Bewaren van chatberichten

Handreiking voor de Rijksoverheid

2022 - Versie 2.0

Rijksprogramma
Duurzaam
Digitale
Informatiehuishouding

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
25 juli 2022	Tekst over 'niet automatisch wissen' toegevoegd

Inhoud

Wijzigingshistorie 2

1 **Inleiding** 4
Aanleiding 4
Doel 4
Scope 4
Opbouw 5

2 **Kaders voor berichtenapps** 6
2.1 Juridisch kader 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 State[1] 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 Rijksoverheid[3] 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	Beschijving 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.

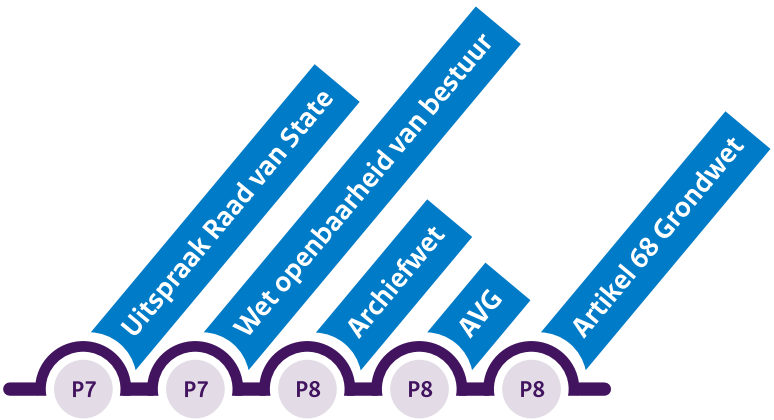
Samengevat geldt het volgende kader:

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.
Dringend advies	Het wordt **dringend geadviseerd** om de functie geautomatiseerde verwijdering, die in diverse chatapps kan worden ingesteld, **niet** te activeren.
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 vervolgprocedures, 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 selectielijsten[7] 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 Assesment 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 bewindspersoon 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 geschift. Archiefwaardige berichten worden handmatig geëxporteerd en veiliggesteld.

Technische exportinstructie

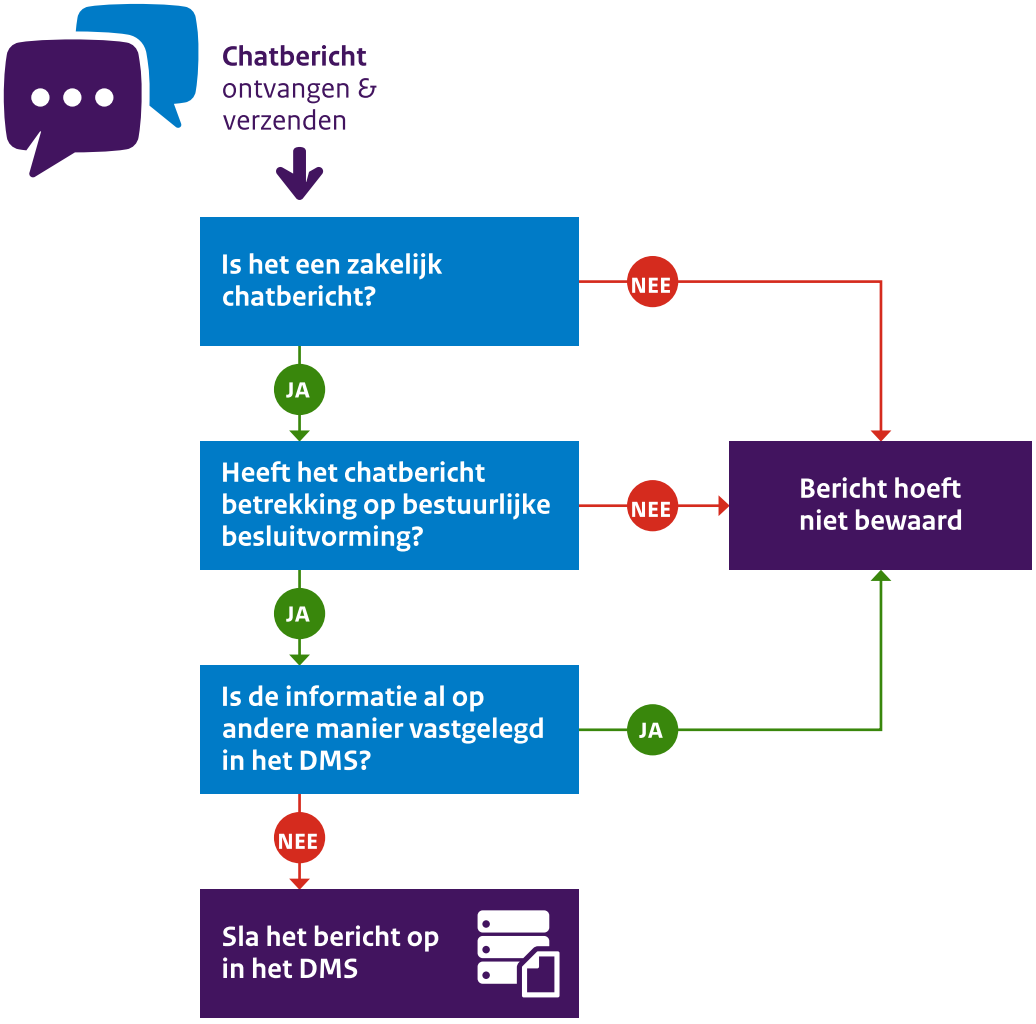
Op 3 juli is door RDDI en het ministerie BZK (CIO Rijk) aan het SG-overleg een technische handleiding opgeleverd voor het (handmatig) exporteren van chatberichten bij de Rijksoverheid. De instructie beschrijft hoe chatberichten veiliggesteld kunnen worden en ondersteunt gebruikers bij het exporteren 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.
- Zoals hiervoor in Hoofdstuk 2 aangegeven, wordt **dringend geadviseerd** om de functie geautomatiseerde verwijdering, die in diverse chatapps kan worden ingesteld, **niet** te activeren.

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



8 Bestuurlijk 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:

Welke berichten bewaren? 3.1
Wiens berichten bewaren? 3.2
Wie bewaart? 3.3
Hoe bewaren? 3.4
Waar bewaren? 3.5
Wanneer bewaren? 3.6
Verwijderen? 3.7

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 anderen[10] 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 werkt[11].

Het *Informatieblad archiveren chatberichten* van het Nationaal Archief biedt meer informatie over de verschillende werkwijzen en methoden[12] 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 bijlages 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 gegevenseigenaar 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 vervolgprocedures, 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 afhankelijke 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 doelgroepen[13].

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***	*Het omzetten van het chatbericht naar een ander formaat en/of het uitsplitsen van chatberichten om ze over te brengen naar verschillende dossiers*
5 **Registreren**	Het autoriseren van de geëxorteerde informatie door de gegevens-verantwoordelijke en vastleggen van de juiste metadatagegevens, 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 bewaren[14] 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 keuzes[15] 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 context-gegevens 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

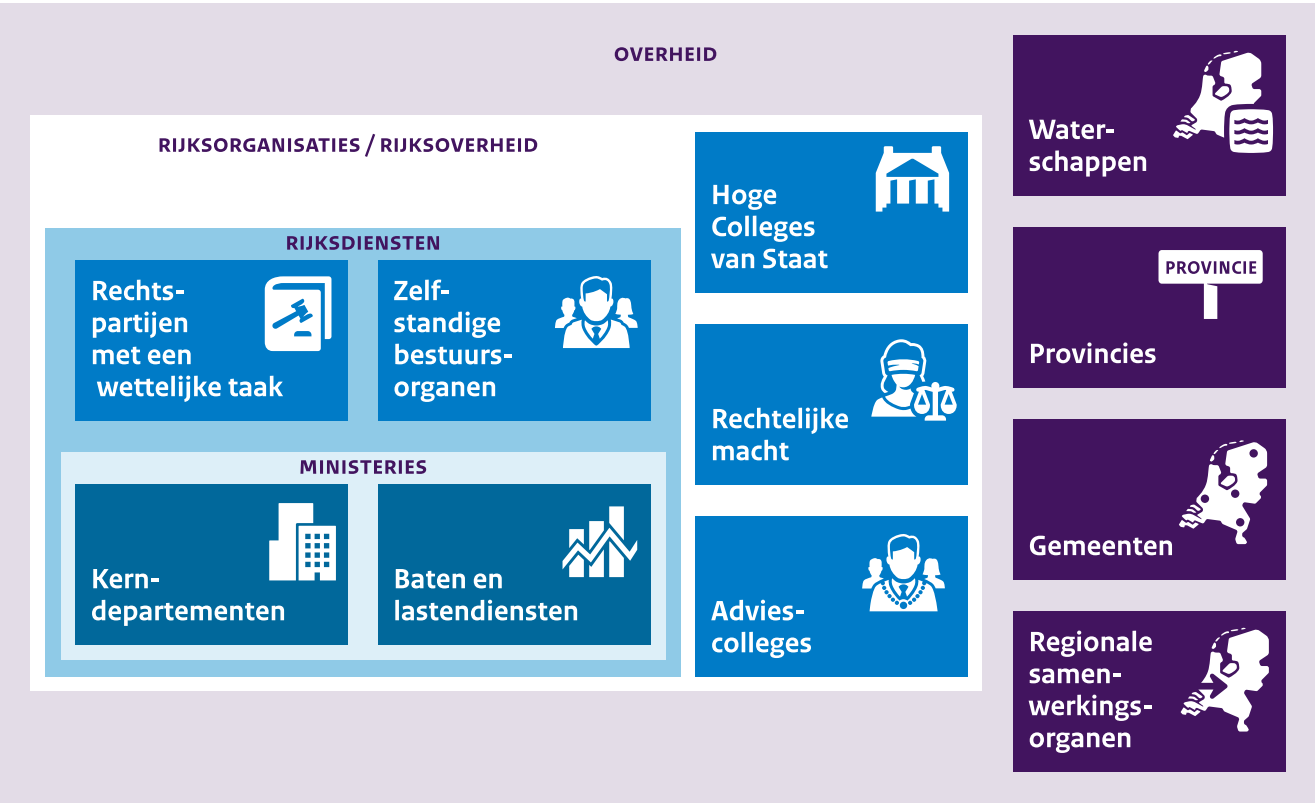
De handreiking is specifiek bedoeld voor adviseurs binnen de Rijksoverheid die verantwoordelijk zijn voor (het organiseren van) het bewaren van chatberichten en/of betrokken zijn bij de behandeling van Wob-verzoeken zoals documentaire informatieadviseurs, informatiemanagers en -beheerders, auditors, 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 onvercijferde 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 integriteits-onderzoeken 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 *Telemessage* 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).

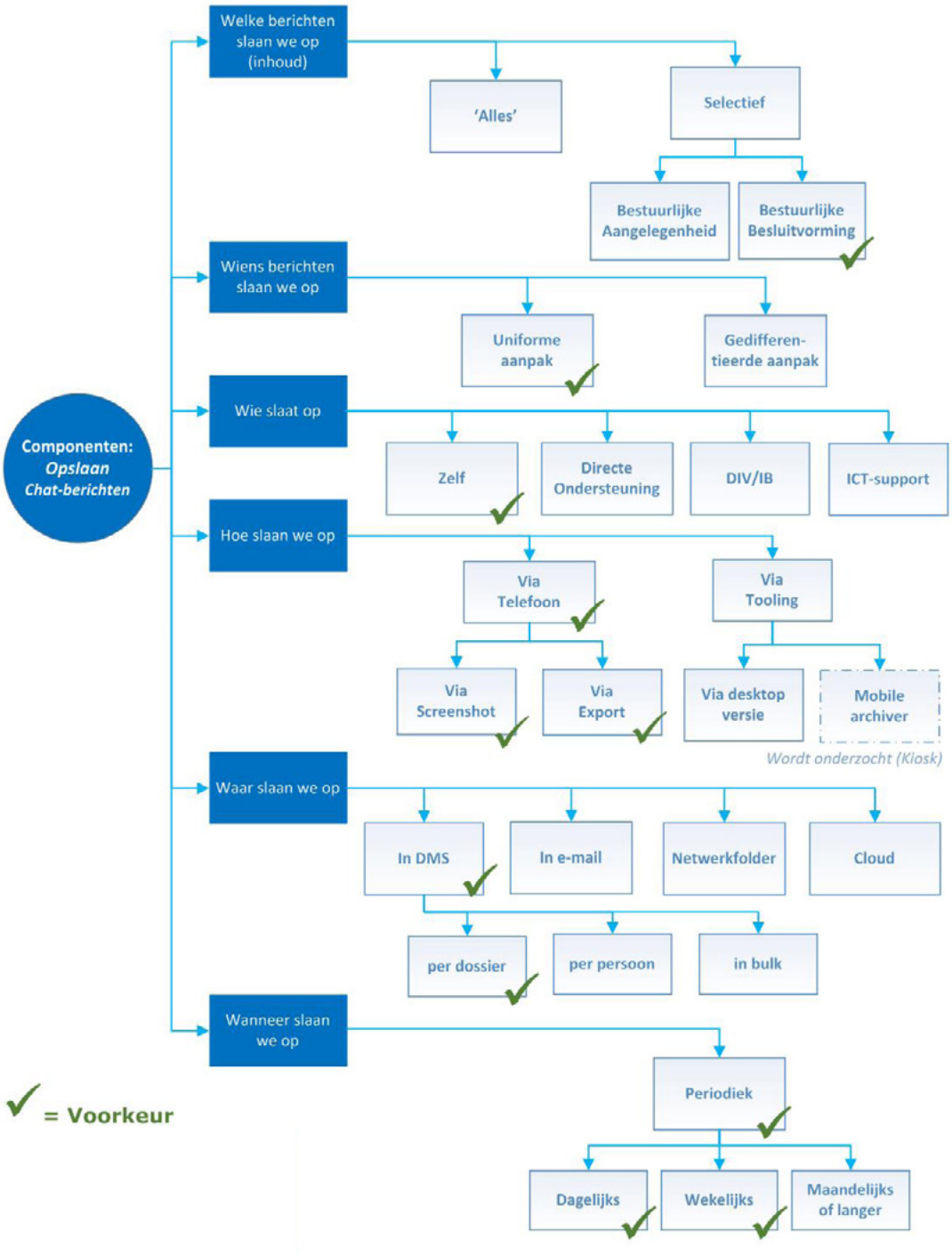
Ter illustratie

- 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 (KamerstukkenII 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" (KamerstukkenII 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 bestemdvoor 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 privacyrechtelijke 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)

Juli 2022