



## 1. Waarover gaat dit informatieblad?

Dit informatieblad geeft voorlichting over de archivering van chatberichten in berichtenapps. Het geeft een analyse van chatberichten als vorm van informatie en gaat in op verschillende aspecten zoals wettelijke plichten, technische mogelijkheden en privacy. Verder geeft het overwegingen die helpen bij het bepalen van een archiveringsstrategie.

## 2. Waarom gebruik je dit informatieblad?

Dit informatieblad is bedoeld om overheidsorganisaties informatie (in de vorm van een afwegingskader) te geven die hen helpt op tactisch niveau zelf keuzes en beleid te maken omtrent het archiveren van chatberichten in berichtenapps.

Dit vraagstuk is meer relevant geworden sinds de [uitspraak van de Raad van State van 20 maart 2019](#) dat *“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”*.

\*Uitgangspunt voor dit informatieblad is de *as is* situatie dat berichtenapps gebruikt worden in het kader van het werk, en een archiveringsstrategie daarom nodig is.

Het is nuttig dat overheidsorganisaties ook beleid opstellen over het gebruik van berichtenapps in algemene zin: in hoeverre, welke, en hoe, mogen berichtenapps gebruikt worden in de organisatie. In dit informatieblad wordt daar verder niet op ingegaan. De overwegingen in dit informatieblad kunnen mogelijk wel helpen een dergelijk beleid op te stellen.

## 3. Voor wie is dit informatieblad bedoeld?

- Adviseurs bij overheidsorganisaties die verantwoordelijk zijn voor (het organiseren van) de archivering van chatberichten. Voorbeelden van deze adviseurs zijn documentaire informatieadviseurs, informatiemanagers en -beheerders, proces- of informatieanalisten, en adviseurs digitale archivering.
- Projectleiders die de opdracht voor het archiveren van chatberichten uitvoeren.
- Managers die verantwoordelijk zijn voor de informatie in werkprocessen en de bijbehorende informatiesystemen. Zij nemen de besluiten over de eisen en ontwerpen en zien er op toe dat deze besluiten worden uitgevoerd. Bijvoorbeeld de directeur bedrijfsvoering of CIO. Managers zullen dit informatieblad niet zelf gebruiken, maar kunnen wel de opdracht geven het toe te passen.

## 4. Waardering en selectie chatberichten

### 4.1. Chatberichten en de Archiefwet

[Overheidsinformatie](#) is alle vastgelegde informatie die de overheid ontvangt, verwerkt of maakt bij het uitvoeren van haar taken en de Archiefwet schrijft voor dat die informatie gearchiveerd wordt.

Omdat het gaat over overheidsinformatie ongeacht de vorm, vallen chatberichten hier ook onder wanneer ze gebruikt worden voor het uitvoeren van overheidstaken. Net zoals dat chatberichten documenten in de zin van de Wob zijn.

### 4.2. Selectiekeuzes chatberichten verantwoord

Overheidsorganisaties maken in samenspraak met het Nationaal Archief (bij decentrale overheden: hun archivaris) keuzes over welke informatie hoe lang te bewaren. Daarbij dienen ze rekening te houden met de Archiefwet en verschillende [belangen](#) waarvoor informatie gearchiveerd wordt. En ze moeten verantwoording kunnen afleggen over hun keuzes via een kenbaar selectiebesluit.

Een verantwoorde waardering van informatie in chatberichten maken en vastleggen in een kenbaar selectiebesluit kan via onderstaande mogelijkheden:

#### 4.2.1. Bewaartermijnen selectielijst

De eerste optie is het volgen van de bewaartermijnen voor informatie zoals die vastgelegd zijn in de bestaande [selectielijst](#) van de organisatie. Daar komen verschillende knelpunten bij naar boven.

Omdat selectielijsten uitgaan van het waarderen van informatie op werkprocesniveau is het vaak moeilijk ze te vertalen naar het selecteren van specifieke informatie in alle applicaties die een organisatie gebruikt.

Een serie chatberichten is vaak ook moeilijk te vatten in een reguliere selectielijst. Omdat de inhoud over verschillende werkprocessen kan gaan, met verschillende bewaartermijnen.

Daarbij komt dat chatberichten vaak helemaal niet zijn te koppelen aan werkprocessen. Omdat ze vaak over niet-zakelijke onderwerpen gaan. Daarom kan het van belang zijn om te bekijken of microselectie mogelijk is. Dat kan bijvoorbeeld door aanvullende hulpmiddelen te bieden om chatberichten te identificeren die niet gearchiveerd hoeven te worden. Bijvoorbeeld vragen als:

- Zou de informatie in dit bericht behalve bij mijzelf ook bij anderen binnen het team/ de afdeling /de organisatie bekend zou moeten zijn?
- Zou de informatie op termijn een rol kunnen spelen bij publieke verantwoording (parlement en Wob) of in rechtszaken?

#### 4.2.2. Sleutelfunctionaris methodiek

In plaats van de bestaande selectielijst als uitgangspunt te nemen, is het mogelijk een aanvullend selectiebesluit te nemen en daarbij te kiezen voor de sleutelfunctionaris methodiek die bij e-mailarchivering voor de Rijksoverheid is voorgenomen.

Deze methodiek is gebaseerd op de capstone methodiek van de Amerikaanse NARA (National Archives and Records Administration). De term 'capstone'

(=deksteen) slaat op het uitgangspunt van deze methodiek: enkel de e-mails van de top van een organisatie worden permanent bewaard. Deze topambtenaren worden zodoende 'capstone officials' (sleutelfunctionarissen) genoemd. De e-mail van niet-sleutelfunctionarissen wordt na een bepaalde termijn (bijv. 10 jaar) vernietigd.

De sleutelfunctionaris methodiek past binnen de bredere waarderingsmethodiek van het Nationaal Archief die de [systeemanalyse](#) heet. In dat kader wordt gesteld dat mailboxen van sleutelfunctionarissen belangrijke informatieknoppunten zijn. Zie voor meer informatie het rapport "[Selectie van sleutelfunctionarissen](#)" op KIA.

Net als voor e-mail zou voor chatberichten een optie zijn om te bepalen dat chatberichten van sleutelfunctionarissen blijvend bewaard worden. Die keuze moet dan wel verantwoord worden in de selectielijst van de betreffende organisatie.

Voor e-mail is het voornemen om deze veilig te stellen via een geautomatiseerde bulkoplossing. Ook dat zou een mogelijkheid zijn bij chatberichten, door deze bijvoorbeeld via de technische oplossing van het uitlezen geautomatiseerd veilig te stellen (zie paragraaf 6.3).

Ook bij toepassing van de sleutelfunctionaris methodiek is het raadzaam te onderzoeken hoe niet-zakelijke berichten kunnen worden uitgezonderd van veiligstelling.

#### **4.2.3. Hotspots**

[Een hotspotmonitor](#) is een methode waarmee periodiek 'hotspots' geïdentificeerd worden: gebeurtenissen die leiden tot opvallende of intensieve interactie tussen overheid en burgers of tussen burgers onderling, en die veel maatschappelijke beroering veroorzaken. De hotspotmonitor wijst informatieobjecten aan die betrekking hebben op zulke hotspots, en selecteert ze voor blijvende bewaring.

Het kan zijn dat in het kader van een hotspot chatberichten worden bewaard, of dat de organisatie zelfs bij gebeurtenissen die potentieel een hotspot kunnen worden preventief informatie – ook in chatberichten – wil veiligstellen.

#### **4.3. Overwegingen selectiekeuzes**

De sleutelfunctionaris methodiek en de hotspotmonitor kunnen naast de bestaande selectielijst worden toegepast.

De bestaande selectielijst biedt handvatten om chatberichten die duidelijk zijn te koppelen aan een bepaald werkproces binnen die context (in een DMS/RMA) te archiveren. Chatberichten kunnen ook als afzonderlijke informatiestroom worden gearchiveerd. Dan komt de sleutelfunctionaris methodiek aan bod. Daarbij is de functie van de medewerker bepalend wat hoe lang wordt bewaard.

In beide gevallen kan de hotspotmonitor worden toegepast. Dat betekent dat chatberichten die normaal op termijn zouden worden vernietigd, alsnog permanent bewaard blijven.

Bij toepassing van de sleutelfunctionarismethodiek betekent toepassing van de hotspotmonitor dat sommige chatberichten van niet-sleutelfunctionarissen alsnog blijvend worden bewaard.

Op basis van de doelstellingen en systematiek van de Archiefwet, en de zich ontwikkelende praktijk, zouden overheidsorganisaties voor chatberichten een *risicobenadering* kunnen volgen:

- in beeld brengen hoe de organisatie en verschillende groepen daarbinnen berichtenapps gebruiken, en welke bewaarbelangen gemoeid zijn met de informatie

- in beeld brengen hoe groot de risico's zijn dat informatie in chatberichten niet meer of slechts met moeite te achterhalen is;
- passende en proportionele organisatorische en/of technische maatregelen treffen om de getaxeerde risico's te ondervangen; wat passend en proportioneel is hangt mede af van de inrichting van de totale informatiehuishouding;
- over de genomen maatregelen verantwoording afleggen in de selectielijst en/of andere bij voorkeur publiek kenbare documenten of besluiten.

## 5. Analyse chatberichten en berichtenapps

### 5.1. Definitie chatberichten en berichtenapps

*Chatberichten* zijn alle berichten, ongeacht hun vorm (tekst, audio, video, bijlagen of hyperlinks) die verzonden worden via een berichtenapp.

*Berichtenapps* zijn besloten kanalen voor het uitwisselen van chatberichten tussen individuen of kleine groepen die voornamelijk gebruikt worden via apps op smartphones (hoewel soms desktop versies mogelijk zijn)

Er is een grote verscheidenheid aan berichtenapps die op verschillende manieren gebruikt worden door overheidsorganisaties voor het versturen en ontvangen van chatberichten. Hieronder een niet-uitputtende opsomming van veel gebruikte berichtenapps:

- SMS
- WhatsApp
- Signal
- Facebook Messenger
- Threema
- iMessage
- WeChat
- Telegram

Er is ook onderscheid te maken naar hoe berichtenapps ingezet worden, en naar het soort informatie dat uitgewisseld wordt:

### 5.2. Gebruik als functionele berichtenboxen (postbus)

Bij functionele berichtenboxen worden chatberichten via een berichtenapp verzonden en ontvangen vanuit naam van een functie/organisatie, in plaats van vanuit een individueel persoon.

Het doel is service verlenen of gerichte informatie geven, zoals inhoudelijke vragen van burgers beantwoorden op een vergelijkbare manier als vanuit een postbus emailaccount.

Voorbeeld hiervan:

- Gemeenten die via een algemeen telefoonnummer met WhatsApp specifieke vragen van burgers beantwoorden tijdens kantoortijden

### 5.3. Gebruik individueel functioneel

Bij individueel functioneel gebruik worden chatberichten via een berichtenapp verzonden en ontvangen door individuele personen, soms in besloten groepen. Het doel is informatie uitwisseling en communicatie uit eigen naam maar gekoppeld aan het uitvoeren van overheidstaken. Op een vergelijkbare manier als gebruik van individuele emails. Voorbeeld hiervan:

- Ambtenaren die overleg plegen over de voorbereiding of uitvoering van beleid.

De intensiteit van het gebruik en het soort informatie dat uitgewisseld wordt kan erg verschillen afhankelijk van de rol van de ambtenaar: In sommige functies gebruiken ambtenaren voornamelijk email voor laagdrempelige informatie-uitwisseling en besluitvorming en zijn berichtenapps alleen aanvullend. In andere functies vindt informatie-uitwisseling en besluitvorming meer via berichtenapps plaats vanwege de laagdrempeligheid en snelheid van het medium.

### 5.4. Informatieobjecten binnen berichtenapps

Via berichtenapps worden verschillende informatieobjecten uitgewisseld. Vanuit het oogpunt van archivering zijn niet alleen de inhoudelijke chatberichten relevant, maar ook de metadata die belangrijke contextinformatie verschaft. Hieronder een niet uitputtende opsomming van het soort informatieobjecten die omgaan in berichtenapps:

#### **Inhoud chatberichten:**

- Tekstberichten (chatbericht)
- Emoticons in chatberichten
- Foto's
- Video's
- Tekstbestand als bijlage
- Audioberichten
- Links naar externe websites
- Live locatiebepalingen

#### **Metadata chatberichten:**

- Afzender chatbericht
- Ontvanger chatbericht
- Overzicht deelnemers groepsapp
- Datum en tijdstip verzenden bericht
- Ontvangstbevestiging bericht op device
- Leesbevestiging bericht
- Base64 encoded thumbnail bij afbeeldingen (specifiek bij WhatsApp)
- Profiel foto gebruiker

## 6.4 Overwegingen voor archiveringsstrategie chatberichten vanuit oogpunt van gebruik berichtenapps

Voor een verantwoorde archiveringsstrategie van chatberichten is het nuttig om inzicht te hebben in hoe berichtenapps gebruikt worden in de organisatie:

- Worden berichtenapps voornamelijk gebruikt als de postbus variant, of door individuele ambtenaren om werkgerelateerde chatberichten te versturen?
- Is bij functioneel individueel gebruik verschil in groepen en rollen van medewerkers in de organisatie voor wat betreft het soort informatie dat gedeeld wordt en de intensiteit van het gebruik van berichtenapps?
- Wordt er vertrouwelijke of gerubriceerde informatie gedeeld in berichtenapps?
- Welke informatieobjecten binnen berichtenapps zijn essentieel om veilig te stellen?

## 6. Archiveringsmogelijkheden chatberichten

Momenteel bestaan er een aantal mogelijkheden om chatberichten te archiveren. Deze mogelijkheden gaan uit van het veiligstellen van chatberichten door ze te *verplaatsen* van de berichtenapp naar een door de organisatie beheerde omgeving. Zodat in de beheerde omgeving de duurzame toegankelijkheid van de chatberichten geborgd kan worden.

De reden dat deze archiveringsmogelijkheden allemaal uitgaan van verplaatsen is omdat momenteel nog geen best practices bekend zijn die [archivering by design](#) in de berichtenapp zelf (het werksysteem) mogelijk maken. Een complicatie daarbij is ook dat berichtenapps vaak niet eigendom zijn van de overheid en het daarom niet mogelijk is om ontwerp- en beheerkeuzes te maken omtrent de berichtenapps zelf.

De onderstaande archiveringmogelijkheden zijn erop gericht om informatie in chatberichten veilig te stellen en duurzaam toegankelijk te houden. Met [duurzame toegankelijkheid](#) wordt hier bedoeld dat informatie – voor zolang als nodig- aan de volgende criteria voldoet:

- **Vindbaar.** De gebruiker kan snel en eenvoudig relevante informatie vinden tussen alle bewaarde informatie. Bij voorkeur op één plaats en met de gebruikelijke zoekfuncties.
- **Beschikbaar.** De gebruiker kan informatie snel en eenvoudig verkrijgen. Bij voorkeur op elk tijdstip, vanaf elke plaats en zonder kosten.
- **Leesbaar.** De gebruiker kan de informatie bekijken en verwerken. Bij voorkeur vanaf zijn eigen werkplek zonder daarvoor speciale applicaties te moeten installeren.
- **Interpreteerbaar.** Het is voor de gebruiker duidelijk wat de betekenis van de informatie was binnen het werkproces waar het is ontvangen of gemaakt. Het is bijvoorbeeld bekend wanneer de informatie is gemaakt, door wie, waar het betrekking op heeft en wat de status is.
- **Betrouwbaar.** De gebruiker kan er op vertrouwen dat de informatie volledig en correct is. Bijvoorbeeld dat de informatie daadwerkelijk opgeslagen is op

het moment en door de persoon zoals aangegeven, en dat er daarna niets in is gewijzigd of verwijderd.

## **6.1. Afwegingskader duurzame toegankelijkheid chatberichten**

Iedere archiveringsmogelijkheid voor chatberichten heeft andere voor- en nadelen qua duurzame toegankelijkheid. Ook is er verschil in welke informatieobjecten veiliggesteld worden.

Overheidsorganisaties maken hun eigen keuzes over welke eisen ze stellen aan de duurzame toegankelijkheid van informatie in chatberichten. Dat zal immers afhankelijk zijn van *door wie, hoe, waarvoor*, berichtenapps gebruikt worden in de organisatie.

Zo kan mogelijk aan informatie in chatberichten met een hoog-risicoprofiel, zoals behorende bij hotspots of sleutelfunctionarissen, hogere eisen gesteld worden op het vlak van duurzame toegankelijkheid.

Ook kunnen de kaders vanuit privacy en uitvoerbaarheid aanleiding geven om voor een bepaald archiveringsmogelijkheid te kiezen.

Hieronder wordt per archiveringsmogelijkheid een overzicht gegeven van het soort informatieobjecten die veiliggesteld worden, en de voor- en nadelen van de archiveringsmogelijkheid vanuit het oogpunt van duurzame toegankelijkheid.

### **6.1.1. Handmatig selecteren en exporteren chatberichten via screenshot naar DMS of andere beheerde omgeving**

Met behulp van de standaard functionaliteit op de telefoon een screenshot maken van een of meerdere bericht(en) en de data doorsturen naar de email om al dan niet vervolgens op te slaan in DMS.

#### **Toelichting resultaat screenshot**

Een screenshot kan alleen van (meerdere) individuele chatberichten gemaakt worden. Een gehele conversatie binnen een berichtenapp vastleggen zou een groot aantal screenshots vergen.

Het resultaat van de screenshot is een statische afbeelding in JPEG of PNG bestand die vastlegt wat de gebruiker van de berichtenapp op het device ziet.

Een overweging bij de screenshot oplossing is dat er verschil is tussen berichtenapps. Zo heeft Telegram een optie voor extra beveiliging die indien 'aan' gezet door de gebruiker, het maken van een screenshot onmogelijk maakt.

Met een screenshot worden de volgende informatieobjecten en metadata vastgelegd:

<b>Informatieobject of metadata</b>	<b>Onderdeel screenshot?</b>
Tekstberichten	Ja. Afhankelijk van de gekozen selectie van berichten voor het maken van de screenshot.
Emoticons in tekstberichten	Ja
Foto's	Ja. Afhankelijk van de gekozen selectie

	van berichten voor het maken van de screenshot.
Video's	Nee, alleen statische afbeelding van het videobericht, niet de dynamische videocontent
Tekstbestand als bijlage	Nee. Bij een screenshot is alleen te zien dat een bijlage is verzonden en is daar een klein deel van zichtbaar. De bijlage als geheel is een apart bestand.
Links naar externe websites	Ja, maar link is niet doorklikbaar omdat de screenshot een statische afbeelding is
Live locatiebepalingen	Nee. Bij een screenshot is alleen te zien dat een live locatiebepaling gedeeld is.
Afzender chatbericht	Deels. Berichtenapps tonen in chatgesprekken alleen de naam van de gesprekspartner, niet de naam van gebruiker van de berichtenapp. Een screenshot toont daarom nooit op zichzelf de gebruiker zelf aan als afzender.
Ontvanger chatbericht	Deels. Berichtenapps tonen in chatgesprekken alleen de naam van de gesprekspartner, niet de naam van gebruiker van de berichtenapp. Een screenshot toont daarom nooit op zichzelf de gebruiker zelf aan als ontvanger.
Overzicht deelnemers groepsapp	Nee. Bij berichtenapps met de mogelijkheid tot groepsapps zoals WhatsApp en Facebook Messenger is het niet mogelijk de lijst met deelnemers samen met de naam van de groepsapp op één screenshot te krijgen.
Datum en tijdstip verzenden bericht	Afhankelijk van berichtenapp. Bij WhatsApp wordt binnen het chatgesprek alleen het tijdstip van versturen berichten getoond. Bij Signal en iMessage wordt zowel de datum als tijdstip onder ieder bericht vastgelegd en is daarmee in een screenshot ook zichtbaar.
Ontvangstbevestiging bericht op device	Afhankelijk van berichtenapp. Bij WhatsApp is het mogelijk de ontvangstbevestiging bij een individueel bericht binnen het chatgesprek te zien en daarmee in een screenshot vast te leggen.



Leesbevestiging bericht	Afhankelijk van berichtenapp. Bij WhatsApp is het mogelijk de leesbevestiging (blauwe vinkjes) bij een individueel bericht binnen het chatgesprek te zien en daarmee in een screenshot vast te leggen.
Base64 encoded thumbnail bij afbeeldingen (specifiek bij WhatsApp)	Nee
Profielfoto gebruiker	Ja, mogelijk als verkleinde representatie binnen een screenshot of als aparte screenshot

### 6.1.2. Duurzame toegankelijkheid *screenshot*

<b>Vindbaar</b>	<p><b>Plus:</b> Met een screenshot kan een selectie van berichten gemaakt worden die aan een dossier en daarmee orderingsstructuur van bijvoorbeeld een DMS te koppelen zijn.</p> <p><b>Min:</b> Met screenshots is het veel werk een volledig chatgesprek vast te leggen.</p> <p><b>Min:</b> Niet alle informatieobjecten en metadata zijn vindbaar. Datum en tijdstip en naam gebruiker ontbreekt.</p> <p><b>Min:</b> Er kan niet fulltext gezocht worden op de inhoud van het gesprek. Om de vindbaarheid te bevorderen is goede (additionele) metadatering van de context nodig.</p>
<b>Beschikbaar</b>	<p><b>Plus:</b> Via een screenshot kunnen een of meerdere berichten geëxporteerd worden naar een beheeromgeving buiten het device van de gebruiker waar de berichten beschikbaar zijn voor derden</p> <p><b>Min:</b> Niet alle informatieobjecten en metadata zijn beschikbaar. Datum en tijdstip en naam gebruiker als verzender/afzender ontbreekt.</p>
<b>Leesbaar</b>	<p><b>Plus:</b> Het resultaat van de screenshot als JPG of PNG open standaard bestandsformaten. Waarbij PNG ook een voorkeursformaat van het Nationaal Archief is.</p>
<b>Interpreteerbaar</b>	<p><b>Plus:</b> Omdat de screenshot een deel van het chatgesprek vastlegt zoals de gebruiker het zelf ziet is de look &amp; feel hetzelfde als in de live omgeving.</p> <p><b>Min:</b> Contextinformatie mist omdat het resultaat onvolledig is en</p>

	<p>bijvoorbeeld metadata rond naam en datum van verzenden/ontvangen berichten is afhankelijk van de berichtenapp.</p> <p>Contextinformatie mist ook omdat het selecteren van berichten voor vastlegging met een screenshot en handmatige en subjectieve keuze is.</p>
<p><b>Betrouwbaar</b></p>	<p><b>Plus:</b> Het JPG/PNG bestand kan minder makkelijk ongeautoriseerd bewerkt worden. Doordat een screenshot een foto is van een chatgesprek is het herkenbaar en herleidbaarheid naar het chatgesprek door de consistentie in opmaak.</p> <p><b>Min:</b> Het selecteren van berichten voor vastlegging met een screenshot is een subjectieve keuze. Er is geen zekerheid voor de latere raadpleger van de screenshot(s) dat deze een volledige weergave van een chatgesprek zijn.</p> <p><b>Min:</b> Een screenshot toont alleen de naam van de gesprekspartner, niet de naam van de gebruiker van de berichtenapp. Daarmee is het aantonen van wie de verzender en ontvanger van de berichten was niet eenduidig. Ook kan binnen de meeste berichtenapps zoals WhatsApp, Signal, en SMS de gebruiker zelf kiezen onder welke naam een gesprekspartner als contactpersoon op te slaan. Om de identiteit van zowel de gebruiker als de gesprekspartner met zekerheid te kunnen vaststellen zijn aanvullende maatregelen nodig, zoals archiveren van het adresboek van de telefoon waarop het chatgesprek heeft plaatsgevonden.</p>

## 6.2. Handmatig selecteren en exporteren chatberichten via exportfunctie WhatsApp naar DMS of andere beheerde omgeving

Met behulp van de standaard functionaliteit aanwezig op de telefoon een export van een geheel chatgesprek doorsturen naar de email om al dan niet vervolgens op te slaan in DMS. Deze mogelijkheid bestaat vooralsnog alleen binnen WhatsApp.

### Toelichting exportfunctie

Een export in WhatsApp kan alleen van een geheel chatgesprek per gesprekspartner of groepsapp gemaakt worden. Het is niet mogelijk een selectie van een deel van een chatgesprek te maken.

De export levert als resultaat een tekstbestand op dat bijvoorbeeld in Notepad te openen is. Het tekstbestand wordt samen met bijlagen in een zip-file verstuurd.

Informatieobject of metadata	Onderdeel export?
Tekstberichten	Ja
Emoticons in tekstberichten	Ja, maar de opmaak van de emoticons verandert doordat de export het omzet naar een tekstbestand.
Foto's	Ja, maar foto's worden afzonderlijk van de tekstsberichten als bijlage opgenomen. En de optie om foto's bij te voegen moet handmatig gekozen worden.
Video's	Ja
Tekstbestand als bijlage	Ja
Links naar externe websites	Ja
Live locatiebepalingen	Nee
Afzender chatbericht	Ja
Ontvanger chatbericht	Ja
Overzicht deelnemers groepsapp	Nee
Datum en tijdstip verzenden bericht	Ja
Ontvangstbevestiging bericht op device	Nee
Leesbevestiging bericht	Nee
Base64 encoded thumbnail bij afbeeldingen (specifiek bij WhatsApp)	Ja
Profielfoto gebruiker	Nee

### 6.2.1. Duurzame toegankelijkheid exportfunctie WhatsApp

<b>Vindbaar</b>	<p><b>Plus/min:</b></p> <p>De gehele chat -niet een afzonderlijk bericht daarbinnen- kan gevonden worden door gebruikers die toegang hebben tot de mailbox of het DMS.</p> <p>Maar afzonderlijke berichten kunnen moeilijker gevonden worden omdat de export van een geheel chatgesprek meerdere onderwerpen beslaat. Dat is moeilijk te koppelen aan de ordeningsstructuur van een DMS. Bewerken van de export om deze op te knippen en te koppelen aan dossiers tast de betrouwbaarheid aan, zie kopje betrouwbaar</p> <p><b>Plus:</b></p> <p>Fulltext zoeken is mogelijk in het resultaat van de export (het tekstbestand).</p>
<b>Beschikbaar</b>	<p><b>Plus:</b></p> <p>Via export kan een geheel chatgesprek geëxporteerd worden naar een beheeromgeving buiten het device van de gebruiker waar de berichten beschikbaar zijn voor derden.</p>

<b>Leesbaar</b>	<p><b>Plus:</b> Het resultaat van de export in een tekstbestand kan vanaf de meeste computers en andere devices geopend worden en is daarmee beschikbaar voor derden.</p> <p><b>Min:</b> Een tekstbestand is geen standaard open bestandsformaat. Lange termijn opslag vraagt eerst conversie naar bijvoorbeeld PDF/A.</p>
<b>Interpreteerbaar</b>	<p><b>Plus:</b> Metadata over naam van verzender en ontvanger en tijdstip van versturen chatberichten is onderdeel van de export.</p> <p><b>Min:</b> Niet alle informatieobjecten kunnen geëxporteerd worden. Onder andere audio,-en videobestanden, blauwe vinkjes, en de opmaak van bepaalde emoticons. Die informatie kan in sommige gevallen zeer relevant zijn. Zoals een tegenstrijdige smiley achter een serieus besluit. Of blauwe vinkjes die bewijzen dat een bericht op tijdstip X gelezen is.</p>
<b>Betrouwbaar</b>	<p><b>Min:</b> Zonder conversie naar bijvoorbeeld PDF/A kan het tekstbestand door iedereen bewerkt worden omdat een statische weergave van het tekstbestand niet mogelijk is. Tekst kan zodanig verwijderd of aangepast worden in de export dat een tekstbestand zelfs helemaal te falcificeren is.</p> <p><b>Min:</b> Ook kan binnen de meeste berichtenapps zoals WhatsApp, Signal, en SMS de gebruiker zelf kiezen onder welke naam een gesprekspartner als contactpersoon op te slaan. Om de identiteit van zowel de gebruiker als de gesprekspartner met zekerheid te kunnen vaststellen zijn aanvullende maatregelen nodig, zoals archiveren van het adresboek van de telefoon waarop het chatgesprek heeft plaatsgevonden.</p>

### 6.3. Geautomatiseerd en in bulk exporteren van chatberichten via uitlezen telefoon

Hard/software oplossing waarmee alle chatberichten of een deel daarvan fysiek worden uitgelezen van de telefoon en de data wordt geëxporteerd om vervolgens lokaal veilig te stellen in bijv. een DMS. Via een 'uitleesbalie' die dan beschikbaar moet zijn.

#### Toelichting:

Informatieobject of metadata	Onderdeel uitlezen?
Tekstberichten	Ja
Emoticons in tekstberichten	Ja
Foto's	Ja

Video's	Ja
Tekstbestand als bijlage	Ja
Links naar externe websites	Ja
Live locatiebepalingen	Nog te onderzoeken
Afzender chatbericht	Ja
Ontvanger chatbericht	Ja
Deelnemers groepsapp	Ja
Datum en tijdstip verzenden bericht	Ja
Ontvangstbevestiging bericht op device	Ja
Leesbevestiging bericht	Ja
Base64 encoded thumbnail bij afbeeldingen (specifiek bij WhatsApp)	Nog te onderzoeken, maar waarschijnlijk komt de afbeelding zelf en niet dit identificerende nummer mee
Profielfoto gebruiker	Ja

### 6.3.1. Duurzame toegankelijkheid *uitlezen*

<b>Vindbaar</b>	<b>Plus:</b> Er zijn selecties te maken in welke data uitgelezen wordt, van gedeeltelijk tot volledig. Het resultaat is met de bijhorende software gericht te doorzoeken.
<b>Beschikbaar</b>	<b>Plus:</b> Via het uitlezen kan zowel een selectie van chatberichten als een volledige weergave van alle chatgesprekken geëxporteerd worden naar een beheeromgeving buiten het device van de gebruiker waar de berichten beschikbaar zijn voor derden.
<b>Leesbaar</b>	<b>Plus:</b> Het resultaat van het uitlezen is leesbaar in xry-formaat.
<b>Interpreteerbaar</b>	<b>Plus:</b> Het resultaat van het uitlezen is een volledige weergave van zowel alle informatieobjecten als alle metadata. Doordat het uitlezen uitgebreid kan worden tot het adresboek is een koppeling te leggen tussen het telefoonnummer en de naam van zowel verzender als ontvanger.
<b>Betrouwbaar</b>	<b>Plus:</b> Via het uitlezen wordt een authentieke en volledige kopie van een chatbericht of chatgesprek gemaakt. Door de hoge betrouwbaarheid wordt deze oplossing gebruikt door forensische diensten en het resultaat is in rechtzalen aanvaard als bewijsmateriaal.

#### **6.4. Geautomatiseerd en in bulk exporteren van chatberichten via routeren chatberichten met aanvullende app**

Het routeren van alle chatberichten, of een deel, via een aanvullende app op de telefoon die de data op de achtergrond kopieert en automatisch via servers van een commerciële (3<sup>e</sup>) partij doorstuurt naar overheidsservers.

Er zijn momenteel commerciële leveranciers die een dergelijke mogelijkheid aanbieden voor zakelijke WhatsApp accounts. Voor privé accounts (en daarmee functioneel werkgerelateerd gebruik) zijn op dit moment nog geen aanbieders in Europa.

Wanneer over deze mogelijkheden meer bekend is, zal nadere informatie en een afwegingskader hierover toegevoegd worden.

#### **6.5. Geautomatiseerd en in bulk exporteren van chatberichten via afvangen met API**

Het rechtstreeks afvangen van alle appberichten op de servers van de berichtenapp-dienst via een interface (API) die beschikbaar is gesteld aan een commerciële (3<sup>e</sup>) partij waarna de data vervolgens veilig wordt gesteld op overheidsservers.

Deze mogelijkheid is naar verwachting moeilijk uitvoerbaar omdat onder andere WhatsApp en Signal gebruik maken van end-to-end encryptie van berichten. Naar verwachting is toestemming van de leverancier van de berichtenapp nodig om de inhoud van berichten via een API af te vangen. Zie kaders vanuit privacy en beveiliging.

Wanneer meer bekend is over deze mogelijkheid zal informatie daarover toegevoegd worden.

### **7. Overwegingen privacy en beveiliging**

Voor een verantwoorde archiveringsstrategie voor chatberichten is een afweging nodig op basis van de risico's op schade. Zoals de gevolgen van het (tijdelijk) niet beschikbaar zijn van (achterliggende) informatiesystemen, informatie die niet integer is en/of informatie die in verkeerde handen valt. Ook kan er in meerdere of mindere mate sprake zijn van dreigingen vanuit berichtenapps, waartegen de organisatie beschermd moet worden.

Bij de keuze voor een aanpak is dus belangrijk of deze wel of niet rekening houdt met de wijze waarop met vertrouwelijke en gerubriceerde informatie wordt omgegaan. En of er dus passende maatregelen (organisatorisch en technisch) zijn getroffen tegen verlies of kennisname van vertrouwelijke c.q. gerubriceerde informatie.

Of passende maatregelen getroffen dienen te worden is afhankelijk van de volgende perspectieven:

- Wel of geen Open Source / Controleerbaarheid (inzage in bijvoorbeeld de code) ;
- Wel of geen optie voor verwijderen berichten (Recovery van ongewild /-geoorloofd verzenden);
- Persoonsgebonden tov nummer gebonden (Informatie kan bij verkeerde persoon aankomen, bijvoorbeeld door nummerovergang);

- Wel of geen grip c.q. beheer over systeem c.q. netwerk (Afhankelijk van beveiligingsniveau derde partij waar geen overeenkomst mee is gesloten);
- Locatie waar de data zich bevindt wel of niet EU (jurisdictie: Delen van gebruikersdata - wie contact richting wie, wanneer contact, waar en hoe vaak - met 3<sup>e</sup> leveranciers toegestaan of richting inlichtingendienst verplicht);
- Wel of geen toegang tot gegevens gebruiker (Dus ook toegang tot gegevens derden, bijvoorbeeld contactgegevens hetgeen in strijd is met AVG);
- Wel of geen informatie beschikbaar over toegang tot de informatie zelf (afvangen of inzien wel of niet – encryptie - mogelijk)

## 8. Overwegingen uitvoerbaarheid

Een archiveringsstrategie voor chatberichten moet ook uitvoerbaar zijn voor zowel de organisatie (in termen van bijvoorbeeld kosten/baten en administratieve lasten) als voor de individuele medewerker.

Uitvoerbaarheid op organisatieniveau hangt samen met de kosten:

- Wat is er voor investering nodig om de aanpak te implementeren
- Wat kosten beheer en ontwikkeling vervolgens
- Wat zijn de administratieve lasten: hoeveel tijd kost het een medewerker gemiddeld vervolgens om compliant te zijn?

Bij uitvoerbaarheid op het niveau van de individuele medewerker is de gebruiksvriendelijkheid van de gekozen aanpak een belangrijke overweging:

- Welke handelingen zijn er nodig om aan het gevraagde te kunnen voldoen
- Hoe logisch passen die handelingen in het werkpakket van de medewerker
- Hoe veel tijd kosten die handelingen vervolgens?

Belangrijke algemene overweging hierbij is dat daar waar meer stappen in dit proces geautomatiseerd worden hoe meer de gebruiksvriendelijkheid wordt vergroot. Ook wordt de persoonlijke kwetsbaarheid van betrokken ambtenaren verkleind omdat de verantwoordelijkheid voor de archivering bij de organisatie in plaats van de ambtenaar gelegd wordt.