeld niet meegenomen.

Optie 3 - "Mobile Archiver"

Er zijn verschillende technische oplossingen op de markt om het veiligstellen van chatberichten te vergemakkelijken. Een "mobile archiver" is een apparaat met software waaraan telefoons worden gekoppeld, die de berichten in ongeveer 10 minuten uitleest. Vervolgens kunnen de relevante berichten worden geselecteerd en veiliggesteld op een goed beveiligde server, DMS of harde schijf. De "mobile archiver" biedt verschillende bestandsformaten en weergaves om een duurzame en toegankelijke opslag van berichten te garanderen. De juiste metadata kan samen met het chatbericht worden meegezonden en gelijk worden opgeslagen in een DMS in machine leesbare formaten, zoals XML en PDF.

Op dit moment wordt deze software nog niet gebruikt voor het bewaren van berichten in het kader van de Wob, RDDI en het ministerie van JenV onderzoeken momenteel de mogelijkheden hiervoor. De resultaten van deze pilot zullen rijksbreed worden gedeeld middels een rapportage. Een oplossing zoals een mobile archiver kan met de nodige ondersteuning worden ingepast binnen een organisatie en daarmee kunnen verschillende processen worden ingericht om berichten veilig te stellen en te selecteren.

3.5 Waar bewaren?

Waar moeten chatberichten worden opgeslagen? Volgens de rijksbrede instructie moeten de berichten worden opgeslagen in het Document Management Systeem (DMS) van de rijksorganisatie. In het DMS:

- Is de informatie vindbaar en toegankelijk;
- Kunnen de informatie en bijbehorende persoonsgegevens worden afgeschermd om tegemoet te komen aan de AVG.

Voor de ordening binnen het DMS heeft de organisatie twee mogelijkheden, die in deze paragraaf worden toegelicht.

Hieronder wordt een tweetal varianten voor het ordenen van chatberichten in het DMS uiteengezet, inclusief voor- en nadelen.

Optie 1 - Zaak-/procesdossiers

Veel rijksorganisaties ordenen hun informatie op basis van zaak- of procesdossiers. Berichten worden in dit geval opgeslagen in het dossier van het desbetreffende onderwerp. De inhoud is hier dus leidend: per zaak, proces of onderwerp staat alle informatie bij elkaar in één dossier.

Voordelen	Nadelen
• Deze ordening past bij de manier waarop veel Rijksorganisatie hun informatiebeheer, beleid (selectielijst) en werkwijze (GWR) hebben ingericht.	• Het kan lastig zijn te achterhalen in welk proces- of zaakdossier de chatberichten moeten worden bewaard en/of wie de dossiereigenaar is. Dit kost tijd en kan ertoe leiden dat chatberichten in beperkte mate worden bewaard.
• De informatie komt altijd terecht bij de verantwoordelijke dossierhouder.	

Optie 2 - Persoonsdossiers

Een andere mogelijkheid is het bewaren van chatberichten in het dossier van de gegevensverantwoordelijke. De dossiers worden dan geordend rond personen binnen de organisatie, waarin al hun relevante berichten worden opgeslagen.

Voordelen	Nadelen
De gegevensverantwoordelijke (eigenaar) hoeft niet te (onder)zoeken in welk proces of zaakdossier de (informatie uit) chatberichten moet worden opgeslagen. Hij heeft al zijn berichten bij elkaar in zijn eigen dossier.	Deze ordening sluit niet aan bij de algemene ordening van de informatiehuishouding bij de Rijksoverheid en is daarmee niet in lijn met de geldende selectielijst.
	Beperkt duurzaam toegankelijkheid van de (informatie uit) chatberichten. Wanneer informatie op onderwerp of dossier wordt gezocht, is deze bij een ordening in persoonsdossiers moeilijker te vinden.

3.6 Wanneer bewaren?

Uitgangspunt

Het bewaren van chatberichten moet consequent en frequent worden uitgevoerd door dossierhouders en gegevensverantwoordelijken. Belangrijk aandachtspunt hierbij is dat hoe langer je wacht, des te groter de kans dat relevante chatberichten over het hoofd worden gezien of dat de context van een bericht verdwijnt.

Het is verstandig om minimaal wekelijks een moment in te plannen om chatberichten over bestuurlijke besluitvorming te bewaren. Hoe langer er namelijk wordt gewacht, des te groter de kans dat relevante chatberichten over het hoofd worden gezien of dat de context van een bericht verdwijnt. Ter ondersteuning bij het dagelijkse gebruik kunnen relevante chatberichten in WhatsApp met een sterretje worden gemarkeerd. Vervolgens worden deze berichten eens per week geëxporteerd conform één van de werkwijzen die zijn beschreven in paragraaf 3.3 en opgeslagen in het DMS. Dagelijks opslaan heeft de voorkeur, omdat de context nog vers in het hoofd zit, maar dat is gezien de praktijk van de omgang met berichtenapps vaak niet haalbaar.

LET OP - Chatberichten die er nog zijn als een Wob-verzoek binnenkomt moeten altijd bewaard blijven tot het gehele traject (inclusief vervolgprocedures) is afgerond.

3.7 Verwijderen?

Uitgangspunt

De chathistorie van gebruikers wordt consequent en frequent verwijderd, nadat de chatberichten inzake bestuurlijke besluitvorming zijn bewaard in het DMS.

Het verwijderen van chatberichten is belangrijk om op termijn op een efficiënte manier te voldoen aan de Wob. Bij een Wob-verzoek moeten namelijk alle berichten worden verstrekt, die op dat moment binnen de organisatie aanwezig zijn. Dus ook de berichten die nog op de mobiele telefoons van werknemers staan. Een zoekactie op alle telefoons van de Rijksorganisatie is echter niet werkbaar. Het heeft dan ook de voorkeur om continu (direct na de conversatie) of minimaal dagelijks alle chatberichten te verwijderen van de mobiele telefoons, nadat de relevante berichten zijn opgeslagen in het DMS.

LET OP - Gedurende de looptijd van een Wob-traject, inclusief vervolgpcedures, gelden bijzondere eisen ten aanzien van het bewaren van documenten (dus ook chatberichten). Berichten mogen op dat moment bijvoorbeeld niet meer verwijderd worden.

4 Proces van bewaren

Uiteindelijk is de precieze invulling van het proces van bewaren afhankelijk van de organisatie, haar situatie en behoeften. Elke Rijksorganisatie vertaalt de rijkskaders naar een invulling die past bij de organisatiestructuur, cultuur en/of de verschillende doelgroepen¹³.

Een belangrijk uitgangspunt hierbij is dat het bewaarproces specifieke rollen en taken kent die door verschillende expertises en doelgroepen worden uitgevoerd. Denk hierbij aan technische support, functionele en privacy adviseurs, maar ook de eindgebruikers zoals directiesecretarissen, dossierhouders en Wob-specialisten. Al deze disciplines maken een soepele en doeltreffende werkwijze voor het bewaren van chatberichten mogelijk.

Dit hoofdstuk beschrijft het proces van het *bewaren van chatberichten* en geeft handvatten omtrent de manier waarop dit bij rijksorganisaties in de praktijk vorm kan worden gegeven.

Doel

Het bewaren van chatberichten is primair gericht op het duurzaam toegankelijk houden en beschikbaar hebben van informatie uit chatberichten. Dit draagt eraan bij dat deze informatie:

- Effectief en efficiënt openbaar kan worden gemaakt, bijvoorbeeld bij Wob-verzoeken;
- Gemakkelijk beschikbaar is in de organisatie en haar werkprocessen;
- Beschikbaar is voor cultuur-historisch onderzoek door derden.

In het vervolg van dit hoofdstuk worden verschillende aspecten van het proces verder uitgelicht. We gaan achtereenvolgens in op:

Procesoverzicht	Een kort overzicht van de achtereenvolgende stappen bij het bewaren van chatberichten
Actoren	Een overzicht van de actoren die een rol spelen bij het bewaren van chatberichten
Verdieping processtappen	Een nadere toelichting van de processtappen

¹³ Chatberichten met bestuurlijke besluitvorming bevinden zich voornamelijk in chatconversaties van de politieke en bestuurlijke top. Rijksorganisaties lopen bij de chatconversaties van deze doelgroep het grootste risico dat de informatie niet beschikbaar is voor de behandeling van Wob-verzoeken. Een zorgvuldig ingericht bewaarproces is daarom ook van het grootste belang.

4.1 Procesoverzicht

Bij het bewaren van chatberichten worden de volgende stappen doorlopen:

1 Identificeren	Het herkennen van de inhoud van een chatbericht als bestuurlijke besluitvorming
2 Selecteren	Het vaststellen dat de informatie in de chatconversatie moet worden bewaard omdat het besluitvorming betreft en niet op andere wijze is vastgelegd in het DMS
3 Exporteren	Het overbrengen van het chatbericht of de chatberichten uit de berichtenapp naar een daarvoor aangewezen locatie
4 Transformeren*	<i>Het omzetten van het chatbericht naar een ander formaat en/of het uitsplitsen van chatberichten om ze over te brengen naar verschillende dossiers</i>
5 Registreren	Het autoriseren van de geëxporteerde informatie door de gegevensverantwoordelijke en vastleggen van de juiste metadatatagegevens, toegangsbeveiliging en bestandsformaten voor het DMS
6 Opslaan	Het vastleggen van de informatie uit het chatbericht in het DMS

* Stap 4, Transformeren is een inrichtingskeuze en derhalve optioneel.

4.2 Actoren

Bij het bewaren van chatberichten kunnen de volgende actoren (procesrollen) met bijbehorende taken en rollen worden onderscheiden:

A. Gegevensverantwoordelijke

De verzender/ontvanger van chatberichten die bestuurlijke besluitvorming bevatten en daarmee de eindverantwoordelijke persoon voor het bewaren van chatberichten.

B. Directe ondersteuner

De persoonlijk adviseur, assistent of secretariaat die door de gegevensverantwoordelijke gemandateerd wordt en verantwoordelijk is voor het uitvoeren van processtappen bij het bewaren van chatberichten.

C. Dossierhouder

De eigenaar van het dossier waar het chatbericht betrekking op heeft. Een dossierhouder draagt de verantwoordelijkheid om de relevante chatberichten voor zijn dossier in een goede geordende staat op te slaan.

D. Inhoudelijk adviseur

(a) De Wob-jurist en/of -specialist en (b) de DIV/DIM professional. Een inhoudelijk adviseur die de gegevensverantwoordelijke advies geeft over (a) de interpretatie van bestuurlijke besluitvorming en (b) informatiebeheer van chatberichten.

E. Technische support

De “berichtenapp-specialist” vanuit IV/DIV/DIM of ICT. Een inhoudelijk adviseur kan de gegevensverantwoordelijke ondersteunen bij functionele of technische vragen.

F. Beheerder DMS

De applicatie- of functioneel beheerder van het DMS. De functioneel adviseur geeft de gegevensverantwoordelijke advies bij functionele of technische vragen over het DMS.

G. Privacy-adviseur

De AVG-specialist weet hoe gedurende het hele proces verantwoord kan worden omgegaan met persoonsgegevens. De privacy-adviseur geeft advies over de maatregelen om de privacy te waarborgen.

	Identificeren	selecteren	exporteren	transformeren	registreren	opslaan
Gegevensverantwoordelijke	●	●	●	●	●	●
Directe ondersteuning	●	●	●	●	●	●
Dossierhouder						●
Inhoudelijk adviseur	●	●				
Technisch support		●	●	●		
Functioneel adviseur				●	●	●
Privacy-adviseur	●	●	●	●	●	●

LEGENDA

De actor is verantwoordelijk voor de **Blauwe** [●] processtappen, kan deze verantwoordelijkheid mandateren aan **Groen** [●] en kan ondersteund worden door **Paars** [●].

4.3 Toelichting processtappen

Om rijksorganisaties op weg te helpen bij het inrichten van het bewaren van chatberichten worden de processtappen uit paragraaf 4.1 hieronder verder toegelicht.

Stap 1 en 2 - Inrichting t.b.v. identificeren en selecteren

Het identificeren en selecteren wordt idealiter door de gegevensverantwoordelijke zelf uitgevoerd.

Deze kan (al dan niet in overleg met de dossierhouder) het beste inschatten:

- Of het om bestuurlijke besluitvorming gaat;
- Of de informatie belangrijk is binnen de context van het dossier;
- Of de informatie op korte of lange termijn belangrijk is (of kan worden) in het kader van Wob-verzoeken. Ook kunnen doorgaans alleen gegevenseigenaren het belang van bewaren¹⁴ beoordelen binnen de context van het dossier, al dan niet in overleg met de dossierhouder.

Voor bepaalde groepen gegevenseigenaren (bijvoorbeeld de politieke en ambtelijke top) kan het identificeren en selecteren van chatberichten eventueel door een directe ondersteuner worden uitgevoerd. Hier kleven wel risico's aan: in de regel heeft de directe ondersteuner een beperkter inzicht in de intenties en belangen dan de gegevensverantwoordelijke die betrokken is bij de chatconversatie. Daarnaast zou de

¹⁴ Niet alleen bij bestuurlijke besluitvorming is het van belang om de chatberichten te bewaren. Ook politieke, bestuurlijke, maatschappelijke of procesrisico's kunnen aanleiding geven om chatberichten op te slaan.

directe ondersteuner inzicht kunnen krijgen in de privé-gesprekken van de gegevensverantwoordelijke, wat privacyrisico's met zich meebrengt.

Op microniveau is geen omschrijving te geven welke berichten nu precies wel of niet moeten worden geïdentificeerd en geselecteerd. Het is daarom raadzaam om voor ondersteuning te zorgen vanuit afdelingen die zich bezig houden met informatiebeheer, privacy en Wob-gerelateerde zaken, als het onduidelijk is welke chatberichten moeten worden bewaard en welke niet worden bewaard.

Stap 3 en 4 - Inrichting t.b.v. Exporteren en transformeren

Hoe de chatberichten van mobiele telefoons worden geëxporteerd is afhankelijk van de keuzes¹⁵ die de individuele rijksorganisaties daarbij zelf maken, (zie paragraaf 3.3). Hierbij is het in ieder geval belangrijk dat de gegevensverantwoordelijke (of directe ondersteuner/dossierhouder) zoveel mogelijk de contextgegevens rondom de bestuurlijke besluitvorming overbrengt, zoals de verzender, ontvangen datum en tijdstip van versturen. Alleen met deze gegevens is een goede reconstructie van de besluitvorming mogelijk voor onder andere het inwilligen van Wob-verzoeken.

Een ander aandachtspunt is dat de gemiddelde rijksmedewerker niet bekend is met het exporteren van chatberichten uit mobiele telefoons. Het is dan ook raadzaam dat rijksorganisaties praktische gebruikershandleidingen en/of instructievideo's beschikbaar stellen. Daarmee kunnen rijksmedewerkers deze stap eenvoudiger uitvoeren.

Voor het versturen van de geëxporteerde informatie uit een berichtenapp (inclusief contextgegevens) zijn verschillende mogelijkheden. De gegevensverantwoordelijke (of diens directe ondersteuner) kan de export versturen naar:

- a. Het eigen zakelijke mailadres om vervolgens de informatie op te slaan in een dossier;
- b. Het zakelijke mailadres van een directe ondersteuner of een "postbus" van waaruit de mails met relevante chatberichten worden getransformeerd en opgeslagen in (verschillende) dossiers;
- c. Het zakelijke mailadres van de verantwoordelijke dossierhouder die de informatie zelf opslaat in het dossier.

Voordeel van werkwijze c. is dat de inhoudelijk verantwoordelijke dossierhouder kennis heeft van (de inhoud van) de chatsessie over de bestuurlijke besluitvorming en deze informatie op de juiste plaats, met de juiste gegevens en autorisaties borgt binnen het DMS van de organisatie.

Stap 5 en 6 - Inrichting t.b.v. registreren en opslaan

Relevante informatie moet op de juiste manier worden bewaard in het DMS, bij het relevante persoons- of zaakdossier (zie paragraaf 3.4). Dit houdt ook in dat:

- Ook de contextuele metagegevens worden opgeslagen;
- De juiste toegangsbeveiliging wordt toegepast (i.v.m. vertrouwelijkheid en/of privacygevoeligheid);
- Wordt opgeslagen in het juiste bestandsformaat (bij voorkeur PDF/A2).

LET OP - wanneer de chatberichten niet door de gebruiker of gegevensverantwoordelijke zelf zijn geëxporteerd (maar bijvoorbeeld door een ondersteuner), moet de gegevensverantwoordelijke na de export verifiëren dan wel autoriseren dat de opgeslagen chatberichten kloppen, oftewel integer en authentiek zijn.

De inhoudelijke en privacy-adviseurs kunnen hiervoor ondersteuning bieden.

¹⁵ Bij enkele rijksorganisaties is het systeemtechnisch mogelijk om een export van chatberichten te maken vanuit WhatsApp en deze vervolgens vanuit de werkmail te sturen naar 'eigen' zakelijke e-mailadres.

Bijlage 1

Doelgroep, definities en referentiedocumenten

Doelgroep

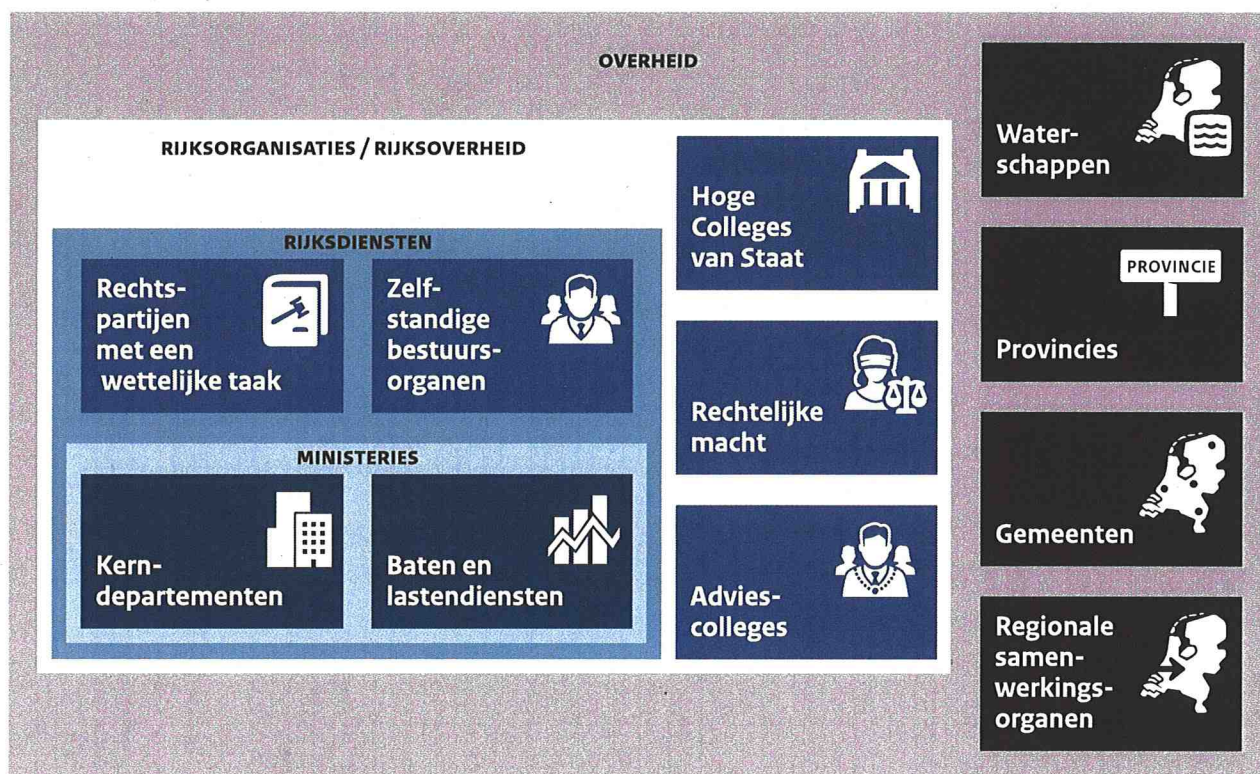
De handreiking is specifiek bedoeld voor adviseurs binnen de Rijksoverheid die verantwoordelijk zijn voor (het organiseren van) het bewaren van chatberichten en/of betrokken zijn bij de behandeling van Wob-verzoeken zoals documentaire informatieadviseurs, informatiemanagers en -beheerders, auditors, proces- of informatieanalisten en adviseurs digitale archivering. Ook voor managers en projectleiders die verantwoordelijk zijn voor de inrichting van werkprocessen en bijbehorende informatiesystemen levert deze richtlijn uitgangspunten op bij het uitvoeren van de nieuwe beleidslijn.

Definities

In de handreiking worden enkele begrippen gebruikt die om nadere toelichting en/of duiding vragen:

- **Berichtenapps**
Besloten kanalen, gekoppeld aan mobiele telefoonnummers, voor het uitwisselen van berichten via internet tussen individuen of kleine groepen middels applicaties op smartphones (hoewel sommige berichtenapps op desktop zijn te gebruiken). Voorbeelden zijn: WhatsApp, SMS, Signal, Threema, maar ook iMessage, WeChat, Skype en Facebook messenger.
- **Chatberichten**
Alle berichten ongeacht hun vorm (tekst, audio, video, bijlagen of hyperlinks) die verzonden worden via een berichtenapp.
- **Bewaren**
Het hele proces van identificeren van een relevant bericht tot het opslaan in een beheerde omgeving.
- **Opslaan**
Een of meerdere chatberichten voor duurzame en toegankelijke bewaring plaatsen in een beheerde omgeving.
- **Schiften**
Een microselectie maken van de chatberichten die in aanmerking komen voor opslaan in het DMS of verwijderen.

Rijksoverheid



Referentiedocumenten / Bronverwijzingen

Referentiedocument	Bronverwijzing
Uitspraak 201800258/1/A3 (Ministerie VWS – BTN)	https://www.raadvanstate.nl/@114477/201800258-1-a3/
Informatieblad archiveren chatberichten	https://www.nationaalarchief.nl/archiveren/informatieblad-archiveren-chatberichten
Beleidslijn CIO Beraad Berichtenapps	Zie bijlage 1
Beleidsadvies en aanpak Berichtendiensten Rijksoverheid	Zie bijlage 2 voor de conclusie
Instructie bewaren chatberichten	Zie bijlage 3

Bijlage 2

Rijksbrede beleidslijn (CIO-Beraad)

Vastgesteld door het CIO beraad op 7 februari 2018

Binnen de Rijksoverheid wordt het gebruik van berichtenapps ontraden voor communicatie over bestuurlijke aangelegenheden. Er zijn momenteel meerdere publiek beschikbare berichtenapps die, door de toepassing van encryptie, meer beveiliging bieden dan onversleutelde sms. Te denken valt hierbij aan apps zoals Signal, WhatsApp, Threema en BlackBerry Connect.

Afhankelijk van de situatie waarin deze apps gebruikt worden, kunnen de voor- en nadelen van de ene app zwaarder wegen dan de andere (zie de voor- en nadelen van de apps zoals verwoord in de bijlage). Er wordt daarom niet rijksbreed opgelegd welke berichtenapp gebruikt mag worden. Mocht een berichtenapp toch gebruikt worden voor communicatie over bestuurlijke aangelegenheden, dan is deze communicatie onderhevig aan de gangbare eisen van archivering en openbaarheid. Met het oog op deze eisen en eisen van informatiebeveiliging mag er dus zeker geen gevoelige of gerubriceerde informatie in staan. Er zijn andere producten beschikbaar die door het NBV zijn goedgekeurd voor het communiceren van gerubriceerde informatie. Voor de omgang en archivering van digitale berichten is de 'Gedragsregeling voor de digitale werkomgeving' van kracht.

Bijlage 3

Beleidsadvies en aanpak berichtenapps

Geaccordeerd door het SG-overleg op 3 juli 2019

Matrix integraal

	Ontraden van chatberichten	Toestaan en handmatig op stuksniveau schiften en exporteren ¹	Toestaan, maar gedifferentieerde aanpak ¹	Functionele scheiding, deels ontraden / deels toestaan ¹
1. Snelle inventarisatie is mogelijk (Wob)	5 ²	4	3	2,5
2. Selectiestrategie stelt informatie veilig (Wob/WOO/ Aw)	1	2	4	3
3. Informatie is duurzaam toegankelijk (Aw/WOO)	1	3	4	3 ⁴
4. Uitvoerbaarheid voor organisatie en medewerker	1	3	4	2
5. Vertrouwelijke c.q. gerubriceerde informatie is geborgd	5	2	2	2
6. Bescherming van privacy & verwerking gegevens (AVG)	5 ³	4		
SCORE	18	18	19	15,5

¹ M.u.v. gerubriceerde informatie en het zakelijk appen op een privé device. Eerder is al door de MR besloten dit allebei te verbieden.

² Belangrijke kanttekening hier is dat deze score alleen gehaald kan worden indien de score wordt nageleefd. Verwachting is dat dit niet of beperkt haalbaar is.

³ Indien beleid niet wordt nageleefd is de score 1. Dan worden persoonsgegevens alsnog verwerkt.

⁴ Score is laag (1) voor medewerker, maar hoog voor sleutelpersonen (5)

TOELICHTING OP SCORE - Score 1 = onvoldoende t/m score 5 = uitstekend

Advies

Uit de wegingsmatrix hierboven komt de risico-aanpak (optie 3) over het geheel genomen het beste uit de bus. Wij realiseren ons echter dat deze variant vergaande implicaties heeft voor de privacy van de sleutelfunctionarissen, die een mix van formeel zakelijke, informeel zakelijke, politieke, en ook persoonlijke informatie op hun devices hebben staan.

Omdat de berichten van de sleutelfunctionarissen in deze optie in bulk worden geoogst, en het vooraf schiften dus vervangen wordt door het op voorhand veilig stellen van het totaal aan informatie en achteraf doorzoeken, scoort deze variant dan ook laag op compliance met de AVG.

Wij adviseren daarom om over te gaan tot implementatie van de MR-voorkeursvariant: periodiek schiften op stuksniveau, en handmatig exporteren van de relevante informatie naar een DMS of mailbox.

De MR-variant leent zich goed voor snelle implementatie binnen de Rijksoverheid. Ze kan, indien nageleefd, leiden tot een beleidslijn die verdedigbaar is onder zowel Wob als Archiefwet, de belangrijkste richtlijnen voor informatiebeveiliging en de AVG. De aanpak is bovendien redelijk kostenefficiënt. Ons advies is dan ook om deze MR-variant de komende maanden uit te rollen, maar daarbij wel een drietal flankerende maatregelen te treffen, die toezien op het verlagen van de uitvoeringslasten en het vergroten van de kans op adequate naleving.

1. Beperk het gebruik van berichtenapps zo veel als mogelijk – en ontraad het voor bestuurlijke aangelegenheden.

De verwachting is dat bij implementatie de uitvoerbaarheid gering is door de hoge gebruikerslasten, met name voor de ambtelijke en politieke top en hun naaste adviseurs, maar ook voor andere ambtenaren. Indien naleving onvoldoende aantoonbaar is, kan bij rechtszaken mogelijk niet worden volgehouden dat inventarisatie van chatberichten uit het DMS voldoende is.

Wij adviseren daarom om bovenstaande aanpak in te voeren ondersteund door een **rijksbrede bewustwordingscampagne**, waarin ambtenaren aangespoord worden om bewust te communiceren en berichtenapps *zo min mogelijk* te gebruiken voor formeel zakelijke communicatie. Ambtenaren moeten zich bewust zijn van de risico's die gepaard gaan met het gebruik van een berichtenapp, en de hoge administratieve lasten die het periodiek schiften en vervolgens exporteren op stuksniveau met zich meebrengt, alsmede van het belang van het veiligstellen van informatie die omgaat in de media die zij gebruiken en het risico dat zij lopen als zij de informatie niet veilig stellen.

Dit vergroot niet alleen de naleving en daarmee het bestaan van een aantoonbaar uitgevoerde beleidslijn, maar beperkt ook de administratieve lasten en daarmee de kosten van de voorkeursvariant. Als er vrijwel geen relevante berichten meer verstuurd worden, dan kost schiften immers nog weinig tijd en hoeft er niets tot weinig geëxporteerd te worden. Naast een dergelijke eenmalige campagne zou er structureel meer aandacht moeten zijn voor dit onderwerp, bijvoorbeeld bij de introductiedag voor nieuwe medewerkers.

In het geval dat er toch via de berichtenapp gecommuniceerd wordt over bestuurlijke aangelegenheden, of bij twijfel over de aard van het bericht, dan is het belangrijk dat ambtenaren weten wat hen te doen staat. Dat betekent dat er een *technische instructie* voor het exporteren beschikbaar en algemeen bekend is, alsmede een *inhoudelijke instructie* die hulp biedt bij het individueel taxeren van de betreffende informatie: behoort het bericht inderdaad opgeslagen te worden in het Document Management Systeem (DMS), of is dat niet aan de orde?

Een voorbeeld van een technische en inhoudelijke instructie zijn bij deze white paper bijgevoegd. Wij adviseren deze documenten, indien het SG-overleg dit advies overneemt, door het RDDI in een volgende fase nog eens goed te laten controleren op bruikbaarheid in de praktijk.

2. Ontzorg daar waar mogelijk of gewenst

Er is op dit moment nog geen goede, gebruiksvriendelijke (technische) optie voor handen om berichten op stuksniveau te schiften en te exporteren. Zeker voor sleutelfunctionarissen (Bewindslieden, SG's, DG's, en hun staf), die weinig tijd hebben, veel gebruik maken van berichtenapps, en bovendien een hoog 'risico-profiel' hebben (de kans is groot dat hun berichten relevante informatie aangaande bestuurlijke aangelegenheden bevat), het betekenen dat zij veel tijd kwijt zijn met het doorwerken van de berichten die zij verzonden hebben en het op stuksniveau schiften, en afhankelijk van de hoeveelheid relevante informatie aangaande bestuurlijke aangelegenheden die zij verzonden hebben, ook nog aan het exporteren van die relevante berichten.

Een mogelijkheid om hen te ontzorgen, die op korte termijn en kostenefficiënt te realiseren is, betreft het beschikbaar stellen van een zogeheten mobile archiver op het departement: een apparaat met software waar de telefoons aan gekoppeld en vervolgens uitgelezen kunnen worden, en de berichten geëxporteerd en veilig gesteld worden op een goed beveiligde server of harde schijf. Deze software ondersteunt het selectief binnenhalen (en kan privé-chats uitsluiten).

Voordeel van deze aanpak is ook dat het sleutelfunctionarissen **beschermt** tegen verdenkingen dat zij (door zelf te schiften) informatie aan de openbaarheid onttrekken. Wel is extra aandacht voor de bescherming van de privacy van betrokkenen in de volgende fase noodzakelijk. Zo moet met het oog op de AVG de doelbinding voor toegang tot de betreffende informatie kraakhelder zijn, en gelijk aan die bij e-mail boxen nu het geval is: alleen bij Wob-verzoeken, parlementaire enquêtes en integriteitsonderzoeken en in beginsel met instemming van de gebruiker. Ook moet er aandacht zijn voor het personeel dat dan vervolgens toegang heeft om relevante berichten eruit te filteren op bijvoorbeeld naam en onderwerp. Dit moeten speciaal hiervoor getrainde en gecertificeerde medewerkers zijn.

NB. Een vergelijkbare aanpak is door het RDDI nu ook opgesteld voor e-mailboxen. De mailboxen van medewerkers van de Rijksoverheid worden allemaal overgebracht naar een externe, beveiligde server waar zij gedurende tien jaar worden bewaard. De mailboxen van sleutelfunctionarissen worden daarna met tijdelijke beperkingen van de openbaarheid overgebracht naar het Nationaal Archief.

3. Bouw op redelijk korte termijn een evaluatiemoment in

We adviseren aanvullend om een interdepartementaal **evaluatiemoment** in te bouwen om te bekijken of de gekozen aanpak werkt, en waar mogelijk **verbeteringen** door te voeren, en tegelijkertijd een aantal **alternatieven** voor het geautomatiseerd **exporteren en veilig stellen van informatie** verder uit te werken, alsmede een verdiepende slag uit te voeren op het wegingskader en de gekozen criteria. Met name op het gebied van uitvoerbaarheid, informatieveiligheid, privacy en duurzame toegankelijkheid.

Het is sowieso raadzaam om de aanpak dynamisch te houden, de technische ontwikkelingen op dit gebied gaan razendsnel. Een oplossing die op het moment van schrijven nog onmogelijk is, ligt misschien over een jaar binnen handbereik ligt. Zo is nu in de VS de app *Telemesssage* beschikbaar, een app op je telefoon die als een schil om WhatsApp draait en die de berichten binnen WhatsApp routeert via externe en beveiligde servers naar de departementale opslaglocatie waar de informatie wordt veilig gesteld. Mogelijk komt deze ook in Europa beschikbaar en biedt die een goede oplossing.

Bijlage 4

Instructie bewaren chatberichten

Vooraf

Het gebruik van digitale middelen biedt mogelijkheden die een zeker risicobesef vragen. In het bijzonder dient terughoudendheid te worden betracht bij het gebruik van WhatsApp en vergelijkbare diensten voor werkgerelateerde doeleinden en dient er altijd rekening te worden gehouden met de aard van de informatie.

Deze instructie heeft enkel betrekking op het bewaren van App en SMS-berichten (verder: chatberichten) en ziet niet op (het bewaren) van e-mails en andere documenten. Een chatbericht kan de vorm hebben van een geschreven bericht, afbeelding of een geluidsopname.

NB - Privé-berichten en interne "partijpolitieke" aangelegenheden hoeven sowieso niet te worden bewaard.

Welke chatberichten moeten worden bewaard?

Stap 1

Heeft het chatbericht betrekking op de 'bestuurlijke besluitvorming'?

- NEE, het bericht kan worden verwijderd
- JA, ga door naar stap 2

TOELICHTING - De meeste chatberichten die gewisseld worden in het kader van een bestuurlijke aangelegenheid, niet zijnde de besluitvorming zelf, betreffen vanwege de aard van het sociale medium enkel procesmatige of (betekenisloze) details. Aan dergelijke berichten komt geen zelfstandige betekenis aan toe, zodat het bewaren ervan niets zou toevoegen aan het belang dat gesteld wordt met het bewaren van overheidsinformatie, namelijk ter publieke controle en verantwoording. Om die reden wordt de selectie gericht op chatberichten die betrekking hebben op de 'bestuurlijke besluitvorming'.

Stap 2

Is de informatie uit het chatbericht al op een andere manier vastgelegd?

- JA, het bericht kan worden verwijderd
- NEE, het bericht moet worden bewaard. Ga door naar stap 3.

TOELICHTING - Relevante informatie in een chatbericht is in veel gevallen ook terug te vinden in andere documenten zoals e-mails, memo's en nota's. Uit oogpunt van deugdelijke en overzichtelijke dossiervorming hoeft die informatie niet dubbel bewaard te worden ('schiften van gelijksoortige informatie'). Controleer daarom of de informatie in het relevante chatbericht in enige vorm al is terug te vinden in een ander document. Is de relevante informatie in het chatbericht ook al terug te vinden in een ander document, dan kan het chatbericht worden verwijderd. Is dat niet het geval, dan moet het chatbericht worden bewaard en geëxporteerd naar het DMS. Zie hiertoe de technische instructie.

Stap 3

Een chatbericht kent een verzender en een ontvanger. Het is niet nodig dat binnen 1 bestuursorgaan beide hetzelfde chatbericht bewaren en zo nodig exporteren. Maak hierover heldere afspraken.

TOELICHTING - Uitgangspunt hierbij is dat de verantwoordelijkheid voor het bewaren van (de informatie in) het relevante chatbericht wordt belegd bij de inhoudelijk verantwoordelijke dossierhouder. Is diegene niet zelf betrokken bij de chatsessie dan draagt diens leidinggevende of organisatieverantwoordelijke daartoe zorg, afhankelijk van betrokkenheid bij de chatsessie. Waar het uiteindelijk om gaat is dat de inhoudelijke verantwoordelijke dossierhouder kennis heeft van (de inhoud van) de chatsessie inzake de bestuurlijke besluitvorming en deze informatie borgt binnen de organisatie. Bewindspersonen en de ambtelijke top hoeven *enkel* zorg te dragen voor berichten *die alleen zij hebben* (en dus qua inhoud niet ook al op een andere wijze zijn vastgelegd).

Ter illustratie

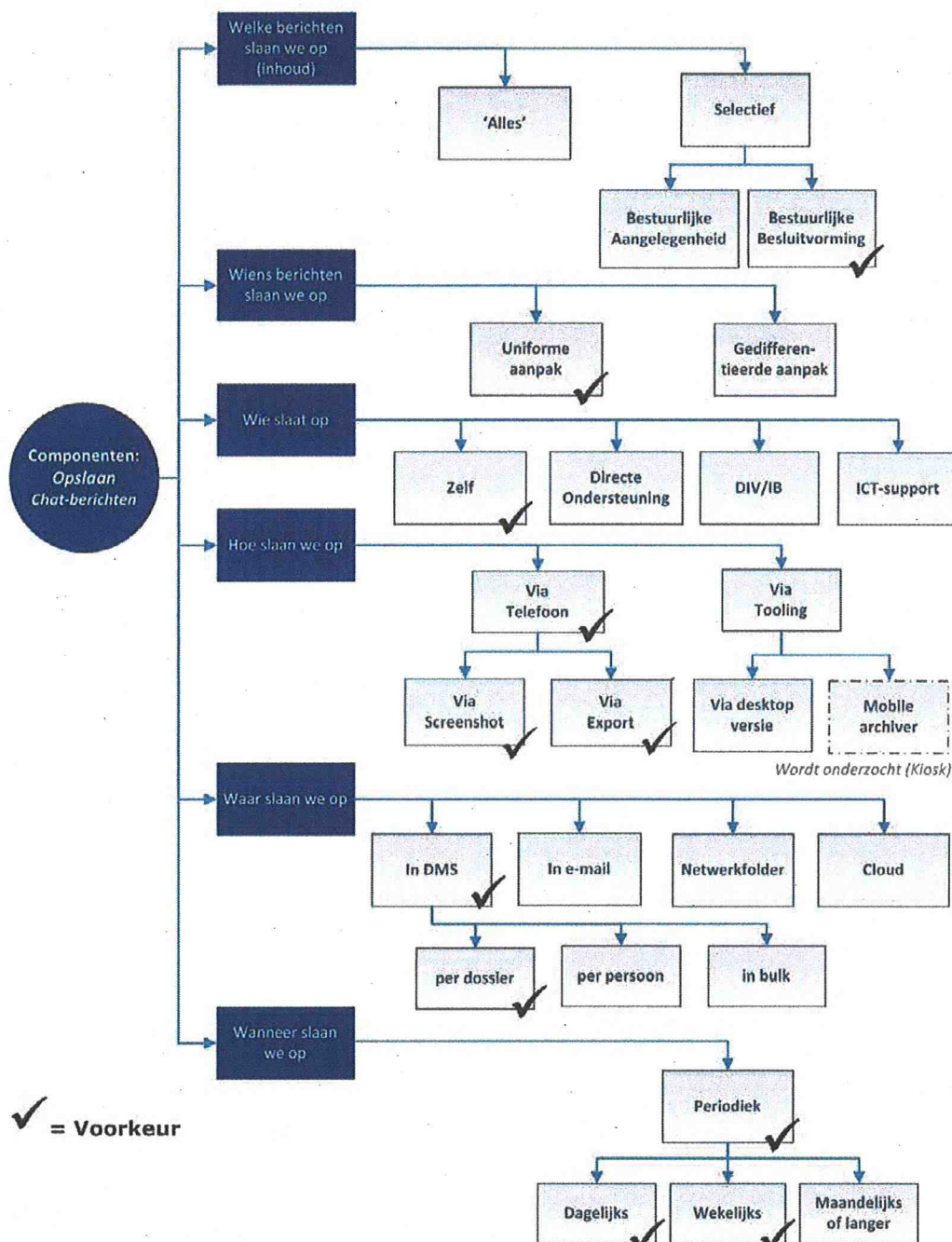
- Is de ambtelijk organisatie betrokken bij de chatconversatie met een of meerdere bewindspersonen of de ambtelijke top, dan regelt het ambtelijk veld dat er wordt bewaard;
- Zijn uitsluitend bewindspersonen en ambtelijke top betrokken bij de conversatie, dan regelt de ambtelijke top dit;
- Is uitsluitend de ambtelijke top betrokken bij de conversatie met externen (buiten het ministerie), dan moet de ambtelijke top dit regelen;
- Zijn uitsluitend bewindspersonen betrokken bij de conversatie (tussen bewindspersonen en/of met externe derden), dan dragen de bewindspersonen hiervoor zorg.

Meerdere personen en/of departementen betrokken

- Bij zogenaamde 'groepsapps' kan als uitgangspunt worden gehanteerd dat de 'beheerder' ervan zorg draagt voor het bewaren van de relevante informatie inzake (reconstructie van) de bestuurlijke besluitvorming;
- Bij betrokkenheid van meerdere departementen bij 1 chatconversatie ligt de verantwoordelijkheid voor het bewaren van de relevante chatberichten bij de departementen zelf.

Bijlage 5

Componenten: overzicht en richtlijnen



Bijlage 6

Annotatie uitspraak Raad van State

Uitspraak van 20 maart 2019 (ECLI:NL:RVS:2019:899) van de Afdeling bestuursrechtspraak van de Raad van State.

Noot M.A.J. West en F.C. van der Jagt

1. Deze Afdelingsuitspraak komt als slotakkoord na de Wob-uitspraak van de meervoudige kamer van de Rechtbank Midden-Nederland van 28 november 2017. In laatstgenoemde uitspraak werd voor het eerst geoordeeld dat sms- en WhatsApp-berichten als objecten onder de documentdefinitie van artikel 1 onder a van de Wob vallen, en daarmee door middel van een verzoek om informatie zijn op te vragen bij een bestuursorgaan, voor zover de berichten een bestuurlijke aangelegenheid behelzen. Dit heeft de nodige media-aandacht gekregen, en ook in dit tijdschrift is bij de rechtbankuitspraak stilgestaan (AB 2018/34, m.nt. M.A.J. West). Begin dit jaar heeft de Afdeling bestuursrechtspraak het oordeel van de Rechtbank Midden-Nederland in de kern bevestigd, met grote gevolgen voor de bestuurlijke praktijk, met name in de uitvoering.
2. Een document in de zin van de Wob is:
 - a. een schriftelijk stuk of ander materiaal dat gegevens bevat;
 - b. berustend bij een bestuursorgaan.
3. Bij de parlementaire behandeling van de Wob in 1986 werd al voorzien dat de techniek – omschreven als ‘de ontwikkeling van de computertechniek’ – naar verwachting tot nieuwe gegevensdragers zal leiden en daarmee tot ‘nieuwe’ documenten als bedoeld in de Wob (Kamerstukken II 1986/87, 19 859, nr. 3, p. 21). Aldus geschiedde. Vanwege de ruime betekenis die aan het begrip ‘document’ moet worden toegekend – in de memorie van toelichting omschreven als “niet alleen de door de overheidsorganen zelf gecreëerde stukken of ander materiaal” maar “ook alle van buiten komende stukken en ander voor overheidsorganen bestemd materiaal” (Kamerstukken II 1986/87, 19 859, nr. 3, p. 21) – vallen sms- en WhatsApp-berichten volgens de Afdeling bestuursrechtspraak onder de huidige documentdefinitie van de Wob. Het gaat om “een schriftelijk stuk of ander materiaal dat gegevens bevat” zoals bedoeld in artikel 1 onder a Wob. Sms- en WhatsApp-berichten lijken volgens de Afdeling bestuursrechtspraak in functie en gebruik op e-mailberichten, welke berichten volgens vaste jurisprudentie reeds onder het bereik van de Wob vallen. De informele en vluchtige aard van sms- en WhatsApp-berichten verandert dit niet, reeds omdat aan de aard van het gebruikte materiaal in de (hiervoor beschreven) parlementaire geschiedenis geen betekenis wordt toegekend voor het antwoord op de vraag of sprake is van een document als bedoeld in de Wob. In de vorige volzin is bewust – en dus anders dan in de hier gepubliceerde uitspraak – het woord ‘reeds’ gebruikt. E-mailberichten, documenten waarmee sms- en WhatsApp-berichten door de Afdeling bestuursrechtspraak worden vergeleken in dit verband, zijn in veel gevallen namelijk naar hun aard eveneens vluchtig en informeel, maar vallen toch onder de Wob (overigens al ruim voor 12 augustus 2012, zie ABRvS 20 december 2006, ECLI:NL:RVS:2006:AZ4788, r.o. 2.8).
4. Wanneer berusten sms- en WhatsApp-berichten aangaande een bestuurlijke aangelegenheid onder een bestuursorgaan? De toegepaste techniek werd door de Rechtbank Midden-Nederland voor de toepassing van de Wob niet doorslaggevend geacht. In mijn naschrift [red.: West] bij die uitspraak in dit blad heb ik die aanpak toegejuicht, omdat onderscheid in techniek in de huidige tijd niet houdbaar is, een tijd waarin documenten zowel in hard-copy, op een harde schijf, web-based alsook in de cloud kunnen worden opgeslagen. Het oordeel van de rechtbank over het vraagstuk ‘berusten onder’ sprong in het oog, voor zover daarbij een onderscheid werd gemaakt tussen sms- en WhatsApp-berichten op telefoons van ambtenaren met een abonnement op naam van (de organisatie van) het bestuursorgaan

enerzijds, en op privé-telefoons van ambtenaren anderzijds. Wat betreft de 'werktelefoons' dient het bestuursorgaan volgens de rechtbank een methode te vinden om berichten over een bestuurlijke aangelegenheid te kunnen achterhalen. Voor soortgelijke berichten op privételefoons zou dit uitgangspunt niet opgaan omdat deze berichten niet zouden berusten onder het bestuursorgaan. Ik aarzelde hierover in mijn naschrift, want ook dit onderscheid tussen werktelefoons en privételefoons bij de toepassing van de Wob lijkt in de huidige tijd niet goed vol te houden. Die aarzeling blijkt terecht. Doorslaggevend is volgens de Afdeling bestuursrechtspraak het antwoord op de vraag of het gaat om documenten van het bestuursorgaan (die dus berusten onder dat bestuursorgaan), en documenten bestemd voor het bestuursorgaan (die behoren te berusten onder het bestuursorgaan). In mijn eerdere naschrift heb ik dit geduid als de 'organisatorische relatie' die bestaat tussen een (tot het betrokken publiekrechtelijke rechtspersoon behorende) bestuursorgaan en de persoon die in die betrokken organisatie werkzaam is. Een en ander brengt met zich volgens de Afdeling bestuursrechtspraak dat onder 'berusten onder' als bedoeld in artikel 1 onder a jo. artikel 3 lid 1 van de Wob en anders dan de rechtbank voor ogen had, zowel sms- en WhatsApp-berichten vallen die staan op werktelefoons van bestuurders of ambtenaren met een abonnement op naam van het bestuursorgaan, als sms- en WhatsApp-berichten die staan op privételefoons. Omdat sms- en WhatsApp-berichten die bestemd zijn voor het bestuursorgaan maar op privételefoons staan bij het bestuursorgaan behoren te berusten, dient het betrokken bestuursorgaan al het redelijkerwijs mogelijke te doen om deze documenten alsnog te achterhalen. Tot deze inspanningsverplichting voortvloeiend uit artikel 4 van de Wob behoren inspanningen om binnen de eigen organisatie de verzochte documenten te achterhalen, dan wel door dit op andere wijze te doen bijvoorbeeld door navraag te doen bij de bestuurlijke aangelegenheid betrokken instanties die mogelijk (ook) over de verzochte informatie beschikken (vgl. ABRvS 26 augustus 2015, ECLI:NL:RVS:2015:2684, r.o. 4).

5. De Afdeling bestuursrechtspraak is zich ervan bewust dat het voor de uitvoeringspraktijk van bestuursorganen belastend kan en veelal zal zijn dat bij de beoordeling van Wob-verzoeken ook sms- en WhatsApp-berichten moeten worden betrokken en worden beoordeeld. Terecht maakt de belasting bij juiste toepassing van de Wob door het bestuursorgaan, bij rechtmatige verzoeken om informatie niet dat de Wob om die reden niet op deze documenten van toepassing is. Evenwel is de Afdeling bestuursrechtspraak minder goed te volgen daar waar lijkt te worden gesuggereerd dat de beoordeling van een Wob-verzoek waaronder sms- en WhatsApp-berichten vallen, niet het privéleven van de betrokken werknemer raakt. Hierbij moet wat ons betreft onderscheid worden gemaakt enerzijds tussen de wijze waarop informatie uiteindelijk openbaar wordt gemaakt, en anderzijds het (interne) proces dat tot die beslissing heeft geleid. Bij het uiteindelijke besluit over de verzochte openbaarmaking van sms- en/of WhatsApp-berichten zorgt de juiste toepassing van de weigeringsgronden uit de Wob (artikel 10 lid 1 onder d, en artikel 10 lid 2 onder e) er inderdaad voor dat de privacy van de betrokken ambtenaren kan worden beschermd. Een ander (juridisch, en onder omstandigheden wellicht onhoudbaar knel)punt ziet op het besluitvormingsproces dat daaraan voorafgaat. De Afdeling bestuursrechtspraak stelt dat de minister geen toegang heeft tot de privételefoon van de werknemer maar dat de werknemer de berichten die daarop staan, dient over te dragen aan de werkgever (r.o. 7.1). Het is de vraag op welke wijze de betrokken overheidsinstantie kan aantonen dat daadwerkelijk alle relevante berichten door de ambtenaar voor onderzoek zijn overgedragen. Daarnaast geldt dat de beoordeling of sms- en WhatsApp-berichten onder de reikwijdte van een Wob-verzoek vallen, in de regel niet wordt gemaakt door de betrokken bestuurders of ambtenaren. Om te kunnen vaststellen of (delen van) sms- en WhatsApp-berichten onder een tot een bestuurlijke aangelegenheid behoren én onder het Wob-verzoek vallen, zullen die sms- en WhatsApp-conversaties veelal integraal moeten worden gelezen en beoordeeld door anderen dan de ambtenaar in kwestie. Het onderzoeken van de berichten, los van het feit of deze afkomstig zijn van de privé- of zakelijke telefoon van de ambtenaar, kan derhalve privacy-rechtelijke gevolgen hebben. Delen van conversaties kunnen ook privacygevoelige informatie bevatten, zoals bijvoorbeeld het feit dat een ambtenaar een collega in het gesprek informeert dat hij ziek is, niet kan reageren op een bericht wegens een overlijden in de familiesfeer e.d. Uiteraard kan de ambtenaar die berichten van zijn privételefoon dient over te dragen worden verzocht om dergelijke berichten weg te 'lakken'. Ook hierbij kan echter discussie ontstaan over de authenticiteit en integriteit van de door de ambtenaar aangeleverde berichten.

6. Het raadplegen van sms- en WhatsApp-berichten levert een verwerking van persoonsgegevens in de zin van artikel 4 onder 2 van de Algemene Verordening Gegevensbescherming ('AVG') op, hetgeen de overheidsinstantie – net als bij bijvoorbeeld de controle van zakelijk internet en e-mailverkeer – dwingt om bepaalde basisbeginselen in acht te nemen. Zoals Molendijk betoogt (R. Molendijk, 'Recente jurisprudentie over de Wet openbaarheid van bestuur en de mogelijke gevolgen daarvan voor de dagelijkse Wob-praktijk', Gst. 2018/110, p. 568) is het een uitdaging om tot privacyverantwoorde werkwijze te komen. Zonder volledigheid te willen betrachten, stippen wij een aantal zaken aan. Zo zal het onderzoek zelf steeds de proportionaliteits- en subsidiariteitstoets moeten kunnen doorstaan: zo min mogelijk persoonsgegevens moeten op een zo min mogelijk privacyinbreukmakende manier worden verwerkt. Verder dient de toegang tot de sms- en WhatsApp-berichten beperkt te worden tot de personen die daadwerkelijk betrokken dienen te zijn bij de uitvoering van (de beoordeling van) het Wob-verzoek. Tevens dient de ambtenaar in kwestie te zijn geïnformeerd dat zijn sms- en WhatsApp-berichten mogelijk kunnen worden onderzocht in het kader van het voldoen aan Wob-verzoeken (zie onder meer artikel 12–14 AVG). Werkprotocollen kunnen hierbij behulpzaam zijn. Indien bij een overheidsinstantie een intern privacystatement aanwezig is, wordt aanbevolen deze informatie eveneens daarin op te nemen.

Ook in werkprotocollen kan het gebruik van privételefoons voor het ontvangen van werkgerelateerde berichten worden uitgesloten. Dit biedt echter geen garantie dat ambtenaren zich hieraan zullen houden, als gevolg waarvan alsnog voor Wob-verzoeken relevante informatie zich op privételefoons kan bevinden. Het is zeer de vraag of een overheidsinstantie zich kan verschuilen achter het bestaan van een dergelijk werkprotocol in relatie tot de Wob-verzoeker en de beoordeling van het Wob-verzoek. Het ligt voor de hand dat nog een additionele inspanning moet worden verricht zoals het vragen van een schriftelijke bevestiging van de betrokken ambtenaar dat hij geen werkgerelateerde berichten op zijn privételefoon heeft staan, of dat de betreffende berichten alsnog integraal beoordeeld moeten worden door het bestuursorgaan. De systematiek van en de rechtspraak over de Wob lijkt het laatste te verlangen, nu niet de ambtenaar maar het bestuursorgaan waarvoor de ambtenaar werkt het Wob-bevoegde orgaan is.

De hier gepubliceerde uitspraak maakt in ieder geval nieuwsgierig naar de praktische omgang met Wob-verzoeken waaronder sms- en WhatsApp-berichten vallen, mede vanuit privacyrechtelijk perspectief. Wij vermoeden dan ook dat dit niet onze laatste gezamenlijke annotatie zal zijn.

Dit is een uitgave van:

Rijksprogramma Duurzaam Digitale
Informatiehuishouding (RDDI)

Mei 2020



Ministerie van Volksgezondheid,
Welzijn en Sport

Bestuursraad Bedrijfsvoering
2 juli 2020

**Secretaris Generaal / plv.
Secretaris Generaal**
Dir Organisatie, Bedrijfsv en
Personeel
Afd. CIO kern en
informatiemanagement

Ontworpen door

5.1.2.e

5.1.2.e

T 070-340512e

5.1.2.e @minvws.nl

nota

(ter beslissing)

Datum

24 juni 2020

Paraaf directeur OBP

Paraaf pSG

1 Aanleiding voor deze nota

Voor het veiligstellen en archiveren van informatie is een beleidslijn nodig voor het chat/berichtenverkeer. Op korte termijn is deze van belang bij de archivering van de zogeheten Hotspot Covid-19. De beschreven beleidslijn is reeds in uitvoering. Vaststelling hiervan is nodig voor de formele vereisten bij deze dossiervorming.

2 Beslispunten, advies en mogelijk alternatief

De voorgelegde beleidslijn is reeds in werking. Vaststelling is noodzakelijk om de bewaring van deze berichten (in dossiers Covid-19) te formaliseren.

3 Samenvatting en conclusies

- Chatberichten vallen onder verplichtingen van Wob en Archiefwet;
- Met name van zogeheten sleutelfiguren en groeps-apps zijn deze berichten relevant ter bewaring;
- Stel chatberichten (en mogelijk andere vormen zoals sms) veilig en archiveer in overleg met het projectteam Covid-19;
- Met de ervaringen bij de vorming van het Hotspot-dossier Covid-19 zal deze beleidslijn worden aangevuld en opnieuw ter vaststelling worden aangeboden. Hierbij is de (technische) bewaring van sms en andere vormen nog te verbeteren.

4 Draagvlak politiek

Archivering en verantwoording van chatberichten is conform rijksbrede richtlijnen, zoals die van het Rijksprogramma Duurzaam Digitale Informatiehuishouding. De actieve bewaring van berichten van bewindslieden is reeds opgestart.

5 Draagvlak maatschappelijk en eenduidige communicatie

De vastgestelde beleidslijn is mede noodzakelijk voor de uitvoering van Wob-verzoeken i.h.k.v. Covid-19.

Binnen VWS-kerndepartement zal de beleidslijn worden gecommuniceerd. Hierbij wordt advies en ondersteuning aangeboden door het projectteam Hotspot Covid-19.

**Secretaris Generaal / plv.
Secretaris Generaal**
Dir Organisatie, Bedrijfsv en
Personeel
Afd. CIO kern en
informatiemanagement

6 Financiële en personele gevolgen

De structurele werklast van advisering en bewaring van berichtenverkeer wordt in kaart gebracht en geborgd door OBP. Omdat berichtenverkeer op persoonlijke smartphones staat is altijd betrokkenheid van individuele medewerkers nodig. We proberen dit met zoveel mogelijk ondersteuning te minimaliseren.

7 Juridische aspecten haalbaarheid

Voorgestelde lijn past binnen rijksbrede richtlijnen.

8 Afstemming (intern, interdepartementaal en met veldpartijen)

Voorstel is afgestemd met BPZ, WJZ en OBP. Medezeggenschap wordt geïnformeerd.

9 Gevolgen administratieve lasten

Naast enige druk op reguliere archiverings-taken geen bijzonderheden.

10 Toezeggingen

N.v.t.

11 Fraudetoets

n.v.t.

5.1.2.e

5.1.2.e

Ministerie van Volksgezondheid,
Welzijn en Sport

Secretaris Generaal / plv.
Secretaris Generaal
Afdeling Bedrijfsvoering
Kennisplein

Datum
24 juni 2020

*Correspondentie uitsluitend
richten aan het retouradres
met vermelding van de datum
en het kenmerk van deze
brief.*

Veiligstelling Covid-19 chatberichten

Dit memo beschrijft hoe wordt omgegaan met de mobiele chatberichten gedurende de Covid-19 crisis. Dit beleid is van toepassing vanaf de start van de COVID-19 crisis (December 2019) tot en met het einde van de crisis (of tenminste tot het einde van 2020). Na afloop zal geëvalueerd worden of dit beleid staand beleid kan worden of dat er aanpassing nodig is.

Achtergrond

Verantwoord gebruik van berichtenapps is cruciaal met het oog op de rechtelijke uitspraak van de Raad van State, die benadrukt dat mobiele chatberichten onder het Wob-regime (en dat van de Archiefwet) vallen en veiliggesteld dienen te worden. In deze uitspraak wordt benadrukt dat het hierbij kan gaan om WhatsApp chatberichten, maar ook om sms-berichten of andersoortige chatapps. Ook de Covid-19 crisis vereist een goede vastlegging van chatberichten om het overheidshandelen te kunnen verantwoorden en te reconstrueren.

Vanuit Rijksbrede richtlijnen, o.a. RDDI, wordt geadviseerd om:

- A. WhatsApp, sms-berichten of andersoortige chatapps zo min mogelijk te gebruiken
- B. Alleen bestuurlijke besluitvorming (en de totstandkoming hiervan) te archiveren.
- C. Medewerkers zelf hun berichten te laten archiveren

Ministeries kunnen hierin een eigen risicoafweging maken. Door de projectgroep Hotspot COVID-19 is de volgende risicoafweging gemaakt:

1. Er wordt binnen VWS heel veel geappt met interne en externe medewerkers, relaties etc. rondom Covid-19. Dit ontraden is in de crisis beperkend voor de slagkracht van VWS.
2. Heel veel berichtenverkeer dat het project tot nu toe gezien heeft werpt licht op het handelen van VWS, ook als er niet altijd bestuurlijke besluitvorming heeft plaatsgevonden. Dit niet veilig stellen leidt ertoe dat VWS geen inzicht heeft in veel processtappen en zich niet kan verantwoorden over het gevoerde beleid.
3. Medewerkers hebben vaak geen tijd of ruimte om zelf te archiveren, door hen hierin te ondersteunen kunnen zij zich focussen op hun kerntaken en wordt er meer en beter gearchiveerd.

Beleid: veilig stellen berichten informatieknooppunten Covid-19

Ter verantwoording en reconstructie worden chatberichten van sleutelfiguren, c.q. informatieknooppunten, Covid-19 veiliggesteld (geëxporteerd en gearchiveerd). In een informatieknooppunt komen informatiestromen samen en /of is er sprake van informatie die belangrijk is voor evaluatie en verantwoording rondom Covid-19.

De volgende informatieknooppunten worden veilig gesteld:

1. Appgroepen m.b.t. (onderdelen van) de Covid-19 crisis met VWS medewerkers

2. Appgroepen m.b.t. (onderdelen van) de Covid-19 crisis waarin ook externen zitten (zoals de Appathon-appgroep)
3. Leden van de Bestuursraad en bewindspersonen (voor zover niet appgroep gerelateerd berichtenverkeer)
4. Andere VWS-kern medewerkers die na onderzoek een belangrijk informatieknooppunt blijken te zijn voor Covid-19.

**Secretaris Generaal / plv.
Secretaris Generaal**
Afdeling Bedrijfsvoering
Kennisplein

Hoe?

1. Medewerkers laten berichten in hun telefoon staan.
2. Vanuit het project wordt contact opgenomen met de betreffende medewerker en/of diens ondersteuning. De medewerker stelt een 1^e keer op afspraak de telefoon ter beschikking aan de ondersteuner vanuit het project om op locatie de telefoon uit te lezen. Deze berichten worden na schoning gearchiveerd door het projectteam hotspot Covid-19
3. Na de 1^e uitlezing wordt bij beheerders van appgroepen de projecttelefoon van het project Hotspot toegevoegd aan de berichtenapp. Zo kan vervolgens wekelijks op afstand door de ondersteuner de appgroep gearchiveerd worden.
4. Tijdens de Bestuursraad op vrijdagochtend worden de telefoons van de leden van de Bestuursraad uitgelezen. Deze uitlezing wordt periodiek herhaald. Deze berichten worden na schoning gearchiveerd door het projectteam hotspot Covid-19.
5. Telefoons van de bewindspersonen worden door periodiek door BPZ uitgelezen. Deze berichten worden na schoning gearchiveerd door het projectteam hotspot Covid-19.
6. Bij het uitlezen van de telefoons wordt een exportbestand gemaakt. Dit bestand wordt na export door het projectteam geschoond en ter accordering gedeeld met de betrokken medewerker. Het geschoonde bestand wordt gearchiveerd, het originele bestand wordt vernietigd.
7. Schoning vindt plaats met in acht nemen van de AVG en privacy van betrokken medewerkers:
 - a. Overduidelijke privé berichten worden verwijderd uit het export bestand
 - b. Bijzondere persoonsgegevens (medisch, strafrecht) worden verwijderd uit het export bestand
 - c. Berichten die niet gaan over Covid-19 worden verwijderd uit het export bestand.

Bijlage 1 do's en dont's berichtenverkeer voor Medewerkers

**Secretaris Generaal / plv.
Secretaris Generaal**
Afdeling Bedrijfsvoering
Kennisplein

1. Werk met appgroepen en duidelijke beheerders
2. Meld appgroepen in het kader van Covid-19 aan bij
5.1.2.e @minvws.nl voor archivering
3. Laat besluiten en toezeggingen per app ook bevestigen per e-mail en doe dit zelf ook
4. App zo min mogelijk 1 op 1 i.v.m. onderlinge vervangbaarheid
5. Gebruik geen Signal (kunnen we nu niet archiveren)

Bijlage 2 toelichting Schoning

Na veiligstelling kunnen de chatberichten bewerkt worden door de DIV-ondersteuner. Enkel berichten met persoonsgegevens die niet vallen onder de uitzonderingen van de AVG worden verwijderd. Dat betreft bijzondere persoonsgegevens (medische) en strafgegevens. Naar onze inschatting zal dit niet of bijna nooit voorkomen. Overduidelijke privé berichten gericht aan familie, vrienden etc. worden ook verwijderd voor archivering. Dit is toegestaan met het oog op Wob-verzoeken, maar ook met het oog op een parlementaire enquête. Overige chatberichten worden bewaard.

Wanneer de ondersteuner berichten niet kan interpreteren, wordt de eigenaar van de berichten gevraagd om enige toelichting.

Ministerie van Volksgezondheid,
Welzijn en Sport

agenda

Betreft Bestuursraad Bedrijfsvoering
 Vergaderdatum en -tijd 2 juli 2020 09:30-11:00
 Vergaderplaats WebEx
 Aanwezig pSG, pDGV, pDGCZ, pDGLZ, dbvRIVM, dFEZ,
 dOBP, dWJZ, pdBPZ, dDICIO, dbvIGJ, lrvbZiNL,
 adviseur BPZ
 Afwezig -

**Secretaris Generaal / plv.
Secretaris Generaal**
 Directie Bestuurlijke en
 Politieke Zaken
 Bureau Bestuurlijke-politieke
 advisering

Bezoekadres:
 Parnassusplein 5
 2511 VX Den Haag
 T 070 340 79 11
 F 070 340 78 34

www.rijksoverheid.nl

Inlichtingen bij
5.1.2.e
 (Senior) Adviseur

T 0621101925
5.1.2.e @minvws.nl

Datum
 25 juni 2020

Bijlage(n)
 Ja

Aantal pagina's
 1

*Correspondentie uitsluitend
 richten aan het retouradres
 met vermelding van de datum
 en het kenmerk van deze
 brief.*

- 1. Opening en mededelingen**
 - 1.1 buiten reikwijdte 09.30-09.35
- 2. Ter besluitvorming**
 - 2.1 Beleidslijn veiligstellen en archiveren chat- en berichtenverkeer COVID-19 09.35-09.45
5.1.2.e (OBP)
 - 2.2 buiten reikwijdte 09.45-09.55
- 3. Ter bespreking**
 - 3.1 buiten reikwijdte 09.55-10:05
 - 3.2 buiten reikwijdte 10:05-10:25
 - 3.3 buiten reikwijdte 10:25-10:45
- 4. Actualiteiten** 10:45-11:00
- 5. Hamerstukken/stukken ter kennisname**
 - 5.1 buiten reikwijdte

Van: [REDACTED]@minvws.nl
Aan: Groep VWS medewerkers kern
Onderwerp: 5.1.2e
Datum: vrijdag 17 juli 2020 17:37:54

Beste collega's,

buiten reikwijdte

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Aanleveren stukken voor bewindspersonen tijdens het reces

buiten reikwijdte

[REDACTED]

Covid-19 programmadirectie

buiten reikwijdte

[REDACTED]

buiten reikwijdte

[REDACTED]

Vakantie in het buitenland

buiten reikwijdte

[REDACTED]

buiten reikwijdte

[redacted]

Workshops volgen tijdens de zomer
buiten reikwijdte

[redacted]

Archiveren van informatie over corona

De zomer is vaak het uitgelezen moment om je archief op orde te brengen, omdat het dan wat rustiger is. Om ons nu en in de toekomst te kunnen verantwoorden over het handelen tijdens de coronacrisis, is het belangrijk dat alle relevante informatie over corona/Covid-19 wordt veiliggesteld en gearchiveerd. Dit geldt voor documenten, e-mails, chatberichten van WhatsApp of iMessage, berichten op social media, enzovoort. Het uitgangspunt is: gooi niets weg! Om je te helpen, vind je op Rijksportaal een [pagina met veelgestelde vragen](#). Wil je meer informatie over het veilig stellen en archiveren van informatie? Lees dan ook het bericht op [VWSnet](#) of neem contact op met CoronaArchivering@minvws.nl.

Nieuwe poll 'vakantiebestemming' en vakantiefotowedstrijd
buiten reikwijdte

[redacted]

buiten reikwijdte

[redacted]

[redacted]

Met vriendelijke groet,

5.1.2e

[redacted]

Ministerie van Volksgezondheid,
Welzijn en Sport

Aan de leden van de Bestuursraad

Deadline: 16 april
2021

pSG
pSG
Nafase COVID-19

Ontworpen door
5.1.2e

nota

(ter beslissing)

Paraaf pSG

Datum
8 april 2021

Kenmerk
2342898-1006392

Zaaknummer
1006392

1 Aanleiding voor deze nota

De COVID-19 crisis leidt tot een ongekennde en alsmaar groeiende hoeveelheid aan relevante documenten, e-mails en chatberichten. Het huidige informatiebeheer van VWS belemmert een efficiënte verwerking van COVID-informatie in het kader van de hotspot-archivering, de verantwoording richting parlement en de Onderzoeksraad voor Veiligheid (OVV), het afhandelen van Wob-verzoeken en het maken van reconstructies.

2 Beslispunten, advies en mogelijk alternatief

Gaat de Bestuursraad akkoord met:

- De voorgestelde wijze van ontsluiten en doorzoeken van e-mails en documenten in het kader van verantwoording?
- Het geautomatiseerd uitlezen en selecteren van chatberichten?

3 Samenvatting en conclusies

Voorstel 1 betreft de geautomatiseerde werkwijze van ontsluiten en doorzoeken van e-mails en documenten, zoals overeengekomen voor Wob-verzoeken, welke ook voor de overige verantwoordingsverzoeken zal worden gehanteerd. Dit betreft MT-leden van de betrokken directies en de ambtelijke leiding. Daar waar e-mailboxen van zogenaamde 'sleutelfunctionarissen'¹ (dus niet zijnde MT-leden van de directies en de ambtelijke leiding) in beeld komen zal om toestemming gevraagd worden om deze geautomatiseerd te doorzoeken.

¹ Een sleutelfunctionaris is een functionaris die door het vervullen van een specifieke taak of rol - of door de combinatie van beide - van bijzonder belang is binnen de aanpak van de COVID-19 crisis.

Ten opzichte van de huidige situatie betekent dit dat de programmadirectie Nafase COVID-19:

- o De e-mailboxen van MT-leden van de betrokken directies en de ambtelijke leiding automatisch zal ontsluiten en doorzoeken ter beantwoording van de verantwoordingsverzoeken conform de procedure zoals overeengekomen voor de Wob;
- o Het initiatief zal nemen voor specifieke afstemming met de ambtelijk adviseurs e.a. voor het automatisch ontsluiten van de e-mailboxen van de politieke leiding. Voor de politieke leiding is geen sprake van "automatisch ontsluiten in een centrale omgeving";
- o Sleutelfunctionarissen de keuze geeft zelf e-mails te verplaatsen naar de dienstpostbus van de eigen directie, zodat deze e-mails doorzoekbaar zijn óf dat de programmadirectie de e-mailboxen van sleutelfunctionarissen, na hun goedkeuring, automatisch zal doorzoeken ten behoeve van de beantwoording van de verantwoordingsverzoeken;
- o De in het kader van verantwoording gebruikte stukken zal opslaan op een door de directie OBP aan te wijzen document management systeem en deze stukken vanuit hier zal aanbieden aan het Nationaal Archief;
- o Regie neemt in het proces zodat dit transparant, efficiënt en privacy-vriendelijk is en voldoet aan de gestelde vereisten.

pSG
pSG
Nafase COVID-19

Kenmerk
2342898-1006392

Voorstel 2 betreft de wijze van het uitlezen en selecteren van chatberichten. De voorgestelde werkwijze bestaat uit het (indien de betrokkene daarvoor toestemming geeft) verder automatiseren van het uitlezen van chatberichten uit telefoons en het automatisch selecteren van relevante chatberichten, conform de procedure zoals deze wordt gehanteerd bij de Wob.

Ten opzichte van de huidige situatie betekent dit dat de programmadirectie Nafase COVID-19:

- o De betrokkene vier opties voorlegt:
 1. De betrokken persoon levert zelf de voor de verantwoording aangaande COVID-19 crisis noodzakelijke berichten aan;
 2. De betrokken persoon laat dit doen door zijn/haar secretariaat of door zijn/haar persoonlijke beleidsmedewerker;
 3. De betrokken persoon geeft toestemming aan de programmadirectie Nafase COVID-19 om de relevante berichten in het kader van COVID-19 geautomatiseerd uit te nemen en te selecteren op relevantie;
 4. De persoon kan weigeren. Duidelijk wordt gemaakt aan de medewerker dat weigeren geen arbeidsrechtelijke consequenties heeft.
- o Regie neemt in het proces zodat dit transparant, efficiënt en privacy-vriendelijk is en voldoet aan de gestelde vereisten.

De betrokken personen zullen worden geïnformeerd over de nieuwe werkwijze en een werkinstructie wordt gemaakt voor degene die zelf de relevante berichten wil (laten) selecteren.

Wanneer de Bestuursraad akkoord gaat met de voorgestelde werkwijzen (voorstel 1 en 2) zorgt dit voor een efficiëntere manier van werken en een eenduidige en transparante afhandeling van verantwoordingsverzoeken, terwijl de privacy van de betrokken personen gerespecteerd wordt door het aanbieden van bovenstaande keuzemogelijkheden en het eventueel geven van toestemming door de persoon. Het naleven van de geldende privacyregels is van belang voor het draagvlak in de

organisatie voor de voorgestelde werkwijze. Vanwege de grote werkvoorraad aan reeds uitgelezen chatberichten is de programmadirectie Nafase COVID-19, na akkoord van de pSG op 12 maart 2021, alvast gestart met het automatisch selecteren van relevante chatberichten.

pSG
pSG
Nafase COVID-19

Gezien de behoefte aan bredere informatieverstrekking naar aanleiding van de POK werkt de directie OBP – in samenwerking met andere departementen – aan een generieke beleidslijn omtrent het veiligstellen en archiveren van berichtenverkeer. Vooruitlopend hierop kan het zinvol zijn om in het kader van de door de programmadirectie Nafase COVID-19 bewaarde berichten blijvend veilig te stellen ten behoeve van nog volgende verantwoordingsdossiers. De directie OBP zal op korte termijn aan betrokkenen toestemming vragen om bewaard berichtenverkeer duurzaam op te slaan. Een uitgewerkt voorstel hiertoe wordt uiterlijk in mei aan de BRBV voorgelegd.

Kenmerk
2342898-1006392

Zowel in de huidige werkwijze als voorgestelde werkwijzen wordt gebruik gemaakt van analysesoftware (ZyLAB) in de publieke cloud (uiteraard met veiligheidswaarborgen). De directie OBP werkt aan het onderbrengen van deze software bij SSC-ICT ("on premise"), maar hier zullen nog enkele maanden overheen gaan. In de tussentijd wordt een preselectie van de informatie door middel van Zoek&Vind gemaakt, vóórdat de informatie door ZyLAB gaat (en dus in de cloud terecht komt). Zo wordt in de regel uitgesloten dat vertrouwelijke informatie (Dep V en/of Stg gerubriceerd) onderdeel wordt van het dossier. Deze informatie zou niet in e-mailboxen of chatberichten mogen voorkomen, maar de praktijk wijst uit dat hier incidenteel toch sprake van is. In die incidentele situatie geldt de volgende procedure:

- De programmadirectie NC19 meldt dit als incident bij de BVA;
- De BVA onderzoekt de incidentmelding (en belanghebbenden dienen door VWS geïnformeerd te worden);
- De programmadirectie NC19 zal betreffende stukken uit de dataset verwijderen.

Tot slot is in deze nota ter informatie aan de Bestuursraad de werkwijze opgenomen die de programmadirectie Nafase COVID-19 hanteert ten aanzien van de consortia naast het Landelijk Consortium Hulpmiddelen (LCH). De programmadirectie Nafase COVID-19 zal ten aanzien van de overige consortia de zogenaamde 'LCH-lijn' inzake het veiligstellen van informatie continueren.

4 Draagvlak politiek

Met de in deze nota voorgestelde inhoudelijke keuzes voor het ontsluiten en doorzoekbaar maken van bronnen als WhatsApp en mailverkeer gaat VWS mee in de lijn van de kabinetsreactie op de POK, waarin is toegezegd dat er meer openheid en transparantie in de informatievoorziening naar de Kamer zal komen. Ervaringen en inzichten die in het programma Nafase COVID-19 worden opgedaan, worden meegenomen in de aanpak die de directie OBP ontwikkelt om te komen tot een duurzaam informatiebeheer, dit eveneens als uitvloeisel van de toezeggingen van het kabinet.

5 Draagvlak maatschappelijk en eenduidige communicatie

Idem "Draagvlak politiek".

6 Financiële en personele gevolgen

De directie OBP neemt de kosten die het geautomatiseerd uitlezen en selecteren van chatberichten met zich mee brengt voor haar rekening.

pSG
pSG
Nafase COVID-19

7 Juridische aspecten haalbaarheid

Kenmerk
2342898-1006392

In de zomer van 2020 heeft de BRBV besloten om mobiele telefoons uit te lezen van VWS-ambtenaren van het kerndepartement, die betrokken zijn bij de bestrijding van de COVID-19 crisis. Daarbij is onvoldoende aandacht besteed aan privacyaspecten. Dat is in de context van toen zeer verklaarbaar ("het is crisis; we moeten snel handelen"). Op dit moment is er wél tijd en ruimte om die afweging zorgvuldig maken.

Het volgende is van belang. Het is werkgevers niet toegestaan om inbreuk te maken op de privacy van werknemers, tenzij er sprake is van een wettelijke grondslag, een legitiem doel en een geschikt middel om het doel te bereiken. Daarnaast moet de inbreuk proportioneel zijn en voldoen aan het subsidiariteitsvereiste.

Er bestaat geen wettelijke grondslag in de zin van de AVG voor uitlezen van mobiele werktelefoons. De grond 'toestemming' is niet van toepassing omdat er sprake is van een machtsrelatie tussen werkgever en werknemer. Voor deze gegevensverwerking is een *Data Protection Impact Assessment* (DPIA)² vereist waarin de grondslagen, de afwegingen, de proportionaliteit, de overwogen alternatieven en de risico's voor de organisatie duidelijk in beeld komen. Deze DPIA is in ontwikkeling. De directies OBP, WJZ en Nafase COVID-19 werken hier constructief samen. Naar verwachting is de DPIA eind april gereed. De bestuursraad zal op de hoogte worden gesteld van de uitkomst van de DPIA. Mocht de DPIA leiden tot aanpassing van de voorgestelde werkwijze dan zal dit uiteraard aan de Bestuursraad worden voorgelegd.

Andere wetgeving, met name de Wob en Archiefwet verplicht VWS om gereede inspanningen te verrichten om de informatie uit berichtenverkeer veilig te stellen voor verantwoording, beantwoording van Wob-verzoeken en archivering in het algemeen belang.

Om privacyrisico's te mitigeren, is bij voorstel 2 opgenomen dat een VWS-ambtenaar mag weigeren om chatberichten veilig te stellen en dat dit geen arbeidsrechtelijke consequenties heeft. Daarnaast is bij voorstel 2 opgenomen dat het uitgelezen chatverkeer met instemming van de betrokkene wordt bewaard, op basis van besluitvorming van de BRBV. Een uitgewerkt voorstel hiertoe wordt door de directie OBP uiterlijk in mei aan de BRBV voorgelegd.

8 Afstemming (intern, interdepartementaal en met veldpartijen)

BPZ, WJZ en OBP zijn nauw betrokken geweest bij de totstandkoming van deze nota en de nota is besproken met de Functionaris Gegevensbescherming. Zij kunnen zich vinden in de lijn zoals deze is neergelegd voor wat betreft het proces en de beschrijving daarvan.

² Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

WJZ wijst separaat op het volgende: het heeft de voorkeur met de daadwerkelijke uitvoering van de hierboven voorgestelde werkwijze te beginnen na afronding van de DPIA; dat laat onverlet dat er voorbereidingen voor de uitvoering getroffen kunnen worden.

pSG
pSG
Nafase COVID-19

De nota wordt op 15 april besproken door de OR.

Kenmerk
2342898-1006392

Daarnaast zijn de voorstellen uit deze nota mondeling besproken met de directeuren (en/of MT-leden) van de volgende directies: CZ, DICIO, DMO, GMT, Jeugd, LZ, MEVA, PDC19, PG, Sport en Vaccinatie. Deze directies kunnen zich allemaal goed vinden in de voorstellen 1 en 2.

9 Gevolgen administratieve lasten

N.v.t.

10 Toezeggingen

N.v.t.

11 Fraudetoets

N.v.t.

5.1.2.e

Beleidsadviseur Nafase COVID-19

Toelichting

1. Aanleiding

De COVID-19 crisis leidt tot een ongekeerde en alsmaar groeiende hoeveelheid aan relevante documenten, e-mails en chatberichten. Het adequaat veiligstellen, onderzoekbaar maken en ter beschikking kunnen stellen van deze informatie is essentieel vanuit de verplichtingen uit de Wet openbaarheid van bestuur (Wob), Archiefwet, Wet op de parlementaire enquête en artikel 68 Grondwet (inlichtingenplicht ministers en staatssecretarissen). Het huidige informatiebeheer van VWS belemmert een efficiënte verwerking van COVID-informatie in het kader van de hotspot-archivering, de verantwoording richting parlement en OVV, het afhandelen van Wob-verzoeken en het maken van reconstructies. In het voorjaar van 2020 is, op verzoek van de SG, daarom reeds bewust gekozen voor een aparte werkwijze ten aanzien van het doorzoeken van e-mails en documenten voor de afhandeling van Wob-verzoeken (zie nota in de bijlage), om de beleidsdirecties te ontlasten.

Met de in deze nota voorgestelde inhoudelijke keuzes voor het ontsluiten en onderzoekbaar maken van chatberichten en mailverkeer gaat VWS mee in de lijn van de kabinetsreactie op de POK, waarin is toegezegd dat er meer openheid en transparantie in de informatievoorziening naar de Kamer zal komen. Ervaringen en inzichten die in het programma Nafase COVID-19 worden opgedaan, worden meegenomen in de aanpak die de directie OBP ontwikkelt om te komen tot een duurzaam informatiebeheer, dit eveneens als uitvloeisel van de toezeggingen van het kabinet. De nog te ontwikkelen aanpak voor een duurzaam informatiebeheer komt echter te laat voor een voorspoedige verwerking van alle relevante COVID-informatie. Deze notitie bevat een tweetal voorstellen om de gekozen werkwijze bij de afhandeling van de Wob-verzoeken te verbreden, waardoor we ook de hotspot-archivering, de verantwoording richting parlement en OVV, en het maken van reconstructies op een efficiënte wijze kunnen oppakken.

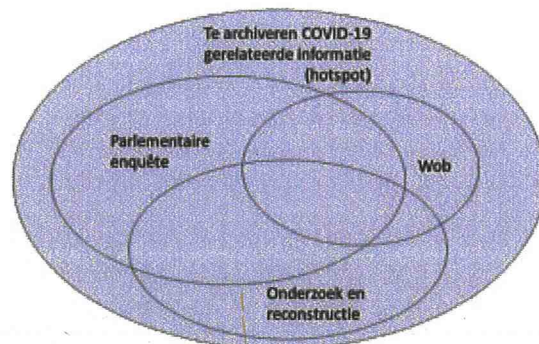
2. Stand van zaken

Veiligstellen

De huidige lijn wat betreft het veiligstellen van relevante COVID-informatie is dat VWS-medewerkers is verzocht niets te vernietigen. Daarnaast stelt SCC-ICT de e-mailboxen van medewerkers van VWS standaard veilig, om 10 jaar te bewaren. De programmadirectie stelt ook actief informatie veilig. Enerzijds bij het vertrekken van een werknemer of in geval van een volle e-mailbox (zodat voorkomen wordt dat relevante informatie verloren gaat); hier gaat het om informatie die al in een VWS omgeving staat. Anderzijds wordt COVID-informatie die niet binnen de VWS-omgeving staat hier naartoe gebracht, zoals chatberichten die aanwezig zijn op de werktelefoons van medewerkers, maar ook documenten uit omgevingen als samenwerkruimtes.

Soort en omvang informatie

Welke informatie relevant is vanuit de verschillende taakvelden van de programmadirectie bezien, valt uiteen in subsets welke elkaar deels overlappen (hiernaast visueel weergegeven). Op 1 januari 2021 was sprake van ruim 2,6 miljoen relevante documenten, mails en chatberichten. Ontdubbeld komt dit neer op ongeveer 500.000 documenten, mails en chatberichten. Ter vergelijking: het ministerie van Financiën beschikte in het kader van de kinderopvangtoeslag over 50.000 documenten. Na ontdubbeling resulteerde dit in 5.000 documenten. Uiteindelijk



pSG
pSG
Nafase COVID-19

Kenmerk
2342898-1006392

heeft het ministerie van Financiën circa 2.500 documenten aan de onderzoekscommissie overgedragen.

pSG
pSG
Nafase COVID-19

3. Voorstellen

Kenmerk
2342898-1006392

Voorstel 1: Wijze van ontsluiten en doorzoeken e-mails en documenten

Van uitvraag naar "sleepnet"

In het voorjaar van 2020 is, op verzoek van de SG, gekozen voor een nieuwe werkwijze ten aanzien van het doorzoeken van e-mails en documenten voor de afhandeling van Wob-verzoeken. Voorheen verzocht de Wob-coördinator de betrokken beleidsambtenaar relevante e-mails en documenten te verzamelen. In de nieuwe werkwijze voor de afhandeling van Wob-verzoeken worden de relevante e-mails en documenten gezocht door middel van een 'geautomatiseerd sleepnet' dat netwerkschijven en e-mailboxen (van MT-leden en de ambtelijke leiding) doorzoekt. De documenten en relevante e-mails worden tevens automatisch gelakt op basis van de met de Wob-juristen overeengekomen regels aangaande privacy, schuttingtaal en Wob-relevante criteria. Deze werkwijze minimaliseert de belasting voor de ambtelijke organisatie.

Wat betreft de politieke leiding neemt de programmadirectie Nafase COVID-19 het initiatief voor specifieke afstemming met de ambtelijk adviseurs e.a. voor het automatisch ontsluiten van de e-mailboxen. Voor de politieke leiding is geen sprake van "automatisch ontsluiten in een centrale omgeving".

Keuzemogelijkheid

De werkwijze zoals deze bij Wob-verzoeken wordt gehanteerd is getoetst en goedgekeurd door de privacy officer en CISO door middel van een DPIA. Deze werkwijze dient als basis voor alle komende verantwoordingsverzoeken aan VWS die dezelfde reikwijdte en diepgang hebben (dat wil zeggen, dezelfde directies, betrokken MT-leden en ambtelijke leiding). Voor toekomstige verantwoordingsverzoeken die *buiten* deze reikwijdte en diepte vallen, komen zogenaamde 'sleutelfunctionarissen'³ in beeld (denk bijvoorbeeld aan een senior/coördinerend beleidsmedewerker), onder andere in het kader van parlementaire verantwoording of overdracht aan het Nationaal Archief. Aan hen zal de keuze worden voorgelegd om:

1. Zelf e-mails te verplaatsen naar de dienstpostbus van de eigen directie, zodat deze e-mails in het sleepnet vallen;
2. De programmadirectie Nafase COVID-19 toestemming te verlenen de e-mailbox te mogen doorzoeken.

De tweede optie heeft de voorkeur omdat dit zorgt voor een zo volledig mogelijke verzameling aan e-mails, daar de subjectieve beoordeling van de sleutelfunctionaris van wat relevante e-mails zijn, wegvalt. Deze maatregelen zijn genomen in overleg met de privacy officer, omdat de verwachting is dat de privacy impact door sleutelfunctionarissen als groot kan worden ervaren.

Archivering

De in het kader van verantwoording gebruikte stukken worden opgeslagen op een door de directie OBP aan te wijzen document management systeem (vooralsnog Marjolein). De uiteindelijk te archiveren stukken bestaan uit de totaalsom van de

³ Een sleutelfunctionaris is een functionaris die door het vervullen van een specifieke taak of rol - of door de combinatie van beide - van bijzonder belang is binnen de aanpak van de COVID-19 crisis.

stukken gebruikt ter verantwoording aangaande Wob-verzoeken (verantwoording naar burgers en media), de voorbereiding voor een parlementair verantwoordingstraject (een onderzoek of een enquête) en het kunnen reconstrueren van de COVID-19 crisis (verantwoording naar OVV en de NSOB-tijdlijnen), aangevuld met de hotspotlijst zoals overeengekomen met het Nationaal Archief.

pSG
pSG
Nafase COVID-19

Kenmerk
2342898-1006392

Beschouwing

Aan de hand van een viertal belangrijke aspecten wordt de voorgestelde werkwijze hieronder nog kort beschouwd:

Verantwoording: Door het centraal ontsluiten (door middel van ZyLAB en Marjolein) en doorzoekbaar maken (door middel van Zoek&Vind) van data ontstaat een *eenduidige werkwijze* van veiligstellen en afdoen van verantwoordingsverzoeken.

Volledigheid: Alle relevante stukken worden voor de verschillende trajecten (Wob, parlementaire enquête, hotspot, etc.) geautomatiseerd ontsloten en doorzocht in *één centrale omgeving*. Hiermee ontstaat een effectievere en efficiëntere wijze van veiligstellen en afdoen van verantwoordingsverzoeken.

Beveiliging: Afhankelijk van de gevraagde verantwoording zal informatie behandeld worden conform de geldende wet- en regelgeving, waarbij een *zorgvuldige, integrale belangenafweging* zal plaatsvinden tussen vertrouwelijkheid, privacy en andere belangen.⁴ Beveiligingsincidenten worden eenduidig afgehandeld en gerapporteerd. Onderliggende stukken worden in een kluis geplaatst.

Inzet individu/directie: De sleutelfunctionaris bepaalt zelf in welke mate hij of zij ontzorgd wil worden, rekening houdend met de door hem of haar gewenste privacy. Beleidsdirecties worden *op maat bediend, ontzien* en alleen bij incidentele gevallen geconsulteerd.

Advies: het instemmen met de voorgestelde werkwijze.

Beslispunt: gaat de Bestuursraad akkoord met de voorgestelde werkwijze?

⁴ Meer concreet betekent dit dat staatsgeheime confidentiële informatie in de dataset na ontdekking zo snel mogelijk naar een andere locatie/beheeromgeving verplaatst zal worden, nadat gekeken is of deze informatie relevant is/kan zijn voor de doeleinden van het programma. Daarnaast:

1. Staatsgeheime confidentiële informatie zal nooit verstrekt worden in Wob-verzoeken;
2. Wanneer staatsgeheime confidentiële informatie wordt opgevraagd in een parlementaire enquête of enig ander onderzoek zal een belangenafweging gemaakt worden of en zo ja onder welke voorwaarden deze informatie verstrekt kan worden (rekening houdend met onder meer de Wet op de parlementaire enquête);
3. Staatsgeheime confidentiële informatie zal pas na de-rubricering gearchiveerd worden en (na verloop van 20 jaar) worden overgedragen aan het Nationaal Archief indien dit onder de hotspot valt.

Voorstel 2: Wijze van uitlezen en selecteren van chatberichten

pSG
pSG
Nafase COVID-19

Kenmerk
2342898-1006392

Het tweede voorstel betreft de werkwijze omtrent het uitlezen en selecteren van chatberichten. Vaststaat dat een aantal berichten nu aanwezig op de telefoons van de politieke leiding, ambtelijke leiding, MT-leden van betrokken directies en een selectie sleutelfunctionarissen van belang is voor de noodzakelijke verantwoording (zoals hierboven benoemd). Waar het gaat om een sleutelfunctionaris moet sprake zijn van een dringende reden om zijn of haar chatberichten uit te lezen en te selecteren op relevantie, dit wordt indien van toepassing gemotiveerd omschreven. Chatberichten die bij het uitvoeren van overheidstaken zijn gebruikt vallen, op grond van de uitspraak van de Raad van State van 20 maart 2019⁵, onder het bereik van de Wob en de Archiefwet. Het bestuursorgaan moet er dan ook zorg voor dragen dat deze niet verloren gaan.

Het *uitlezen* van telefoons gebeurt op dit moment voor 1/3^e deel automatisch en 2/3^e deel handmatig, dit is een arbeidsintensief traject. Het *selecteren* van relevante chatberichten gebeurde tot 12 maart 2021 volledig handmatig.

Geautomatiseerd uitlezen en selecteren

Op basis van een proeftuin blijkt dat het geautomatiseerd uitlezen en vervolgens selecteren van relevante chatberichten uit telefoons, conform de procedure zoals deze wordt gehanteerd bij de Wob mogelijk is, waardoor het handmatig selecteren van relevante chatberichten niet langer noodzakelijk is. Vanwege de grote werkvoorraad aan uitgelezen chatberichten is de programmadirectie Nafase COVID-19, na akkoord van de pSG op 12 maart 2021, alvast gestart met het automatisch selecteren van relevante chatberichten. Het automatisch selecteren houdt in dat met behulp van (COVID-gerelateerde) trefwoorden wordt gezocht naar relevante chatberichten. Op basis van de met de Wob-juristen overeengekomen regels aangaande privacy, schuttingtaal en Wob-relevante criteria zullen delen van de chats automatisch worden gelakt. De geselecteerde chats zullen onderdeel uitmaken van het verantwoordingsproces. Uit het oogpunt van doelbinding zullen niet-relevante chats worden verwijderd.⁶

Privacy

Het automatisch selecteren van relevante chatberichten is niet alleen efficiënter, ook het privacy-aspect is hiermee beter gewaarborgd: de automatisch geselecteerde chatberichten zullen worden gevalideerd door de gegevenseigenaar en getoetst door een jurist aan de hand van de van toepassing zijnde wettelijke bepalingen, in plaats van het onder ogen krijgen van alle uitgelezen chatberichten door een collega, om de relevante chats te kunnen selecteren. Opmerking verdient hier wel dat de uitgelezen chatberichten door een collega handmatig moeten worden omgezet van Zip-bestand naar Word-bestand, om vervolgens automatisch de relevante chats te laten selecteren. In dit proces zal niet inhoudelijk naar de chatberichten worden gekeken, al blijft dit theoretisch wel mogelijk.

De gedachte die ten grondslag ligt aan de hieronder voorgestelde werkwijze is dat waar e-mailberichten in grote mate een zakelijk karakter kennen, dit bij chatberichtenverkeer anders is. Uit eigen onderzoek blijkt dat persoonlijke en zakelijke conversaties aangaande het onderwerp COVID-19 door elkaar lopen. Dit betekent dat de betrokken persoon (lees: politieke leiding, ambtelijke leiding, MT-

⁵ ABRvS 20 maart 2019, ECLI NL RVS 2019 899, bevestigd in ABRvS 21 oktober 2020, ECLI:NL:RVS:2020:2477.

⁶ Onderzocht wordt of deze selectie ook past bij de vereisten vanuit de Archiefwet en hotspotlijst.

leden van betrokken directies of sleutelfunctionarissen) hier een hogere mate van gevoeligheid, in de zin van aantasting van zijn of haar privacy, kan ervaren.

PSG
pSG
Nafase COVID-19

Vier opties

In de voorgestelde werkwijze krijgt de betrokken persoon de keuze tussen vier opties, waarbij het recht van de persoon om te weigeren en in het geheel niet mee te werken aan het uitnemen of aanleveren van chatberichten expliciet een optie is. Duidelijk wordt gemaakt aan de medewerker dat weigeren geen arbeidsrechtelijke consequenties heeft. Door de keuzemogelijkheid houdt de persoon regie op zijn of haar berichten en daarmee op zijn of haar privacy. De vier opties waar de persoon uit kan kiezen zijn als volgt:

Kenmerk
2342898-1006392

1. De betrokken persoon levert zelf de voor de verantwoording aangaande COVID-19 crisis noodzakelijke berichten aan;
2. De betrokken persoon laat dit doen door zijn/haar secretariaat of door zijn/haar persoonlijke beleidsmedewerker;
3. De betrokken persoon geeft toestemming aan de programmadirectie Nafase COVID-19 om de relevante berichten in het kader van COVID-19 geautomatiseerd uit te nemen en te selecteren op relevantie;
4. De persoon kan weigeren.

De persoon die voor optie 3 kiest, krijgt bij het maken van een afspraak voor het uitlezen van de telefoon een formulier toegestuurd waarbij hij of zij kan aangeven of hij of zij alle chats wil laten uitlezen (zonder selectie van tevoren), zelf irrelevante chats vóór het overhandigen van de telefoon wil verwijderen, of aan de programmadirectie Nafase COVID-19 wil aangeven welke chats dan wel chatgroepen relevant zijn. Dit kan direct op het formulier worden aangegeven.

Informatievoorziening naar de betreffende personen

De betrokken personen, inclusief diegenen waarvan reeds de telefoon is uitgenomen en de relevante chatberichten al van zijn geselecteerd, zullen worden geïnformeerd over de nieuwe werkwijze. Ook wordt een werkinstructie gemaakt voor degene die zelf de relevante berichten wil (laten) selecteren (optie 1 en 2). Zo wordt het laagdrempelig en gemakkelijk gemaakt voor de persoon om zelf de regie te houden. Daarnaast wordt de betrokken persoon ook geïnformeerd over het feit dat de geselecteerde chats na automatische selectie (indien hij of zij voor optie 3 kiest) eerst nog ter validatie aan hem of haar worden voorgelegd voordat de chatberichten ten behoeve van een verantwoordingsverzoek toegankelijk worden gemaakt. Tot slot zullen betrokkenen individueel om toestemming worden gevraagd om het bij hen uitgenomen chatverkeer blijvend te mogen bewaren voor zover dat destijds integraal bij hen is uitgenomen, dus ook met betrekking tot bestuurlijke besluitvorming over andere onderwerpen. Hiermee wordt geanticipeerd op besluitvorming in de BRBV. Chats met betrekking tot COVID-19 die in het kader van de Wob zijn uitgenomen, blijven hoe dan ook integraal bewaard op grond van de Archiefwet. De Archiefwet biedt voldoende grond om privacy ook op lange termijn te borgen.

Beschouwing

Aan de hand van een viertal belangrijke aspecten wordt de voorgestelde werkwijze hieronder nog kort beschouwd:

Verantwoording: Door middel van het uitnemen van telefoons en het selecteren van relevante chatberichten of het aanleveren daarvan door de betrokken personen, wordt rechtgedaan aan de uitspraak van de Raad van State en kan aan

toekomstige verantwoordingsverzoeken worden voldaan. Het belang van het verlenen van medewerking hierbij door de individuele medewerker is eerder door de SG en pSG al benadrukt (zie de door hen verstuurde mails in de bijlage). Dit laat onverlet dat de medewerker het recht heeft medewerking hieraan te weigeren, zoals reeds hierboven benoemd.

pSG
pSG
Nafase COVID-19

Kenmerk
2342898-1006392

Volledigheid: De chatberichten worden bij optie 3 geautomatiseerd geselecteerd op hun relevantie. Doordat met bepaalde trefwoorden wordt gezocht bestaat het risico dat een aantal relevante chatberichten niet wordt gevonden. De inschatting is dat ongeveer 95% *volledigheid* zal worden bereikt. Bij optie 1 en 2 is de volledigheid afhankelijk van de (subjectieve) selectie door de betreffende persoon.

Transparantie: Het geautomatiseerd uitlezen en selecteren van chatberichten leidt tot een werkwijze die vergelijkbaar is met de manier waarop het e-mailverkeer binnen de Wob-procedure wordt toegepast, hetgeen zorgt voor een *goed uit te leggen en transparante werkwijze*.

Inzet individu: Door te kiezen voor één van de vier werkwijzen *bepaalt de persoon zelf* in welke mate hij of zij ontzorgd wil worden, rekening houdend met de door hem of haar gewenste privacy.

Advies: het instemmen met de voorgestelde werkwijze.

Beslispunt: gaat de Bestuursraad akkoord met deze voorgestelde werkwijze?

4. Ter informatie: Continuering LCH-lijn t.a.v. overige consortia

Ten slotte willen we u ter informatie meegeven dat de programmadirectie Nafase COVID-19 de zogenaamde 'LCH-lijn' zal continueren ten aanzien van de overige consortia. De LCH-lijn houdt in dat alle informatie waarover ambtenaren van VWS beschikken inzake het LCH en de in dat kader tot stand gekomen overeenkomsten of afspraken, worden veiliggesteld bij VWS. In bredere zin betekent dit dat de programmadirectie enkel de stukken van VWS-kerndepartement medewerkers (inclusief gedetacheerden vanuit andere ministeries) veiligstelt die een rol hebben gespeeld in de betreffende consortia en de in dat kader tot stand gekomen overeenkomsten of afspraken, dus alleen datgene waar VWS verantwoordelijkheid voor draagt. De LCH-lijn is in lijn met de Archiefwet en dienstig aan de afhandeling van Wob-verzoeken.



Ministerie van Volksgezondheid,
Welzijn en Sport

verslag

**Secretaris-Generaal/ plv.
Secretaris-Generaal**
Directie Bestuurlijke en
Politieke Zaken
Bureau Bestuurlijke-politieke
advisering

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34

www.rijksoverheid.nl

Inlichtingen bij
5.1.2.e
(Senior) Adviseur

Datum
20 april 2021
Aantal pagina's
3

Betreft	Bestuursraad
Vergaderdatum en -tijd	16 april 2021 12:00 – 14:30 uur
Vergaderplaats	Webex
Aanwezig	5.1.2e (verslag)
Afwezig	IG IGJ

1. Actualiteiten

a. Vooruitblik BR en Actualiteitenstaf

buiten reikwijdte

Actualiteiten

buiten reikwijdte

buiten reikwijdte

buiten reikwijdte

**Secretaris Generaal / plv.
Secretaris Generaal**
Directie Bestuurlijke en
Politieke Zaken
Bureau Bestuurlijke-politieke
advisering

Datum
9 april 2021

2. Inhoudelijke Onderwerpen

a. buiten reikwijdte

b. Geautoriseerd veiligstellen (NC19), 5.1.2.e, 5.1.2.e en 5.1.2.e

- De COVID-19 crisis leidt tot een ongeken- en alsmaar groeiende hoeveelheid aan relevante documenten, e-mails en chatberichten. Doel is het op een zoveel mogelijk automatische, eenduidige en efficiënte manier informatie veilig te stellen en te ontsluiten voor de MT leden en de BR, waarbij directies zoveel mogelijk worden ontzorgd terwijl de privacy van de betrokken personen goed wordt geborgd.
- Ten opzichte van de huidige situatie stelt NC19 voor de betrokkenen in het vervolg vier opties voor te leggen op welke wijze informatie wordt aangeleverd. Betrokkene kan ook weigeren m.b.t. aanleveren chats. Vanuit de BR wordt aangegeven dat de informele consequenties daarvan goed doordacht moeten worden. WJZ heeft aangegeven dat weigeren geen arbeidsrechtelijke consequenties heeft.
- De BR stemt in met de beslispunten. Daarnaast wordt in voorliggende nota aangegeven dat in het kader van duurzaam veiligstellen en archiveren van berichtenverkeer zinvol kan zijn om het berichtenverkeer breder te archiveren. De BR neemt hier nu geen besluit over.
- Vanuit de BR wordt waardering uitgesproken voor het geleverde werk van het team m.b.t. het veiligstellen van informatie.

c. buiten reikwijdte

buiten reikwijdte

d. buiten reikwijdte

**Secretaris Generaal / plv.
Secretaris Generaal**
Directie Bestuurlijke en
Politieke Zaken
Bureau Bestuurlijke-politieke
advies

Datum
9 april 2021

3. Collegiale toetsing

Ministerie van Volksgezondheid,
Welzijn en Sport

Aan:
De minister van VWS
De minister voor MZS
De Staatssecretaris van VWS

Deadline: 31 mei 2021

Secretaris Generaal / plv.
Secretaris Generaal
plv. SG
Nafase Covid-19

Ontworpen door

5.1.2.e

5.1.2.e @minvws.nl

Datum

17 mei 2021

Kenmerk

2362605-1009188

Zaaknummer

1009188

nota

Veiligstellen chats

(ter beslissing)

Paraaf directeur

1 Aanleiding voor deze nota

VWS wil transparant zijn over haar handelen tijdens de COVID-crisis en de keuzes die zijn gemaakt zorgvuldig toelichten. Om dit te realiseren is de programmadirectie Nafase COVID-19 medio september 2020 opgericht. Eén van de taken van de programmadirectie is het veiligstellen en archiveren van alle relevante informatie over COVID-19 binnen het kerndepartement van VWS. In de eerste helft van 2020 is reeds door de directeur BPZ en directeur WJZ met de minister van VWS gesproken over het archiveren van chats (Whatsapp, iMessage en sms-berichten) uit zijn telefoon. Met de adviseur van de minister is toen een start gemaakt voor archivering van zijn chats. Door de oprichting van de Programmadirectie Nafase COVID-19 is de werkwijze voor het veiligstellen van informatie veranderd. In deze nota wordt u een voorstel gedaan voor een meer solide manier van archivering. Deze werkwijze zorgt er enerzijds voor dat alleen de COVID-gerelateerde chats op een efficiënte wijze worden veiliggesteld en anderzijds dat de niet relevante chatberichten definitief worden verwijderd.

2 Beslispunten

Gaat u akkoord met:

- het veiligstellen van COVID-gerelateerde chatberichten die expliciet door uzelf (voorbereid door uw ambtelijk adviseur) zijn aangemerkt als relevant? Het archiveren van relevante chats gebeurt uitdrukkelijk pas na akkoord op de inhoud van de geselecteerde chats en de niet relevante chatberichten worden definitief verwijderd. U kunt het veiligstellen en archiveren van uw chatberichten weigeren. Hierbij moet worden aangetekend dat de kans bestaat dat dezelfde chats op de telefoons van anderen wel zijn of worden gearchiveerd en via een andere weg toch openbaar gemaakt kunnen worden.

3 Samenvatting en conclusies

Voor het veiligstellen en archiveren van chatberichten zijn binnen het ministerie afspraken gemaakt. Deze afspraken zijn opgenomen in de nota 'Alternatieve wijze veiligstellen COVID-informatie' die de Bestuursraad op 16 april 2021 heeft vastgesteld (zie bijlage). Door de sleutelpositie van de bewindslieden van VWS in de bestrijding van de coronacrisis en de vertrouwelijkheid van deze chatberichten stellen wij in deze nota een op maat gemaakte werkwijze voor.

Secretaris Generaal / plv.
Secretaris Generaal
plv. SG
Nafase Covid-19

Kenmerk

A. Werkwijze veiligstellen chats MVWS

Er is een werkwijze bedacht waarbij uitsluitend de adviseurs van de bewindslieden toegang hebben tot de telefoon en alleen die chats worden uitgenomen waar de bewindslieden uitdrukkelijk toestemming voor hebben gegeven. Uit die selectie worden alleen chats veiliggesteld die voldoen aan het criterium 'COVID-gerelateerd', zakelijk en besluitvormend en deze chats worden pas na expliciete toestemming gearchiveerd. De overige chats uit de selectie, die niet aan deze criteria voldoen, worden definitief verwijderd.

De werkwijze ziet er als volgt uit:

1. Vaststellen wat relevante chatgroepen en "contacten" zijn door de bewindslieden en hun ambtelijk adviseurs.
Uw adviseur legt u een lijst voor met de chats die door uw adviseur voorgeselecteerd zijn als relevant en niet-relevant. U kunt op basis van deze lijst aangeven of deze selectie klopt. De ambtelijk adviseur leest daartoe de chatgroepen en "contacten" uit (bijv. via WhatsApp Web).
2. De adviseurs van de bewindslieden lezen deze geselecteerde relevante chats uit en zetten die op een hiervoor aangewezen laptop.
3. Het automatisch selecteren van relevante en niet relevante berichten door slimme software die zoekt op trefwoorden. Deze werkwijze wordt sinds een jaar gehanteerd bij de afhandeling van COVID-19 gerelateerde Wob-verzoeken en is bewezen effectief.
4. Het terugleggen van geselecteerde chats bij de ambtelijk adviseur om te toetsen op relevantie en verwijderen van gevoelige en/of ongewenste informatie.
5. Het archiveren van de definitieve set van relevante chats en het definitief verwijderen van de niet relevante chats.

B. Beleid aangaande veiligstellen en archiveren chatberichten

Het ministerie van VWS wil relevante informatie rond het coronavirus zorgvuldig vastleggen voor doeleinden zoals in de aanleiding staan beschreven. Op welke wijze dit dient te geschieden, is beschreven in de hiervoor genoemde nota 'Alternatieve wijze veiligstellen COVID-informatie'. In deze werkwijze zijn de privacy en rechten van betrokkenen gewaarborgd en deze zijn besproken met de Functionaris Gegevensbescherming en de Privacy Officer.

4 Draagvlak politiek

Het ministerie van VWS wil transparant zijn over haar handelen tijdens de COVID-crisis en de keuzes die zijn gemaakt zorgvuldig toelichten. Informatie vanuit berichten van de telefoons van bewindspersonen kunnen bijdragen aan deze beoogde transparantie. VWS gaat hierin tevens mee in de lijn van de kabinetsreactie op de POK, waarin is toegezegd dat er meer openheid en transparantie in de informatievoorziening naar de Kamer zal komen.

5 Draagvlak maatschappelijk en eenduidige communicatie

NVT

Secretaris Generaal / plv.

Secretaris Generaal

plv. SG

Nafase Covid-19

6 Financiële en personele gevolgen

NVT

Kenmerk

7 Juridische aspecten haalbaarheid

Wetgeving, met name de Wob en Archiefwet, verplicht VWS om gerede inspanningen te verrichten om de informatie uit berichtenverkeer veilig te stellen voor verantwoording, beantwoording van Wob-verzoeken en archivering in het algemeen belang. Echter om privacyrisico's te mitigeren, mag een VWS ambtenaar weigeren om chatberichten veilig te stellen zonder dat dit arbeidsrechtelijke consequenties heeft. Hierbij moet worden aangetekend dat de kans bestaat dat dezelfde chats op de telefoons van anderen wel zijn of worden gearhiveerd en via een andere weg toch openbaar gemaakt kunnen worden.

8 Afstemming (intern, interdepartementaal en met veldpartijen)

BPZ is nauw betrokken geweest bij de totstandkoming van deze nota.

BPZ, WJZ, OBP en de Functionaris Gegevensbescherming zijn nauw betrokken geweest bij de totstandkoming van de reeds genoemde nota 'Alternatieve wijze veiligstellen COVID-informatie' die de Bestuursraad op 16 april 2021 heeft vastgesteld.

9 Gevolgen administratieve lasten

NVT

10 Toezeggingen

NVT

11 Fraudetoets

NVT

Toestemmingformulier voor het verwerken van chatberichten

Inleiding

Beste heer/mevrouw,

Het adequaat veiligstellen, doorzoekbaar maken en ter beschikking kunnen stellen van Covid-19 gerelateerde informatie kan onderdeel zijn van meerdere wettelijke verplichtingen (Wob, WOO, Archiefwet, Wet op de parlementaire enquête et cetera). Voor de Wob en Archiefwet is op 20 maart 2019 door de Raad van State¹ vastgesteld dat chatberichten die bij het uitvoeren van overheidstaken zijn geproduceerd moeten worden veiliggesteld. Als overheidsorgaan moet het ministerie van Volksgezondheid Welzijn en Sport dan ook zorg dragen dat deze informatie niet verloren gaat. Dit vormt de grondslag voor het verwerken van uw chatberichten. In de e-mail heeft u reeds kunnen lezen waarom we relevante chatberichten veiligstellen. Hieronder lichten we dit verder toe, als ook de gehanteerde werkwijzen.

Wat is een relevant chatbericht?

- Zakelijk;
- COVID-19 gerelateerd;
- Besluitvormend. Hieronder wordt verstaan (zie tevens bijlage 1, pagina 8):
 - Het bericht met het besluit zelf;
 - De berichten die duidelijk maken waarover een besluit wordt genomen;
 - De berichten die duidelijk maken wat de onderbouwing is van het besluit;
 - Relevante informatie die aan het besluit voorafging en die aanleiding kan zijn voor het besluit.

Het gaat hierbij enkel om relevante chatberichten tussen 1 december 2019 tot heden, of de periode tussen uw in-en uitdiensttreding in uw huidige functie.

Werkwijze

De verschillende mogelijkheden voor het uitlezen van Covid-19 gerelateerde chatberichten worden hieronder aangegeven. Wij gaan zorgvuldig om met uw privacy, alle medewerkers van het team V&A hebben een VOG en een geheimhoudingsverklaring getekend.

Vanzelfsprekend worden de uitgelezen chatberichten altijd opgeslagen in een beveiligde omgeving.

Hieronder beschrijven we drie keuzes. U kiest er hier één van. Vervolgens nemen we met u contact op. Ter informatie benoemen wij graag dat wij de gekozen opties vastleggen in onze administratie, in het kader van verantwoording.

¹ ABRvS 20 maart 2019, ECLI:NL:RVS:2019:899, bevestigd in ABRvS 21 oktober 2020, ECLI:NL:RVS:2020:2477.

Keuze 1: Relevante chats veiligstellen

Bij het kiezen voor keuze 1 zal een moment ingepland worden waarin op de Resident uw telefoon wordt uitgelezen om relevante chatberichten veilig te stellen. In dit geval vinkt u keuze 1 aan in onderstaand keuzemenu, geeft u daarbij aan welke chatgesprekken wij zullen uitlezen en stuurt u dit ingevulde formulier retour. Na het veiligstellen van de relevante chatberichten zullen deze chats worden gevalideerd door u in overleg met het team V&A.

Levert u liever zelf uw chatgesprekken bij ons aan, zonder tussenkomst van team V&A? Geeft u dit dan aan in het formulier. Vervolgens nemen wij telefonisch contact met u op om de werkwijze zelfstandig chats uitlezen op afstand toe te lichten.

Keuze 2: Geen relevante chats

U heeft op dit moment geen relevante chatberichten zoals omschreven in de inleiding. In dit geval vinkt u keuze 2 aan in onderstaand keuzemenu en stuurt u dit ingevulde formulier retour.

Keuze 3: Geen medewerking

U bent niet verplicht om mee te werken aan dit proces en kunt er voor kiezen niet mee te werken en uitlezing te weigeren. Dit heeft geen arbeidsrechtelijke consequenties. In dit geval vinkt u keuze 3 aan in onderstaand keuzemenu en stuurt u dit ingevulde formulier retour. Volledigheidshalve willen wij u er wel op wijzen dat degene met wie u een chat of sms heeft uitgewisseld, mogelijk wél zijn/haar berichtenverkeer laat uitlezen en de betreffende berichten gebruikt worden voor het kunnen beantwoorden van een Wob-verzoek en de voorbereiding op een parlementaire enquête.

Keuzemenu

Geef aan welke optie u kiest

- | | |
|--|-----------------------|
| Keuze 1: Relevante chats veiligstellen | ☐ |
| Keuze 2: Geen relevante chats | ☐ |
| Keuze 3: Geen medewerking | ☐ |

Heeft u keuze 1 geselecteerd, ga dan door naar de volgende pagina.

Heeft u keuze 2 of 3 geselecteerd, ga dan door naar pagina 7.

Uitwerking keuze 1

Om uw chatverkeer juist en correct te kunnen verwerken, hebben wij de volgende gegevens nodig:

Voor- en achternaam

.....

Ik kan wel/niet naar de Resident komen.

.....

Is er een periode geweest tussen december 2019 en verder dat u een andere functie dan MT-lid of hoger heeft bekleed? Alleen MT-leden en hoger vallen binnen de reikwijdte van uit te nemen chatberichten.

.....

Wat is uw telefoonnummer?

.....

Welk type telefoon heeft u?

Type telefoon

- Iphone ☐
- Android ☐
- Anders ☐

.....

Welke berichtenapps heeft u gebruikt? (WhatsApp/SMS/iMessage)

.....

Heeft u zelf berichten of chats verwijderd die mogelijk van belang kunnen zijn?

.....

Heeft u gedurende uw huidige functie een nieuwe telefoon gekregen, is uw telefoon gehackt of is er iets voorgevallen wat ervoor kan zorgen dat berichten verloren zijn gegaan?

.....

Ontvangt u binnenkort een nieuwe telefoon?

.....

Gaat u binnenkort uit dienst? Zo ja, per wanneer?

.....

Op welke telefoonnummer of emailadres kunnen we u bereiken als u uit dienst bent?

.....

Heeft u nog vragen en/of opmerkingen?

.....

Ga door naar de volgende pagina.

Tabel relevante chatberichten: zelf invullen.

Nr.	Naam van chat/persoon (individuele en groepschats) Indien alleen telefoonnummer, ook graag volledige naam noteren.	WhatsApp, iMessage of SMS
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		
36		
37		
38		
39		
40		
41		
42		
43		
44		
45		
46		
47		

Meer chatberichten? Zie volgende pagina.

Nr.	Naam van chat/persoon (individuele en groepschats) Indien alleen telefoonnummer, ook graag volledige naam noteren.	WhatsApp, iMessage of SMS
48		
49		
50		
51		
52		
53		
54		
55		
56		
57		
58		
59		
60		
61		
62		
63		
64		
65		
66		
67		
68		
69		
70		
71		
72		
73		
74		
75		
76		
77		
78		
79		
80		
81		
82		
83		
84		
85		
86		
87		
88		
89		
90		
91		
92		
93		
94		

Zie volgende pagina voor afronding.

Ondergetekende geeft toestemming aan Programmadirectie Nafase Covid-19 Veiligstellen en Archiveren om de chatberichten te verwerken.

Naam

Handtekening en datum

.....

.....

Kunt u dit document ingevuld en ondertekend retourneren of meenemen naar onze afspraak? Alvast bedankt.

Bij vragen en opmerkingen kunt u terecht bij:

Email: 5.1.2.e -19@minvws.nl

Telefoonnummer: 06-5.1.2.e

Met vriendelijke groet,

Projectteam Veiligstellen & Archiveren chatberichten van de Programmadirectie Nafase Covid-19

Bijlage 1 App met beleid

📱🗨️ App met beleid; niet over beleid.

Wat delen we wel?

Informele informatie

Zullen we straks even lunchen?

✓ Ok, zie je zo!

Proces- en werkgerelateerde informatie

Kun je nog even kijken naar de nota voor de stuurgroep?

✓ Is goed, ik mail je er vanmiddag over

Verantwoord omgaan met berichtenapps is belangrijk

- Omdat werkgerelateerde berichten op zakelijke- én privételefoons kunnen worden opgevraagd in een Wob-verzoek;
- Om als Rijksoverheid transparant te kunnen handelen;
- Privacy- en cybersecurityrisico's te verkleinen.

Wat delen we niet?

Vertrouwelijke en gerubriceerde informatie

[Redacted]

[Redacted]

✗

Persoonsgevoelige informatie

In welke schaal hadden we Jan Jansen ook alweer ingedeeld?

Schaal 10.4

✗

Let op!

Bestuurlijke besluitvorming

Heb je de beslismaat al gezien?

Ja, scenario 2 is akkoord

!

- ✉ Bestuurlijke besluitvorming? Gebruik dan de mail.
- 🔥 Uitzondering: in geval van crisis mag je appen, als dat handig of nodig is.
- 📁 Wel geappt over bestuurlijke besluitvorming? Dan moeten berichten die van belang zijn voor bestuurlijke besluitvorming worden opgeslagen in het Document Management Systeem.

Lees meer op informatiehuishouding.nl

Deze instructie is een uitwerking van het Rijksbrede beleid voor de omgang met berichtenapps, ontwikkeld door RDDI in samenwerking met de Ministeries van Onderwijs, Cultuur en Wetenschap en Binnenlandse Zaken en Koninkrijksrelaties.



Ministerie van Volksgezondheid,
Welzijn en Sport

Deze nota is bedoeld om openbaar gemaakt te worden: **Nee**

Aan

De leden van de
Bestuursraad

Deadline: 13 mei
grondslag bewaren
berichtenverkeer

nota

Beleid VWS m.b.t. uitlezen en archiveren van
berichtenverkeer ('Beleidslijn berichtenverkeer VWS')

TER BESLISSING

**Secretaris Generaal /
plv. Secretaris
Generaal**

Dir Organisatie, Bedrijfs-
en Personeel
Afd. CIO kern en
informatiemanagement

Opgesteld door

5.1.2.e
5.1.2.e
065.1.2.e
5.1.2.e@minvws.nl

Datum

9 mei 2022

Kenmerk

Uw kenmerk

Zaaknummer

Bijlage(n)

1

1. Aanleiding

VWS dient voorzieningen te treffen voor het uitlezen en archiveren van berichtenverkeer m.b.t. bestuurlijke besluitvorming uit applicaties zoals WhatsApp en SMS. Dit is een gevolg van een uitspraak die de Raad van State in maart 2019 deed. In deze zaak werd bepaald dat dergelijke berichten onder de Wet openbaarheid bestuur (Wob) vallen. Daarnaast vallen deze berichten ook onder de werkingssfeer van de Archiefwet en dienen ze in het formele archief te worden opgenomen. Vanwege de kabinetswissel en het vertrek van bewindspersonen is gekozen om de VWS-brede beleidslijn eind 2021 versneld voor te leggen aan de SG en pSG. Vandaag leggen wij de doorontwikkelde versie van deze beleidslijn voor aan de Bestuursraad.

2. Geadviseerd besluit

De Bestuursraad wordt gevraagd akkoord gaan met:

- deze *Beleidslijn berichtenverkeer VWS*¹ voor het uitlezen en archiveren van berichtenverkeer met betrekking tot bestuurlijke besluitvorming binnen VWS. De uitvoering van deze beleidslijn zal starten na oplevering van een goedgekeurde Data Protection Impact Assessment (DPIA) incl. een advies van de Functionaris gegevensbescherming (FG)²;
- het voorstel om de topfuncties (schaal 16 en hoger) binnen VWS hierbij als primaire doelgroep aan te wijzen, inclusief de leden van de Bestuursraad en de bewindspersonen (voor zover het zakelijk, niet privé of partijpolitiek, berichtenverkeer betreft);
- de verschillende opties voor het uitlezen c.q. de afgifte van relevant berichtenverkeer door betrokkenen;
- het voorstel om bij de uitgifte van zakelijke smartphones de medewerker actief te attenderen op deze beleidslijn en de eigen verantwoordelijkheid ten aanzien van het gebruik van berichtenapps. Daarbij staat voorop dat het gebruik van berichtenapps bij bestuurlijke beleidsvorming ten eerste wordt afgeraden. Mocht in het kader van bestuurlijke besluitvorming een enkele keer wel gebruik gemaakt zijn van berichtenverkeer, dan moet deze informatie óók bevestigd worden (bijvoorbeeld in een nota). Daarna kan het archiveren van de betreffende chatberichten vervallen.

¹ Zie bijlage bij deze nota.

² De andere concernonderdelen van VWS moeten – conform de opdracht vanuit Open op Orde – ook aan de slag, maar doen dat o.b.v. een eigen implementatiestrategie.

- In te stemmen met een pilotfase tot eind 2022. In januari 2023 wordt de evaluatie in BR geagendeerd.

Datum
9 mei 2022
Kenmerk

3. Kernpunten

Met de Beleidslijn wordt aangesloten op de Rijksbrede kaders voor de omgang met berichtenapps.³ Berichtenverkeer met betrekking tot bestuurlijke besluitvorming maakt onderdeel uit van de verantwoordingsinformatie van het Ministerie. De *Beleidslijn berichtenverkeer VWS* heeft als doel dit onder beheer te brengen binnen geldende juridische en beleidsmatige kaders. Omwille van de (technische) uitvoerbaarheid is de reikwijdte nu nog beperkt tot WhatsApp, iMessaging en SMS. Dit laat onverlet dat ook het relevante berichtenverkeer uit andere berichtenapps, zoals Signal, gearchiveerd zal moeten worden (door screenshots).

Bij VWS Kern is met het onder beheer brengen van WhatsApp, iMessaging en SMS al ervaring opgedaan voor wat betreft Covid19-gerelateerde berichten. En er vindt afstemming plaats met de werkwijze bij andere departementen. Voor het periodiek uitlezen van het berichtenverkeer van bewindspersonen en topfuncties staan verschillende opties open.

4. Dilemma's

In verband met de verantwoordingsinformatie van het Ministerie was het van groot belang dat ook het relevante berichtenverkeer van vertrekkende bewindspersonen veiliggesteld werd ten behoeve van de archivering. Vooruitlopend op de vaststelling van deze richtlijn is daarom met instemming van de vertrekkende bewindspersoon, het relevante chatverkeer veiliggesteld. De Bestuursraad wordt daarom nu gevraagd akkoord te gaan met de voorgestelde *Beleidslijn berichtenverkeer VWS*⁴ voor het uitlezen en archiveren van berichtenverkeer binnen VWS. De uitvoering van deze beleidslijn bij VWS Kern zal pas starten na oplevering van een goedgekeurde Data Protection Impact Assessment (DPIA) incl. een advies van de Functionaris gegevensbescherming (FG)⁵.

Berichtenapps staan in de privé-omgeving van mobiele telefoons en worden niet beheerd door SSC-ICT. Voor app-groepen komt binnenkort wel Teams beschikbaar vanuit SSC-ICT. De werktelefoons mogen vanwege privacybelangen niet zomaar worden gevorderd ten behoeve van het uitlezen en archiveren van berichten. Hiervoor moet aan de eigenaar van het relevante berichtenverkeer altijd toestemming gevraagd worden. Dit geldt in het geval van de beleidslijn voor bewindspersonen en voor de topfuncties (schaal 16 en hoger).

Vanwege het voorgaande is de bewindspersoon of de medewerker eigenaar van de informatie en zelf verantwoordelijk voor een goed beheer van deze informatie zolang het in de privé-omgeving van de smartphone staat. Om te kunnen voldoen aan toekomstige raadplegingsverzoeken zonder tussenkomst van de oorspronkelijke eigenaar, stelt de beleidslijn dat na het uitlezen en het gezamenlijk valideren (met OBP en Doc-Direkt) van relevant berichtenverkeer

³ Samengevat in *Bewaren van chatberichten*, een handreiking van het Rijksprogramma Duurzaam Digitale Informatiehuishouding (RDDI, juni 2020)

⁴ Zie bijlage bij deze nota.

⁵ De andere concernonderdelen van VWS moeten – conform de opdracht vanuit Open op Orde – ook aan de slag, maar doen dat o.b.v. een eigen implementatiestrategie.

met betrokkene, VWS als verantwoordelijke overheidsorgaan⁶ de eigenaar is van deze informatie. Daarom wordt het relevante berichtenverkeer niet alleen veiliggesteld maar ook gearchiveerd (conform de archief-selectielijst).

Datum
9 mei 2022
Kenmerk

5. Toelichting

Berichtenverkeer met betrekking tot bestuurlijke besluitvorming (hierna: relevant berichtenverkeer) maakt onderdeel uit van de verantwoordingsinformatie van het Ministerie. De realiteit vraagt om maatregelen om te voorkomen dat relevante informatie verloren gaat.

Deze *Beleidslijn berichtenverkeer VWS* heeft dan ook als doel relevant berichtenverkeer onder beheer te brengen, dit binnen geldende juridische en beleidsmatige kaders en ten behoeve van een zo eenduidig mogelijke uitvoering. De voornaamste doelgroep van deze beleidslijn is de groep topfuncties (schaal 16 en hoger) omdat het voor de hand ligt dat deze beschikt over relevant berichtenverkeer. Hiermee sluiten we aan bij de definitie van sleutelfiguren van de Handreiking e-mail-archivering, en wordt een beperktere scope gehanteerd dan nu toegepast voor COVID-19. Omwille van de juridische haalbaarheid (AVG) en (technische) uitvoerbaarheid is de reikwijdte beperkt tot WhatsApp, iMessaging en SMS.

De beleidslijn dient daarmee te worden beschouwd als een eerste stap in het uitlezen (en archiveren) van dit type bron. Bij VWS Kern is hier al ervaring mee opgedaan voor wat betreft Covid19-gerelateerde berichten: sinds juni 2020 is er een specifieke beleidslijn (en werkwijze) voor het veiligstellen en bewaren van berichtenverkeer met betrekking tot Covid19 in relatie tot de Wob. Een functionaris kan daarbij zelf berichten aanleveren of zich hierbij laten ondersteunen. De processtappen die hiertoe binnen VWS Kern worden gevolgd staan in de bijlage van de beleidslijn. Deze werkwijze kan tevens als voorbeeld dienen voor het Concern. De *Beleidslijn berichtenverkeer VWS* borduurt hierop voort, echter vervangt deze specifieke beleidslijn niet omdat de doelgroep en doelstelling verschilt. Met de beleidslijn wordt tevens aangesloten op de Rijksbrede kaders voor de omgang met berichtenapps.⁷

Op verzoek van de Stuurgroep van de programmadirectie Nafase Covid19 (NC19) wordt het uitlezen en veiligstellen van het berichtenverkeer gedaan door "NC19" tot de einddatum van de onderzoeksperiode van de Parlementaire Enquête Covid-19.

a. Draagvlak politiek

De *Beleidslijn berichtenverkeer VWS* is in lijn met de kabinetsreactie op het rapport van de Parlementaire ondervragingscommissie Kinderopvangtoeslag (POK), waarin is toegezegd dat er meer openheid en transparantie in de informatievoorziening zal komen. Het bewaren van dit berichtenverkeer is onderdeel van het Actieplan VWS Open op Orde.⁸ Ervaringen, inzichten en werkwijzen, die in het programma Nafase Covid19 zijn opgedaan en ontwikkeld voor het uitlezen en bewaren van berichtenverkeer, vormen de basis voor de voorgestelde *Beleidslijn berichtenverkeer VWS*. Echter, het zakelijk appen moet uitzondering blijven, het is een ongewenste manier om besluiten te nemen en voor te bereiden.

⁶ Zoals bedoeld in artikel 1.1 van de Archiefwet 2021

⁷ Samengevat in Bewaren van chatberichten, een handreiking van het Rijksprogramma Duurzaam Digitale Informatiehuishouding (RDDI, juni 2020)

⁸ Actieplan informatiehuishouding VWS: VWS Open en op orde 2021-2026, versie 1.0, d.d. 1 juli 2021.

b. Draagvlak maatschappelijk en eenduidige communicatie
Idem als bij a.

Datum
9 mei 2022

Kenmerk

c. Financiële en personele gevolgen

In maart 2019 heeft de Afdeling bestuursrechtspraak van de Raad van State bepaald dat WhatsAppberichten, sms'jes en gelijksoortige chatberichten documenten zijn in de zin van de Wet openbaarheid van bestuur⁹. De WhatsAppberichten vallen ook onder de werkingssfeer van de Archiefwet, voor zover de inhoud ziet op bestuurlijke aangelegenheden die niet op andere wijze is gearriveerd. Daarom dienen deze berichten of onderdelen daarvan in het formele archief te worden opgenomen.

Voor het (periodiek) uitlezen ontstaan nieuwe werkzaamheden, evenals voor de verdere verwerking en opslag van het uitgenomen berichtenverkeer. Immers: in veel gevallen zullen de uitgelezen berichten een bruto-set aan informatie¹⁰ vormen, die ten behoeve van archivering en of Wob-verzoeken tot een relevante netto-set gereduceerd moet worden op basis van een verantwoorde methodiek.

Dit vraagt extra personele inzet en toepassing van software. Er zal worden gestart met een pilot van 3 maanden waarin 40 functionarissen zullen worden ondersteund. De ambitie is om na afloop van de pilot de doelgroep binnen het kerndepartement structureel te ontzorgen. Voor 2022 heeft OBP hiervoor een budget van € 100.000,- beschikbaar.

De impact zal zich hoofdzakelijk beperken tot het kerndepartement, aangezien daar de grootste groep medewerkers met een bestuurlijke functie werkzaam is. Elders in het Concern is het aantal topfuncties en de benodigde personele inzet beperkt. Alleen bij het RIVM is de doelgroep eveneens omvangrijk.¹¹ Het uitlezen en archiveren van relevant berichtenverkeer van vertrokken bewindslieden is opgepakt.

d. Juridische aspecten haalbaarheid

Mobiele werktelefoons mogen vanwege privacy-issues niet zomaar worden gevorderd ten behoeve van het uitlezen en archiveren van berichten. Hiervoor moet aan de eigenaar van het relevante berichtenverkeer altijd toestemming gevraagd worden. Voor de gegevensverwerking in het kader van de Covid-crisis is eerder een DPIA uitgevoerd waarin de grondslagen, de afwegingen, de proportionaliteit, de overwogen alternatieven en de risico's voor de organisatie duidelijk in beeld zijn gekomen. De DPIA, die in dit kader wordt uitgevoerd, betreft het proces van verwerken, opslaan en archiveren van het berichtenverkeer. De Quick Scan hiervoor is reeds in vergevorderd stadium en inhoudelijk afgestemd met WJZ. Hierbij zijn geen blokkerende issues aangetroffen voor de tenuitvoerlegging van deze beleidslijn.

De Functionaris voor de Gegevensbescherming zal op advies van de privacy officer de DPIA beoordelen en van advies voorzien. Naar verwachting is dit proces in het derde kwartaal gereed.

De voorgestelde *Beleidslijn berichtenverkeer VWS* geeft de medewerker de ruimte om privacygevoelige informatie uit te zonderen van archiveren. De medewerker kan een eigen voorselectie maken van uit te nemen informatie (*opties 1 en 2 op*

⁹ ABRvS 20 maart 2019, ECLI:NL:RVS:2019:899, bevestigd in ABRvS 21 oktober 2020, ECLI:NL:RVS:2020:2477.

¹⁰ Naast berichten in het kader van bestuurlijke besluitvorming zullen ook andersoortige berichten in deze set zitten.

¹¹ Binnen VWS Kern gaat het om ca 40 topfuncties, het RIVM telt 29 topfuncties. Het aantal topfuncties elders binnen VWS is beperkt.

blad 2) of het berichtenverkeer wordt uitgenomen, waarbij relevante berichten worden geselecteerd teneinde te worden bewaard (*optie 3 op blad 2*)¹². De voor bewaring geselecteerde berichten worden vervolgens geïdentificeerd, geclassificeerd naar de beleidsonderwerpen van VWS en opgenomen in een formeel dossier. Een persoon kan ook weigeren mee te werken (*optie 4*), maar gezien de rol en positie van de doelgroep mag redelijkerwijs worden aangenomen dat zij medewerking verleent door gebruik te maken van een van de andere opties.

Datum
9 mei 2022
Kenmerk

Bij de afhandeling van de DPIA wordt mede getoetst of het treffen van mitigerende maatregelen uit oogpunt van privacy het risico met zich meebrengt dat verantwoordingsinformatie van VWS niet wordt gearcheveerd.

Zoals hierboven opgemerkt moet binnen de geselecteerde berichten nog een selectie worden gemaakt welke informatie betrekking heeft op bestuurlijke aangelegenheden en die niet op een andere wijze gearcheveerd zijn en daarom gearcheveerd moeten worden.

e. Afstemming (intern, interdepartementaal en met veldpartijen)

Deze beleidslijn is afgestemd binnen OBP, met de Programmadirecties Nafase Covid-19 en PDO, BPZ, WJZ en de privacy officer van OBP.

Alle medewerkers van VWS worden geïnformeerd over deze richtlijn en werkwijze, in het bijzonder de functionarissen en bewindspersonen, die onder de werking van de *Beleidslijn berichtenverkeer VWS* zullen vallen.

Binnen de Vakgroep Informatiehuishouding VWS wordt de beleidslijn behandeld teneinde de onderdelen goed te informeren.

In Q2 2023 wordt deze beleidslijn geëvalueerd en waar nodig bijgesteld.

f. Gevolgen administratieve lasten

De groep functionarissen (topfuncties schaal 16 en hoger, incl. de leden van de Bestuursraad en de bewindspersonen) waar de beleidslijn op van toepassing is, valt samen met de groep medewerkers waarvan het zakelijk mailverkeer op grond van het Rijksbrede beleid met betrekking tot e-mailarchivering voor blijvende bewaring in aanmerking komt. Van de betreffende functies wordt door iedere Rijksdienst (en dus ook door VWS) jaarlijks een opgave gedaan aan BZK. Deze opgave vormt daarmee de basis voor het (periodiek; bij voorkeur ieder kwartaal) uitlezen van berichtenverkeer als bedoeld in de beleidslijn.¹³ In aanvulling op deze groep wordt het berichtenverkeer van de bewindspersonen ook uitgenomen, dit tévens in lijn met de reeds bestaande werkwijze met betrekking tot het Covid-gerelateerde berichtenverkeer.

Met het van kracht worden van de nieuwe beleidslijn worden de mobiele telefoons van zowel de topfuncties als die van de bewindspersonen "breed" uitgelezen, dat wil zeggen dat al het berichtenverkeer met betrekking tot bestuurlijke besluitvorming, inclusief de COVID-gerelateerde berichten, in één keer wordt uitgelezen zodat de groep topfuncties en de bewindspersonen zo min mogelijk wordt belast.

Grondslag voor de selectie van relevante onderwerpen is het overzicht van de portefeuilles van de bewindspersonen zoals dat door BPZ wordt bijgehouden. Voor VWS Kern wordt dit geoperationaliseerd en onderhouden door OBP, dit in samenspraak met BPZ.

¹² Zie paragraaf 6 van de *Beleidslijn berichtenverkeer VWS*

¹³ Dit ingevolge het *Kader Topstructuur en Topfuncties Rijk 2017*.



Ministerie van Volksgezondheid,
Welzijn en Sport

Organisatie en werkwijze van archiveren en
verwijderen berichtenverkeer van VWS-
kerndepartement

**Secretaris Generaal /
plv. Secretaris
Generaal**
Dir Organisatie, Bedrijfsv
en Personeel
Afd. CIO kern en
informatiemanagement

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
Postbus 20350
2500 EJ Den Haag
www.rijksoverheid.nl

Inlichtingen bij

5.1.2.e

5.1.2.e

Kern en IM

M +31(0)5.1.2.e
5.1.2.e@minvws.nl

Bijlage bij beleidslijn Berichtenverkeer VWS

Datum

9 mei 2022

Aantal pagina's

4

1. Inleiding

Na vaststelling van de Beleidslijn berichtenverkeer VWS in de Bestuursraad krijgt deze praktische invulling voor het VWS-kerndepartement. De vaststelling van deze beleidslijn doet geen afbreuk aan de Beleidslijn veiligstelling COVID-19 chatberichten¹ en is mede hierop gebaseerd. De in deze bijlage beschreven procesgang en beslisboom is opgesteld en wordt beheerd door de afdeling CIO Office Kern en Informatiemanagement van de Directie OBP. Vragen, opmerkingen en verbetervoorstellen kunnen bij deze afdeling worden ingediend.

2. Scope en reikwijdte

De beleidslijn is van toepassing op VWS Concern (Kerndepartement, de hieronder ressorterende concernonderdelen, diensten en ZBO's zonder rechtspersoonlijkheid) en heeft betrekking op

- WhatsApp, iMessaging en SMS;
- alle soorten berichtenverkeer in deze drie toepassingen (zowel appgroepen als één-op-één conversaties).

In deze bijlage wordt de uitvoering voor het kerndepartement beschreven.

3. Algemene uitgangspunten

- Het gebruik van berichtenapps voor formeel zakelijke communicatie wordt zoveel mogelijk beperkt;
- Het gebruik van berichtenapps voor bestuurlijke besluitvorming wordt ten zeerste ontraden. Mocht in het kader van bestuurlijke besluitvorming wel gebruik gemaakt zijn c.q. worden van berichtenverkeer, dan moet deze informatie óók vastgelegd worden in formele documenten zoals een nota (waarna de apps kunnen worden verwijderd);

¹ Beleidslijn veiligstelling COVID-19 chatberichten, 24 juni 2020; vastgesteld in de BRBV van 1 juli 2020. Scope en werkwijze zijn met nadere besluitvorming in de Bestuursraad aangescherpt voor VWS Kern, zie Nota ter beslissing 'Alternatieve wijze veiligstellen COVID-informatie' d.d. 8 april 2021 (kenmerk 2342898-1006392), Programmadirectie Nafase COVID-19; vastgesteld in de BR van 16 april 2021.

- Het berichtenverkeer dat desondanks plaatsvindt, wordt (periodiek, zeswekelijks) uitgelezen en gefilterd. Voor het kerndepartement gebeurt dit door specialisten van OBP en Doc-Direkt.
- De bewindspersoon of de medewerker is eigenaar van de informatie en is uit dien hoofde ook verantwoordelijk voor een goed beheer van deze informatie. Na het uitlezen en bewerken (filteren en zo nodig persoonsinformatie lakken) van relevant berichtenverkeer door betrokkenen is VWS eigenaar van deze informatie. Bij deze overdracht aan OBP/archivering vindt validatie plaats tussen betrokkene en de specialisten van OBP en Doc-Direkt.

4. Uit te lezen en te archiveren berichten

Alle berichten die van belang zijn voor de reconstructie van bestuurlijke besluitvorming dienen te worden uitgelezen en gearchiveerd, tenzij deze informatie al op een andere manier is vastgelegd en gearchiveerd (in dat geval kunnen de chats worden verwijderd).

5. Doelgroepen

In theorie kan iedere medewerker berichten versturen of ontvangen waarbij er sprake is van bestuurlijke besluitvorming. Van de medewerker wordt verwacht dat deze gevraagd en ongevraagd zelf relevant berichtenverkeer aanlevert aan het archiefbeherend onderdeel van de eigen organisatie.

Het ligt echter voor de hand dat bestuurlijke besluitvorming in berichtenverkeer hoofdzakelijk voorkomt bij ambtenaren in topfuncties. Daarom zien we relevant berichtenverkeer met name bij de groep van topfuncties zoals deze gedefinieerd is als doelgroep van het Rijksbrede beleid voor e-mailarchivering. Het gaat daarbij om functionarissen vanaf schaal 16 (topformatie).² In aanvulling hierop wordt ook berichtenverkeer van de bewindspersonen actief uitgelezen en gearchiveerd voor zover dat geen partijpolitiek of privé karakter heeft.

6. Verantwoordelijkheden voor aanlevering, uitlezen en verwerking

Iedere VWS-medewerker is zelf verantwoordelijk voor het aanleveren aan het archiefbeherend onderdeel van berichten die voor archivering in aanmerking komen. Voor het kerndepartement is dat de Directie Organisatie, Bedrijfsvoering en Personeel (OBP). Voor het uitlezen en archiveren van relevant berichtenverkeer van topfuncties binnen het kerndepartement en dat van de bewindspersonen heeft OBP een faciliterende rol. Het berichtenverkeer wordt daarbij door Doc-Direkt in opdracht van OBP periodiek uitgelezen, of zoveel eerder, bij vertrek van betrokkenen. De overige onderdelen van VWS dienen zelf zorg te dragen voor het uitlezen en archiveren, en worden in de werkwijze ondersteund door OBP.

Voor het uitlezen van het berichtenverkeer van topfuncties staan verschillende opties open:

1. de persoon levert zelf berichten aan die relevant zijn uit oogpunt van verantwoording;
2. de persoon wordt zo nodig daarbij geassisteerd door zijn/haar secretariaat of door zijn/haar persoonlijke (beleids)medewerker, maar betrokkene blijft zelf verantwoordelijk voor het aanwijzen van te bewaren berichten;
3. de persoon geeft toestemming aan het archiefbeherend onderdeel om berichten uit te nemen en nader te selecteren op relevantie, alleen relevante gesprekken worden in het formele dossier opgenomen;
4. de persoon kan weigeren.

² *Handleiding voor het aanwijzen en registreren van sleutelfuncties*, versie 1.3 (RDDI februari 2020); in het bijzonder par. 2.3.1.

NB: In verband met de privacyregels verdient het aanbeveling om de werktelefoon gescheiden te houden van de privételefoon.

7. Verwerkingsprotocol

Het uitlezen, selecteren, valideren en archiveren van berichten zijn verwerkingen in de zin van de AVG. Hiervoor dient door het archiefbeherend onderdeel in een verwerkingsprotocol te worden aangetoond, dat de verwerkingen voldoen aan de regels van de AVG. Nadere selectie, validatie en archivering dienen zo spoedig mogelijk na uitlezen plaats te vinden zodat niet-relevante data niet oneigenlijk wordt bewaard. In het protocol dient vermeld te zijn, wie hiervoor verantwoordelijk is, welke termijnen hiervoor gehanteerd worden, hoe het proces van verwijderen vorm is gegeven, hoe dit wordt gelogd en hoe wordt gedocumenteerd wat er is verwijderd. In dit protocol is ook zo duidelijk mogelijk aangegeven welke informatie in aanmerking komt voor archivering en verantwoording en op basis van welke criteria.

8. Beheeromgeving

Het berichtenverkeer heeft een (persoons)gevoelig en of vertrouwelijk karakter en dient op een afgeschermd plaats te worden gearchiveerd in een beheerde omgeving, bij voorkeur in een DMS of een RM-applicatie.

9. Bewaren en vernietigen

Op de bewaartermijnen van het gearchiveerde berichtenverkeer zijn de vastgestelde selectielijsten van VWS van toepassing. Deze termijnen zijn gekoppeld aan het dossier waarin de betreffende berichten zijn opgenomen of waarvan kan worden verondersteld, dat ze er onderdeel van uitmaken.

Aangezien het bestuurlijke besluitvorming betreft, zullen de berichten in ieder geval voor blijvende bewaring in aanmerking komen indien ze betrekking hebben op beleid. De Archiefwet biedt voldoende grond om de privacy ook op lange termijn te borgen.

Na het uitlezen van de berichtenapps dienen de oorspronkelijke apps uit de telefoon te worden verwijderd.

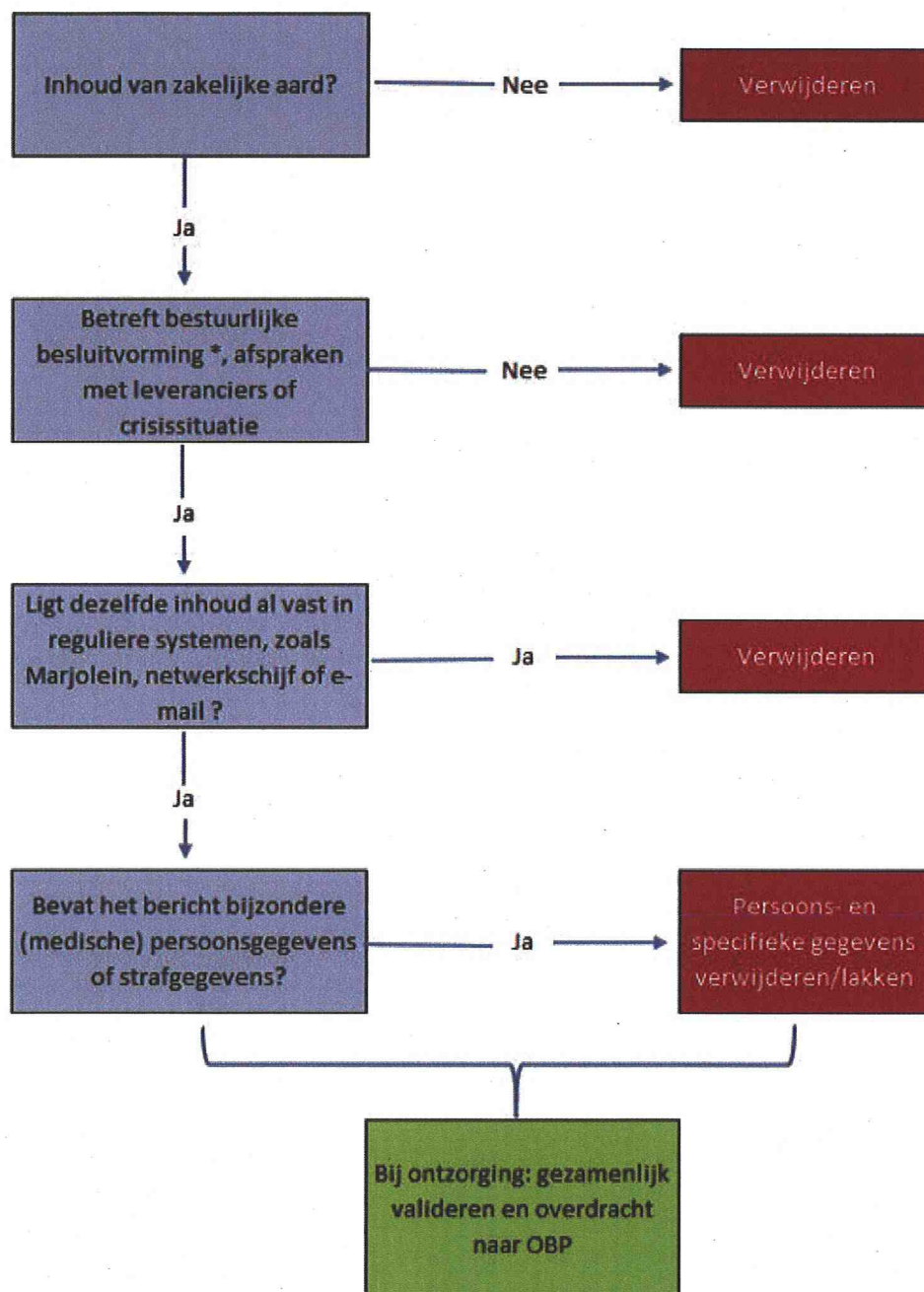
10. Proces- en beslisboom archiveren en verwijderen chatberichten

De hieronder beschreven proces- en beslisboom geldt voor alle medewerkers die relevante chatberichten hebben. Voor topambtenaren vanaf schaal 17 en de bewindslieden wordt ondersteuning aangeboden in samenwerking met Doc-Direkt.

De te bewaren berichten worden voor het kerndepartement opgeslagen in Marjolein, zo nodig in overleg met OBP/Kennisplein.

11. Pilot en evaluatie

Het beschreven proces wordt als pilot opgestart tot eind 2022. In januari wordt de evaluatie geagendeerd voor de Bestuursraad.

Proces- en beslisboom archiveren en verwijderen chatberichten VWS-kerndepartement

* Specificering van bestuurlijke besluitvorming, uit de rijksbrede Handreiking bewaren van chatberichten

3.1 Welke berichten bewaren?

Alle chatberichten die van belang zijn voor de reconstructie van bestuurlijke besluitvorming moeten worden opslagen, tenzij de inhoud van het bericht al op een andere manier is vastgelegd. Van deze chatberichten moet minimaal de volgende informatie worden bewaard:

- Het bericht met het besluit zelf;
- De berichten die duidelijk maken waarover een besluit wordt genomen;
- De berichten die duidelijk maken wat de onderbouwing is van het besluit;
- Relevante informatie die aan het besluit voorafging en die aanleiding kan zijn voor het besluit;
- De ontvanger en verzender van het bericht;
- Het tijdstip waarop het bericht is verzonden of ontvangen.

In deze handreiking wordt onder bestuurlijke besluitvorming verstaan:

Berichten die onderdeel uitmaken van (de toekomstige reconstructie) van besluitvorming in zaken/dossiers met maatschappelijke, politiek-bestuurlijke, financiële, juridische en of organisatorische consequenties die voortvloeien uit overheidshandelen.

Van: 5.1.2.e
Aan: 5.1.2.e 5.1.2.e
Onderwerp: FW: vooruitblik NC19 tweede helft 2021
Datum: donderdag 14 juli 2022 09:19:08
Bijlagen: MAIL vooruitblik NC19 tweede helft 2021.pdf
 OA proces veiligstellen COVID-19 gerelateerde chatberichten.pdf

Hoi 5.1.2.e en 5.1.2.e

Onderstaande mail vond ik nog. Daarna zijn de MT-leden schaal 14 en hoger individueel benaderd.

De mail zit ook als pdf in de bijlagen.

Verder in de bijlagen nog de Q&A die recent is opgesteld met DCo. Wrs. iets te veel al op detailniveau, maar hierbij dan alvast.

Groeten,
5.1.2.e

Van: 5.1.2.e @minvws.nl>
Verzonden: vrijdag 2 juli 2021 10:50
Aan: 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>;
 5.1.2.e @minvws.nl>; 5.1.2.e @minvws.nl>;
 5.1.2.e @minvws.nl>; 5.1.2.e @minvws.nl>;
 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>;
 5.1.2.e @minvws.nl>; 5.1.2.e @minvws.nl>;
 5.1.2.e @minvws.nl>
cc: 5.1.2.e @minvws.nl>; 5.1.2.e @minvws.nl>;
 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>; 5.1.2.e
 @minvws.nl>; 5.1.2.e @minvws.nl>
Onderwerp: vooruitblik NC19 tweede helft 2021

Beste collega's,

Voor velen van jullie start binnenkort de welverdiende zomervakantie. Voorafgaand daaraan wil ik jullie graag informeren over de werkzaamheden van NC19 voor de tweede helft van 2021 zodat jullie ook weten waarom we jullie of jullie medewerkers benaderen.

Reconstructie

Ook in de tweede helft van 2021 zal het team Reconstrueren nog volop bezig zijn met het opstellen van tijdlijnen. Het gaat dan om de tijdlijnen die betrekking hebben op het tweede tijdvak (van september 2020 t/m februari 2021) en het derde tijdvak (van maart 2021 t/m juli 2021). Op 9 juli zal overigens een nota in de BR aan de orde komen waarin we voorstellen om

ook voor de periode vanaf augustus 2021 nog een aantal tijdlijnen op te stellen. Zoals inmiddels te doen gebruikelijk zullen de medewerkers van het team Reconstrueren jullie medewerkers benaderen voor aanvullende informatie met betrekking tot deze tijdlijnen.

Evalueren

Een aantal van jullie is inmiddels benaderd door de Onderzoeksraad voor Veiligheid voor een interview. Deze interviews hebben betrekking op de periode van de start van de COVID-19 crisis t/m augustus 2020. Inmiddels heeft de Onderzoeksraad laten weten het onderzoek uit te breiden met een tweede fase (september 2020 t/m februari 2021) en mogelijk (daar is nog niet over besloten) een derde fase. Als de Onderzoeksraad ook voor de tweede (en mogelijk derde) fase informatieverzoeken voor VWS heeft, dan zal het team Evalueren jullie medewerkers benaderen om te helpen bij het verzamelen van de benodigde informatie of het goedkeuren van de door NC19 verzamelde informatie.

Daarnaast is het team Evalueren gestart met de voorbereiding op een mogelijke parlementaire enquête. Bij de voorbereiding gaat het onder andere om het ordenen van alle veiliggestelde COVID-19 informatie. Op dit moment bedraagt de dataset ruim 13 miljoen documenten (waarvan circa 5,4 miljoen unieke documenten). En die dataset groeit nog steeds. Om die dataset te ordenen, gaat NC19 een zogeheten digitale referentiestructuur (een soort inhoudsopgave) bouwen. De basis voor die referentiestructuur zijn de hiervoor genoemde tijdlijnen. Om een handige referentiestructuur te bouwen hebben we ook jullie hulp nodig! Allereerst hebben we in aanvulling op de tijdlijnen inzicht in "kwetsbare momenten" nodig. Met kwetsbaar bedoelen we onder andere dat als VWS destijds de kennis van nu had gehad, VWS dan wellicht een andere besluit zou hebben genomen. In de tijdlijnen staan nu voornamelijk "kantelmomenten" centraal (i.e. momenten die cruciaal waren in de ontwikkeling en de bestrijding van de COVID-19 crisis). Voor het inventariseren van de "kwetsbare momenten" zullen jullie een uitnodiging voor een gesprek ontvangen. Daarnaast willen we graag zowel de concept-referentiestructuur als de concept-zoektermen die nodig zijn om relevante informatie naar boven te halen, ter toetsing aan jullie medewerkers voorleggen. Immers: een goede referentiestructuur bevordert later het snel zoeken naar informatie ten behoeve van de beantwoording van invorderingsverzoeken van de Tweede Kamer bij een parlementaire enquête.

Veiligstellen van email en documenten

Zoals jullie weten heeft de Bestuursraad in april ingestemd met het automatisch veiligstellen van e-mails en documenten bij jullie directies zodat jullie op dit punt ontzorgd worden. Om te voorkomen dat p-vertrouwelijke of privacy vertrouwelijke informatie automatisch wordt opgehaald is in samenwerking met de adviseurs van OBP een richtlijn uitgewerkt om deze informatie in afzonderlijke mappen op te slaan. Het team OBP-Informatieverzoeken zal voorafgaand aan het veiligstellen van email/documenten met jullie directies een gesprek voeren zodat duidelijk wordt waar de informatie staat die buiten beschouwing moet worden gelaten.

Veiligstellen chatverkeer mobiele telefoons

De Bestuursraad heeft in april 2021 besloten dat van alle MT-leden en hoger de zakelijke, besluitvormende én corona-gerelateerde chatberichten veiliggesteld moeten worden. Een nieuw team is hiermee aan de slag. De doelstelling is om voor november dit jaar van iedereen die daar toestemming voor geeft de mobiele één keer uitgelezen te hebben. We liggen op koers om dit voor elkaar te krijgen. Een aantal van jullie zit nog in het proces en een aantal van jullie heeft dit proces al minimaal één keer doorlopen.

Zouden jullie deze e-mail in jullie directie willen verspreiden?

Een goed weekend alvast.

Groet, 5.1.2.e

5.1.2.e

5.1.2.e

Ministerie van Volksgezondheid, Welzijn en Sport

Mobiel: 06 5.1.2.e

E-mail: 5.1.2.e@minvws.nl

Q&A proces veiligstellen COVID-19 gerelateerde chatberichten

Waarom worden er bij VWS COVID-19 gerelateerde chatgesprekken uitgelezen?

Het adequaat veiligstellen, doorzoekbaar maken en ter beschikking kunnen stellen van COVID-19 gerelateerde informatie kan onderdeel zijn van meerdere wettelijke verplichtingen (Woo, Archiefwet, Wet op de Parlementaire Enquête et cetera). Voor de Wob (inmiddels Woo) en Archiefwet is op 20 maart 2019 door de Raad van State vastgesteld dat chatberichten die bij het uitvoeren van overheidstaken zijn geproduceerd, moeten worden veiliggesteld. Als overheidsorgaan moet het ministerie van Volksgezondheid, Welzijn en Sport er dan ook zorg voor dragen dat deze informatie niet verloren gaat. Dit vormt de grondslag voor het uitlezen van chatgesprekken. Een chatgesprek is een gesprek tussen twee of meerdere personen, welke komen uit applicaties zoals bijvoorbeeld WhatsApp, iMessage en SMS.

Van wie worden er precies chatgesprekken met daarin COVID-19 gerelateerde informatie uitgelezen?

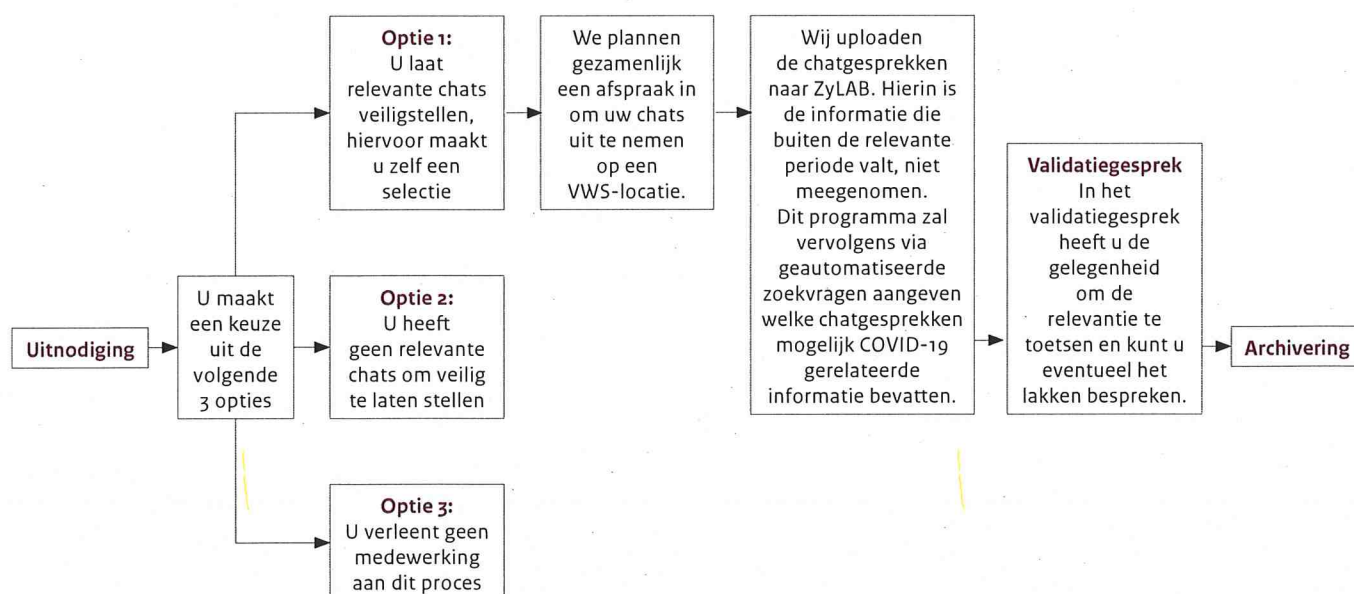
De chatgesprekken worden uitgelezen van iedere VWS Kern medewerker in een functie van MT-lid of hoger.

Ben ik verplicht om mee te werken, wanneer ik een uitnodiging voor het proces ontvang?

Nee, het niet meewerken aan het proces rond het veiligstellen en archiveren van chats heeft geen arbeidsrechtelijke consequenties. Wel kan het voorkomen dat u later alsnog gevraagd wordt om chatberichten vrij te geven, bijvoorbeeld in het kader van een onderzoek, Woo-verzoek of parlementaire enquête, en kan het zo zijn dat andere partijen chats met u vrijgeven. Het is belangrijk om u hiervan bewust te zijn.

Hoe verloopt het proces van chats uitlezen?

In de afbeelding hieronder vindt u een visuele representatie van het proces rondom het uitlezen van chats.



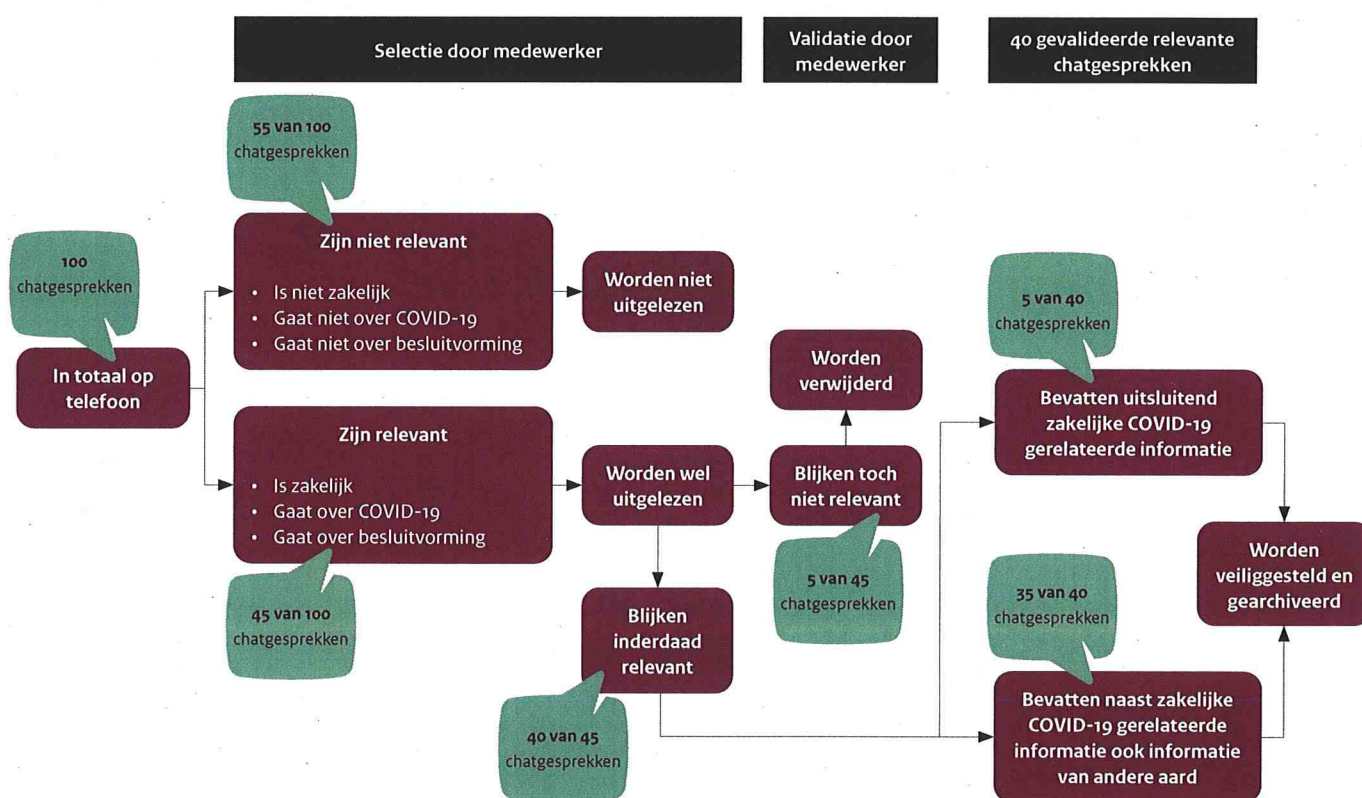
Wat kan ik aanmerken als relevante chatberichten?

Chatberichten zijn relevant als zij aan alle onderstaande criteria voldoen:

- Zakelijk
- COVID-19 gerelateerd
- Besluitvormend. Hieronder wordt verstaan:
 - Het bericht met het besluit zelf;
 - De berichten die duidelijk maken waarover een besluit wordt genomen;
 - De berichten die duidelijk maken wat de onderbouwing is van het besluit;
 - Relevante informatie die aan het besluit voorafging en die aanleiding geweest kan zijn voor het besluit.

Het gaat hierbij enkel om relevante chatberichten tussen 1 december 2019 tot en met 23 maart 2022, of de periode tussen de in- en/of uitdiensttreding van de huidige functie. In de onderstaande afbeelding ziet u hoe u een selectie van uw chats kunt maken.

Hoe maak ik een selectie van mijn chatgesprekken?



Kan het team dat de chatgesprekken uitleest een inschatting maken van relevante chats?

Vanwege de privacygevoeligheid, maakt het team dat de chatgesprekken uitleest zo min mogelijk inschattingen betreffende de inhoud van chatgesprekken. Op deze manier hoeven zij zo min mogelijk met datahouders mee te lezen. Het is dus belangrijk dat u zelf aangeeft welke chats relevante informatie bevatten. Wel kunnen de chats nogmaals bekeken worden na het uitnemen, met ondersteuning van het team Veiligstellen & Archiveren. Ook maakt het team gebruik van een geautomatiseerde zoekvraag op het moment dat de chats zijn uitgenomen, waardoor er een indicatie geboden kan worden van de verwachte relevantie van chats op het moment dat u hierover twijfelt. Dit betekent dat er in de tekst wordt gezocht naar COVID-19 gerelateerde termen. Ook wordt een soortgelijke zoekvraag toegepast op de bijlagen, waardoor de software ook hierin COVID-19 gerelateerde termen kan herkennen. Als er COVID-19 gerelateerde informatie naar voren is gekomen, wordt het chatgesprek en/of bijlage gemarkeerd als 'relevant' en anders als 'niet relevant'. U kunt de uitkomst van deze zoekvragen gebruiken bij het bepalen van de definitieve relevantie. Zo kunt u ook beslissen om de uitkomst van de zoekvragen aan te houden, wanneer het gaat om de relevantie. Uiteindelijk bepaalt u echter of iets als relevant kan worden aangemerkt.