Risico's en maatregelen bewaren van chatberichten

Rijksprogramma
Duurzaam
Digitale
Informatiehuishouding

Risico's en maatregelen bewaren van chatberichten

De laatste jaren wordt bij de Rijksoverheid steeds vaker gecommuniceerd via chatberichten van berichtenapps zoals WhatsApp, Signal en SMS, omdat het snel en makkelijk is. Sinds de uitspraak van de Raad van State in maart 2019[1] kunnen deze chatberichten onderdeel uitmaken van de beantwoording van een Wob-verzoek. Het communiceren met chatberichten gebeurt nu veelal buiten de informatievoorziening van rijksorganisaties om. Chatberichten zijn daardoor niet-beheerde informatie- en communicatiestromen en worden veelal ongestructureerd en contextarm tussen functionarissen van binnen en buiten de Rijksoverheid gedeeld. Dit betekent dat (relevante) informatie uit de chatberichten moeten worden veiliggesteld, opgeslagen en beheerd.

Privacybescherming

Bij het bewaren van chatberichten worden ook persoonsgegevens van medewerkers verwerkt. Als over wordt gegaan op operationalisering van het beleid, moet rekening gehouden worden met de risico's ten aanzien van deze persoonsgegevens. Daarvoor wordt in de regel een pre-PIA-scan[2] en/of een data protection impact assessment (DPIA) uitgevoerd die wordt voorgelegd aan de (departementale) functionaris gegevensbescherming (FG) en, indien nodig, de departementale ondernemingsraad (DOR).

Instructie omgaan met berichtenapps

Hoe kun je het beste omgaan met het beleid over berichtenapps en hoe moet je chatberichten bewaren? Het Interdepartementaal Overleg Wetgeving en Juridische Zaken (IOWJZ) heeft in 2019 een rijksbrede instructie ontwikkeld.[3] Deze juridische instructie beschrijft welke berichten in ieder geval moeten worden opgeslagen en welke kunnen worden verwijderd. Dit leidt tot vraagstukken op het gebied van archivering, informatiebeveiliging, (staats)veiligheid en niet te vergeten, persoonsgegevens en privacy.

De strekking van de instructie is:

- Het gebruik van berichtenapps voor werkgerelateerde communicatie wordt ontraden.
- Gebeurt het toch? Sla dan de chatberichten die van belang zijn voor de reconstructie van bestuurlijke besluitvorming op in een document management systeem (DMS).
- Het is niet toegestaan om persoonsgegevens of vertrouwelijke en gerubriceerde informatie te delen via berichtenapps, behalve in het geval van in de wet genoemde uitzonderingen.

Het Rijksprogramma Duurzaam Digitale Informatiehuishouding (hierna RDDI) heeft de IOWJZ-instructie verwerkt in de rijksbrede *'Handreiking bewaren chatberichten'*. Deze bevat praktische inzichten en richtlijnen voor rijksorganisaties bij de operationalisering van het beleid en de IOWJZ-instructie.

In de handleiding vind je praktische inzichten en richtlijnen voor rijksorganisaties:

- Wat bewaren we?
- Hoe bewaren we?
- Wie bewaart de berichten?
- Waar bewaren we berichten?

Organisatie-specifieke uitwerking

Elke rijksorganisatie maakt zijn eigen (strategische, tactische en operationele) keuzes en zal de manier van veiligstellen en bewaren volgens de rijkskaders vertalen naar één of meerdere werkwijzen die passen bij de organisatiestructuur, cultuur en/of de verschillende doelgroepen. Uiteindelijk voert elke rijksorganisatie een eigen pre-PIA-scan of DPIA uit op de voorgenomen inrichting en werkwijze rondom het bewaren van chatberichten. Als startpunt heeft RDDI de mogelijke risico's en maatregelen die daarbij komen kijken in kaart gebracht.

---

[1] Naar aanleiding van de uitspraak door de Afdeling bestuursrechtspraak van de Raad van State op 20 maart 2019 (ECLI:NL:RVS:2019:899): *"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". Chatberichten zijn niet beheerde informatie- en communicatiestromen die veelal ongestructureerd en contextarm tussen functionarissen binnen en buiten de Rijksoverheid worden gedeeld.*

[2] Deze scan levert informatie op over de noodzaak van een DPIA op de gekozen beleidslijn.

[3] Voor de producten die te maken hebben met de beleidslijn Berichtenapps (zoals handreiking, instructie en beleidslijn), zie de Berichtenapps-projectpagina op de RDDI-website: https://www.informatiehuishouding.nl/projecten/berichtenapps

Dit document is bedoeld voor adviseurs bij overheidsorganisaties die verantwoordelijk zijn voor (het organiseren van) het bewaren van chatberichten en het behandelen van Wob-verzoeken. Denk aan documentaire informatie- adviseurs, Wob-juristen, informatiemanagers en -beheerders, proces- of informatieanalisten en adviseurs digitale archivering. Dit document is ook bedoeld voor directies, managers en projectleiders die verantwoordelijk zijn voor de informatie in werkprocessen en bijbehorende informatiesystemen. Deze handreiking levert praktische inzichten en uitgangspunten op bij het invoeren van de nieuwe beleidslijn.

Scope

Dit document geeft inzicht in de privacy-aspecten bij het bewaren van chatberichten en beschrijft een verzameling van de potentiële risico's die voortvloeien uit het rijksbeleid rondom de omgang met berichtenapps. Het beleid kan worden onderverdeeld in vier uitvoeringsfasen:

0. Chatten (via berichtenapps)
1. Veiligstellen (van het chatbericht uit de berichtenapp)
2. Bewaren (van de chatinformatie in het DMS)
3. Gebruiken (van de chatberichten voor bijvoorbeeld Wob-doeleinden of achivering)

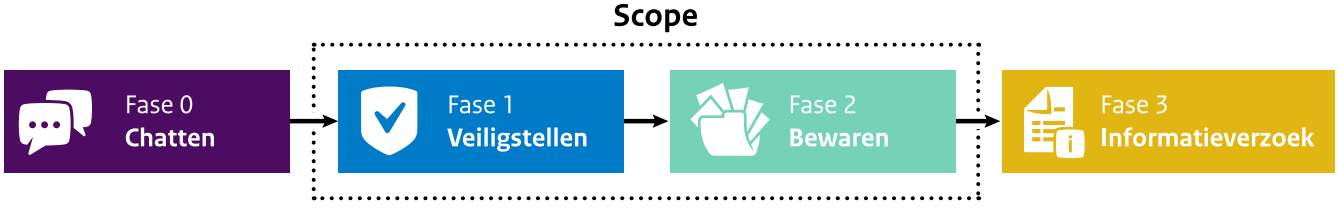
De risico's die worden beschreven in dit document beperken zich tot fase 1 'Veiligstellen' en fase 2 'Bewaren'. Daarnaast is de scope van dit document beperkt tot de drie methodes van veiligstellen die in de 'Handreiking bewaren chatberichten' worden genoemd (screenshot, export en bulkexport via mobile-archiver).

Procesomschrijving bewaren van chatberichten

Fase 1 - Veiligstellen

Er zijn drie manieren om chatberichten veilig te stellen. Bij alle drie wordt gebruikgemaakt van technologie om de chatberichten vanaf de telefoon veilig te stellen, maar relevante chatberichten moeten bij deze manieren steeds eerst handmatig worden geselecteerd.

- Optie 1 - Screenshots
  - Met een smartphone kunnen screenshots gemaakt worden van relevante chatberichten. Deze screenshots kunnen vervolgens per e-mailapplicatie verstuurd worden naar een beheerde omgeving. Vanuit deze beheerde omgeving moet de juiste metadatering aan de screenshots worden toegevoegd, irrelevante persoonsgegevens worden weggelakt en uiteindelijk moeten de chatberichten worden opslagen in het juiste dossier in het DMS.
- Optie 2 - Exporteren of kopiëren via functie berichtenapp
  - In WhatsApp en Signal (alleen bij Android) kunnen conversaties worden geëxporteerd (inclusief de bijlagen) naar een beheerde omgeving, mits de ICT-voorziening het toelaat. Hierbij wordt gebruikgemaakt van de e-mailapplicatie van de rijksorganisatie. Het resultaat is een txt-bestand, dat in een pdf kan worden omgezet. Ook kunnen op deze manier eventuele bijlagen worden veiliggesteld. Na ontvangst moet dan:
    - het zipbestand worden uitgepakt;
    - de berichten die niet relevant zijn handmatig worden verwijderd uit het txt-bestand;
    - het txt-bestand worden omgezet naar een pdf;
    - de pdf samen met de bijlagen worden opgeslagen in het DMS.



WhatsApp heeft ook de mogelijkheid om een of meerdere chatberichten te selecteren en direct als tekst via een e-mail te versturen.

- Optie 3 - Bulkexport via hardware-/softwareoplossing
  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. Vervolgens leest dit apparaat de chatberichten van de telefoon uit en kunnen de relevante berichten handmatig worden geselecteerd en veiliggesteld op een goed beveiligde server, DMS of harde schijf.

Aandachtspunten

- Bij het veiligstellen van chatberichten worden persoonsgegevens verwerkt om tot een geordende en betrouwbare ontsluiting van de berichten te komen. Hoeveel en welke gegevens worden verwerkt, is afhankelijk van de gekozen methode.
- De inhoud van berichten kan invloed hebben op de persoonlijke levenssfeer. In de conversatie zijn hoe dan ook persoonsgegevens zichtbaar, zowel in de content als in metadata. Dit geldt zowel voor de communicatie-gegevens van de verzender als van de ontvanger in deze conversatie.
- Bij het veiligstellen van chatberichten is er toegang tot alle mogelijkheden die de berichtenapp, mobiele telefoon en gebruikte tooling biedt. Zo is het mogelijk dat ook persoonsgegevens of berichten over de persoonlijke levenssfeer worden gekopieerd, doorgestuurd of verwijderd. Dit is voornamelijk een aandachtspunt wanneer een ander dan de eigenaar van de telefoon bij het veiligstellen betrokken is.

Fase 2 - Bewaren

Bewaren bestaat uit drie processtappen en verwerkingen:

- Transformeren: het omzetten van het chatbestand naar een ander format en/of het uitsplitsen van de chatberichten om over te brengen naar verschillende dossiers.
- Registreren: het autoriseren van de geëxporteerde informatie door de gegevensverantwoordelijke en het vastleggen van de juiste metadata, toegangsbeveiliging en bestandsformaten voor het DMS.
- Opslaan: het vastleggen van de informatie uit het chatbericht in het DMS.

De manier van exporteren is dus van invloed op de verwerking in de bewaarfase. In deze fase moet men veelal handmatig enkele gegevens invullen, bijvoorbeeld om namen, profielfoto's, telefoonnummers, locatie-gegevens, leesbevestigingen en data van verzonden berichten te duiden.

Risico's en maatregelen

Onderstaande tabel schetst een aantal potentiële risico's van het implementeren van de opties om chatberichten te bewaren. In de rechterkolom staan maatregelen om het beschreven risico zoveel mogelijk te beperken. Deze informatie kunnen rijksorganisaties gebruiken om een eigen DPIA te ontwikkelen op de gekozen manier voor het bewaren van chatberichten. Deze lijst met risico's en maatregelen is niet limitatief.

#	Risico	Kans	Impact	Maatregel
1	**Betrokkenen hebben geen controle over hun persoonsgegevens** *Een deelnemer aan een chatgesprek heeft geen controle over wat een gesprekspartner of berichten-app-ondersteuner veiligstelt of bewaart. Hierdoor heeft de deelnemer (waaronder ook externen) geen invloed op hoeveel, hoe lang en op welke manier persoonsgegevens bewaard worden. Dit geldt voor alle bewaarde chatconversaties. Dit geldt voor alle chatconversaties die worden bewaard.*	**Grote kans:** • Gegevens worden zonder medeweten van de gesprekspartner verwerkt. • Het is onduidelijk welke berichten relevant zijn voor de reconstructie van bestuurlijke besluitvorming. • Externen zijn zich niet bewust van de regels binnen de overheid.	**Grote impact:** • Het delen van vertrouwelijke informatie en privégegevens kan een grote impact hebben op betrokkenen en verwerkingsverantwoordelijken.	• Stel spelregels op voor wie, wat en wanneer vastlegt. • Creëer een standaard tekst waarin wordt aangegeven dat persoonsgegevens kunnen worden verwerkt als de conversatie bestuurlijke besluitvorming bevat. • Bevestig afspraken per e-mail en bewaar die mail in het DMS. • Bespreek eventuele verkeerde verwerking met betrokkenen ook in P-gesprekken.
2	**Er worden bijzondere of strafrechtelijke persoonsgegevens verwerkt** *Het versturen van bijzondere of strafrechtelijke gegevens is in principe verboden, behalve wanneer er per gebeurtenis sprake is van een uitzonderingsgrond.*	**Aannemelijke kans:** • Bijzondere of strafrechtelijke gegevens worden verstuurd.	**Grote impact:** • Het delen van bijzondere of strafrechtelijke gegevens kan een grote impact hebben op betrokkenen. • Verlies van vertrouwen in overheids-organisaties die transparant met gegevens van burgers en medewerkers moeten omgaan.	• Deel nooit bijzondere of strafrechtelijke persoonsgegevens via berichtenapps. Dit is vrijwel altijd onrechtmatig. Leg dit vast in het uitvoeringsbeleid en communiceer dit binnen de organisatie (bewustwording). • Zorg voor duidelijke communicatie en strikte handhaving van de regels om te zorgen dat elke medewerker zich aan de verwerking houd. • Toets of bespreek binnen een team periodiek of er bijzondere of strafrechtelijke gegevens zijn verstuurd en waarom. • Spreek betrokkenen altijd aan op verkeerde verwerking bijvoorbeeld in P-gesprekken.
3	**Ongeoorloofde toegang van persoonsgegevens** *Gegevens die bij het veiligstellen en bewaren van chatberichten zijn verwerkt kunnen zonder beperkingen doorgezonden worden aan derden. De chatberichten worden verzonden met een eigen werk e-mailadres waar handmatig vernietiging op plaats moet vinden.*	**Grote kans:** Gegevens worden onrechtmatig verspreid omdat de verwerker zonder toezicht de gegevens ook naar derden verstuurt (dit kan ook per abuis gebeuren).	**Grote impact:** • Vertrouwelijke informatie en privégegevens van betrokken personen zijn onrechtmatig gedeeld.	• Stel een datalekprotocol op en zorg dat deze wordt nageleefd. • Stel spelregels op voor wie, wat en wanneer vastlegt. • Bevestig afspraken per e-mail en bewaar die mail in het DMS. • Bespreek eventuele verkeerde verwerking met betrokkenen ook in P-gesprekken.

#	Risico	Kans	Impact	Maatregel
4	**Ongeoorloofde toegang van persoonsgegevens** *Het veiligstellen van chatberichten is voor een groot deel mensenwerk. De beschikbare tijd, voorziening en eigen inschatting zijn bepalend bij het selecteren van relevante chatberichten.*	**Grote kans:** • Er worden meer of minder gegevens verwerkt dan nodig.	**Grote impact:** • Het delen van meer informatie dan noodzakelijk is nadelig voor de betrokkenen en de betrokken departementen.	• Informeer medewerkers en train ze waar nodig in het veiligstellen van chatberichten die relevant zijn voor de reconstructie van bestuurlijke besluitvorming. • Richt hulpdiensten in die kunnen helpen met advies of (technische) ondersteuning. • Zorg voor goede autorisatie-inrichting op het DMS waarin chatberichten worden bewaard.
5	**Ongeoorloofde toegang van persoonsgegevens** *Wordt het veiligstellen van chatberichten overgedragen aan een 'ondersteuner' van de gebruiker? Dan heeft de ondersteuner mogelijk ook toegang tot alle persoonlijke data op de telefoon, zoals ontvangen foto's, filmpjes, communicaties uit de persoonlijke omgeving. Deze ondersteuners kunnen alle bestanden van de telefoon exporteren en delen met derden.* *(Zie risico 3)*	**Grote kans:** • De ondersteuner kan persoonlijke gegevens inzien. • De privacy van de gebruiker kan niet worden gegarandeerd.	**Grote impact:** • Gevoelige informatie kan in de verkeerde handen vallen en de betrokkene kan daarmee in verlegenheid worden gebracht of chantabel worden.	• Hanteer een strikt autorisatieprotocol voor de ondersteuners die chatberichten veiligstellen. Let hierbij op dat er een ongelijke machtsverhouding is tussen de ondersteuner en de gebruiker van de telefoon. • Zorg voor zorgvuldige screening van ondersteuners voor verwerking van gegevens onder het juiste rubriceringsniveau.
6	**Ongeoorloofde toegang van persoonsgegevens** *De tussentijdse kopieën die gemaakt worden om een chatbericht uiteindelijk goed te bewaren moeten handmatig worden vernietigd. Denk hierbij aan e-mails en zip- en txt-bestanden afhankelijk van de manier van veiligstellen die is gekozen.*	**Grote kans:** • Informatie wordt niet volgens bewaartermijnen bewaard of vernietigd doordat kopieën van vernietigde informatie op verschillende locaties kan staan. **Aannemelijke kans:** • Medewerkers bewaren kopieën te lang omdat het verwijderen veel handelingen vergt op verschillende locaties.	**Middelgrote impact:** • De tussentijdse kopieën staan waarschijnlijk in de werkomgeving van de verwerker, die de gegevens toch al in kan zien.	• Informeer medewerkers en train ze waar nodig in het veiligstellen van chatberichten die relevant zijn voor de reconstructie van bestuurlijke besluitvorming. • Doe periodiek onderzoek naar welke informatie op de verschillende locaties staat, en voer vervolgens opschoningsacties uit.

#	Risico	Kans	Impact	Maatregel
7	**Ongeoorloofde toegang van persoonsgegevens** *Bij de optie bulkexport en exportfunctie van de berichtenapp vindt de schifting van chatberichten plaats nadat de chatberichten van de telefoon zijn veiliggesteld.*	**Grote kans:** • Er zijn meer persoonsgegevens verwerkt dan noodzakelijk.	**Middelgrote impact:** • De gegevens blijven binnen het proces. In het geval van bulkexport worden ze ook automatisch weer gewist op de mobile extractor.	• Informeer medewerkers en train ze waar nodig in het veiligstellen van chatberichten. • Richt hulpdiensten in die kunnen helpen met advies of (technische) ondersteuning.
8	**Er zijn onvoldoende maatregelen getroffen op het gebied van de ontvangst en verstrekking van persoonsgegevens aan derden** *Leveranciers van hardware, software en/of cloudopslag die voor het veiligstellen worden ingeschakeld, zijn betrokken bij de techniek om chatberichten veilig te stellen. Ze hebben daarmee ook een verantwoordelijkheid om niet meer (persoons)gegevens te verwerken dan nodig of berichten ongecontroleerd te verspreiden.*	**Kleine kans:** • De leveranciers hebben geen directe betrokkenheid bij het verwerken van de chatberichten en daarmee ook geen directe mogelijkheid om een back-door in de software op te nemen.	**Grote impact:** • Bij deze vorm van een datalek hebben de leveranciers toegang tot alle gegevens op de telefoon of de applicatie.	• Maak met de leveranciers heldere afspraken over de gegevens die worden verwerkt en zie erop toe dat er geen ‘back-doors’ in de software worden opgenomen waarmee gegevens worden gedeeld.
9	**Ongeoorloofde toegang van persoonsgegevens** *Wanneer medewerkers hun chatberichten veiligstellen buiten de Europese Economische Ruimte (EER), bijvoorbeeld op de BES-eilanden, worden de gegevens verstuurd buiten het werkings-gebied van de AVG. Betrokkenen kunnen hun privacy-rechten dan mogelijk niet of lastiger uitoefenen en de vertrouwelijkheid van hun persoonsgegevens kan worden ingeperkt.*	**Kleine kans:** • Berichten worden veiliggesteld buiten de EER.	**Grote impact:** • Bij deze vorm van een datalek hebben leveranciers toegang tot alle gegevens op de telefoon of applicatie. Via deze weg kunnen derden toegang krijgen tot de persoonsgegeven en contacten van de gebruiker.	• Maak met de medewerkers heldere afspraken en een protocol over het opslaan van chatberichten in het buitenland. • Onderzoek nauwkeurig de informatiebeveiliging en tref de benodigde maatregelen. Neem ook maatregelen om doorgiften buiten de EER te voorkomen. • Sluit verwerkingsovereenkomsten af met leveranciers van hardware, software en/of cloudopslag die voor het veiligstellen worden ingeschakeld.

#	Risico	Kans	Impact	Maatregel
10	**Er zijn onvoldoende maatregelen getroffen op het gebied van de ontvangst en verstrekking van persoonsgegevens aan derden** *Indien ooit software/AI/OCR-hardware ingezet gaat worden om automatisch persoonsgegevens te scannen, kan door technische tekortkomingen identificatie van secundair, tot de persoon herleidbare, vertrouwelijke en persoonlijke informatie ten onrechte als relevante informatie worden bestempeld. Hierdoor worden meer (persoons)gegevens verwerkt dan nodig. Dit is een onrechtmatige en niet transparante verwerking en vanwege 'false positives' en 'false negatives' ook onnauwkeurig.*	Op dit moment is het niet mogelijk om voldoende op geautomatiseerde herkenning van persoonsgegevens te kunnen vertrouwen.	**n.t.b.**	• Zet handmatige selectie in voor het veiligstellen van chatberichten. • Maak heldere afspraken met softwareleveranciers over welke gegevens worden verwerkt en op welke manier hiervoor artificiële intelligentie (AI) wordt ingezet.

Dit is een uitgave van:

Rijksprogramma Duurzaam Digitale
Informatiehuishouding (RDDI)

Projectteam Berichtenapps - RDDI

December 2021