Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Adviescollege Openbaarheid en Informatiehuishouding
Postbus 18601
2502 EP Den Haag

DG Digitalisering & Overheidsorganisatie
CIO Rijk en Digitaliseringsbeleid

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag

Onze referentie
2026-0000077739

Datum
Betreft Adviesaanvraag gebruik chatapps en veiligstellen overheidsinformatie

Naar aanleiding van de adviesaanvraag naar het gebruik van chatapps binnen de Rijksoverheid en het veiligstellen van overheidsinformatie (referentie 2025-0000677518) heeft het Adviescollege Openbaarheid en Informatiehuishouding een aantal vragen gesteld die BZK hierbij beantwoord.

1. Welke berichtendiensten voor mobiele telefoons (WhatsApp, Signal, SMS e.a.) worden op dit moment gebruikt door bewindslieden bij de ministeries?

   Antwoord:
   Door bewindslieden wordt vooral gebruik gemaakt van WhatsApp. Binnen Rijksoverheidsorganisaties wordt vooral gebruik gemaakt van WhatsApp en Signal.
   Het gebruik van SMS wordt sterk afgeraden. SMS mag alleen worden gebruikt voor algemene mededelingen die niet vertrouwelijk zijn en niet voor inhoudelijke zaken. CIO Rijk heeft geen kwantitatieve informatie beschikbaar over daadwerkelijk gebruik.

2. Welke gedragsregels gelden en hoe worden deze bekend gemaakt aan bewindslieden?

   Antwoord:
   Voor Rijksambtenaren geldt de gedragsregeling van de digitale en fysieke werkomgeving.
   Voor bewindspersonen geldt het handboek bewindspersonen.
   Het handboek bewindspersonen verwijst naar de handreiking voor bewindspersonen specifiek voor sociale media-, e-mail- en chatgebruik.

   De kern van deze gedragsregels is:
   1) De noodzaak om privé van zakelijke informatie te scheiden. Uitgangspunt daarbij is dat voor privé informatie privé accounts en middelen worden gebruikt en dat zakelijke communicatie alleen via zakelijke accounts en middelen verloopt. Dit is van belang om vermenging van informatiestromen te voorkomen.
   2) Het gebruik van berichten-apps is alleen bedoeld voor informele zaken en niet voor het delen van persoonsgegevens, medische gegevens zoals ziekmeldingen en voor formele zaken, zoals bestuurlijke aangelegenheden: app met beleid maar niet over beleid.

De gedragsregels zijn bij het aantreden van de rijksambtenaren en bewindspersonen toegelicht. Na vernieuwing van gedragsregels worden deze ook weer onder de aandacht gebracht van de geraakte doelgroep(en).

3. Wij begrijpen dat chatconversaties uit WhatsApp op dit moment worden uitgelezen met software, waarbij bewindslieden hun telefoon tijdelijk inleveren.

   Antwoord:
   Ja, dit klopt. Deze informatie is terug te vinden in het rapport n.a.v. uitvraag veiligstelling zakelijke informatie bewindspersonen kabinet Rutte IV dat is opgesteld naar aanleiding van het ADR onderzoeksrapport.

   a. Klopt dit of zijn er nog andere methoden die ministeries benutten?

      Antwoord:
      Deze methode wordt door alle ministeries ingezet. Ingezette software en werkwijze kan per departement verschillen.

   b. Met welke frequentie worden chatconversaties van bewindspersonen op dit moment veiliggesteld en hoeveel tijd is hiermee – per keer – gemoeid?

      Antwoord:
      De tijdelijke instructie schrijft een maandelijks uitleesmoment voor. Veelal wordt deze ook gehandhaafd. De tijd die hiermee gemoeid is, is afhankelijk van een aantal factoren, zoals of dit het eerste uitleesmoment betreft en hoe intensief de persoon de chatapp gebruikt. Dit kan variëren tussen enkele uren tot een kwartier.
      Doordat de *advanced privacy voor chats* optie per conversatie moeten worden gecontroleerd en waar nodig uitgezet om de betreffende chatconversatie te kunnen opslaan, is de tijd die gemoeid is met het uitlezen toegenomen toen deze functie door WhatsApp is geïntroduceerd.

   c. Hoeveel bewindslieden hebben nu naast hun zakelijke telefoon een privé telefoon (of dual simkaart) om zakelijke conversaties te scheiden van privé conversaties en communicatie over aangelegenheden van de eigen partij? Welke andere methoden worden benut om die scheiding aan te brengen?

      Antwoord:
      In 2024 is uitgevraagd of de communicatiestromen van elkaar worden gescheiden. Dit is verwerkt in het rapport. Bij de uitvraag van CIO Rijk hebben alle departementen aangegeven dat er een middelenscheiding plaatsvindt voor de verschillende communicatiestromen.

De (technische) wijze waarop scheiding van communicatiestromen plaatsvindt is niet uitgevraagd, waardoor deze informatie op dit moment niet voorhanden is.

d. Welke ministeries stellen chatconversaties van de ambtelijke top (sleutelfuncties) nu ook al veilig?

Antwoord:
Deze informatie is nog niet formeel uitgevraagd. Van een viertal departementen is bekend dat zij jaarlijks of bij vertrek de chatberichten van de leden van de bestuursraad veiligstellen.

e. Zijn er op bovenstaande punten verschillen tussen de ministeries?

Antwoord:
Ja

4. In de adviesaanvraag van BZK staat dat chatconversaties vanuit Signal niet met software (dus geautomatiseerd) geëxporteerd kunnen worden naar een beheerde omgeving van de Rijksoverheid.

   a. Indien informatie toch nodig is voor publieke verantwoording (onderzoek of vragen parlement, Woo-verzoek) is er dan een manier om (delen van) chatconversaties via Signal achteraf te kopiëren, bijvoorbeeld met screenshots?

   Antwoord:
   Signal berichten kunnen met behulp van screenshots worden veiliggesteld.

   b. In hoeverre wordt Signal nu door bewindspersonen en topambtenaren gebruikt?

   Antwoord:
   Bewindspersonen maken primair gebruik van WhatsApp. Topambtenaren maken gebruik van WhatsApp en Signal. Per ministerie is het gebruik afhankelijk van het departementale privacy- en informatiebeveiligingsbeleid.

5. Welke andere organisatorische, juridische en/of technische knelpunten zijn geconstateerd bij het veiligstellen van conversaties uit de verschillende berichtendiensten?

   Antwoord:
   Knelpunten betreffen veelal de mogelijkheid tot schoning van chatberichten die niet onder de Archiefwet vallen, te weten puur privé en partijpolitieke chatberichten. Hiertoe is een afwegingskader privé, partijpolitiek en personeelsvertrouwelijk in de maak.

Eveneens is de vraag of er blijvend gelakt mag worden binnen zakelijke chatberichten (in het archiefexemplaar) uitgezet bij de Autoriteit Persoonsgegevens. Het betreft hier specifiek het lakken van puur privé of partijpolitieke passages in zakelijke chatberichten (zogenaamde hybride chatberichten). Dit advies wordt medio februari 2026 verwacht.

6. Wat is bij BZK bekend over de situatie bij andere organisaties die deel uitmaken van de Rijksoverheid? Zoals grote uitvoerende diensten (UWV, Belastingdienst e.d.), toezichthouders en zelfstandige bestuursorganen.

   Antwoord:
   BZK heeft geen informatie over de situatie bij andere organisaties (dan ministeries) die deel uitmaken van de Rijksoverheid

Toekomstige chatvoorziening Rijk t.b.v. geautomatiseerde archivering
De Rijksoverheid werkt aan een eigen 'chatvoorziening'. Op basis van het Eindverslag Pilot Chatarchivering begrijpen wij deze als volgt: er wordt een applicatie geïnstalleerd op mobiele telefoons die kan 'praten' met veel gebruikte berichtendiensten zoals WhatsApp en Signal. Wanneer bewindspersonen en ambtenaren via de chatvoorziening communiceren, worden de aldus gewisselde berichten automatisch gearchiveerd c.q. in beheer genomen door de Rijksoverheid.

Wij hebben hierover de volgende vragen:

7. Klopt de bovenstaande omschrijving van de chatvoorziening? Graag ontvangen wij eventuele actuelere beschrijvingen van de beoogde voorziening.

   Antwoord:
   Ja, bovenstaande informatie klopt.

8. Wat zijn de belangrijkste voordelen ten opzichte van de huidige situatie?

   Antwoord:
   1. De Rijksoverheidsorganisatie heeft controle over de aangeboden functionaliteiten en de verwerkte data (metadata en chatberichten).
   2. Data (metadata en zakelijke chatberichten) wordt geautomatiseerd veiliggesteld.
   3. De hele applicatie is versleuteld met encryptiesleutels die onder controle van de Rijksoverheid zijn. Deze encryptiesleutels worden beheerd door de Rijksoverheid.
   4. Vergeleken met de manuele vastlegging na exporteren zou het automatisch vastleggen, veiligstellen en voor archivering aanbieden één aaneengesloten keten met aaneengesloten versleuteling van alle data uit vastgelegde chatberichten betekenen. Dit moet worden geverifieerd via een risico-analyse.
   5. De Rijksbrede voorziening werkt interoperabel, deze kan communiceren met in- en externe WhatsApp en Signal gebruikers.

6. De centrale gateway zorgt ervoor dat alle berichtenuitwisseling met WhatsApp en Signal gebruik maakt van hun respectievelijk end-to-end-encryptie (E2EE)
7. Dit vastleggen over de chat-platformen heen genereert een complete tijdlijn van communicatie over alle chatkanalen heen. In de huidige werkwijze is ingeval van onderzoek (Woo-verzoek of Parlementaire Enquête) het creëren van een accurate tijdlijn over kanalen heen een uitdaging.
8. De voorziening garandeert volledigheid, authenticiteit, bescherming tegen data manipulatie en geeft een bewaringsketen die bewijskracht door de keten heen intact laat, ze is voorzien van beheer- en controlemogelijkheden, met als basis een uitgebreid geïntegreerd logging systeem
9. In de bestaande manuele oplossing wordt ieder geëxporteerd chatbericht door medewerkers gelezen, gemarkeerd en teruggezonden voor validatie. De beoogde voorziening met scheiding van zakelijke en privé mobiele toestellen en automatische vastlegging laat dit '100% meelezen' achterwege. Hier zijn het de zorgdragers zelf die bij aanname van de vastgelegde berichten bepalen of zij op moment van aanname of later gericht na een informatieverzoek berichten classificeren en waar nodig lakken.
10. De bestaande manuele oplossing is zeer arbeidsintensief zowel in exporteren als in review, validatie en redactie van chatberichten.
11. De integriteit van vastgelegde en veiliggestelde berichten is gegarandeerd, ook bij verwerking op grote schaal.

9. Wanneer zal de chatvoorziening in gebruik worden genomen? Ga daarbij s.v.p. uit van een realistische planning.

Antwoord:
De ingebruikname staat gepland voor eind 2026

10. Kunnen bewindslieden en topambtenaren via deze chatvoorziening alleen intern communiceren, dus met anderen binnen de Rijksoverheid, of ook met mensen daarbuiten die gebruik maken van berichtendiensten als WhatsApp, Signal en SMS?

Antwoord:
De voorziening is interoperabel, dat wil zeggen dat vanuit de voorziening met zowel WhatsApp als Signal gebruikers kan worden gechat.

De gedragsregeling voor Rijksambtenaren schrijft voor dat SMS alleen gebruikt mag worden voor algemene mededelingen die niet vertrouwelijk zijn en niet voor inhoudelijke zaken. SMS is niet veilig omdat sms-berichten niet zijn versleuteld waardoor de inhoud gemakkelijk kan worden onderschept.

Bewindspersonen

11. Kan de gehele chatconversatie met mensen die een andere berichtendienst gebruiken worden veiliggesteld in een beheerde omgeving van het Rijk of zijn er beperkingen door de versleuteling van berichten door berichtendiensten als WhatsApp, Signal en SMS?

    Antwoord:
    De gehele chatconversatie met personen die Signal of WhatsApp gebruiken kan worden veiliggesteld in een beheerde omgeving van de Rijksoverheid. Volledigheid, authenticiteit, onveranderlijkheid en bewijskracht zijn gegarandeerd en blijven behouden. SMS is niet in scope van de opdracht, omdat SMS niet mag worden gebruikt voor inhoudelijke zaken.

12. Indien iemand van buiten de Rijksoverheid de conversatie initieert vanuit een andere chatapplicatie, wordt de chatconversatie dan evengoed veiliggesteld? Zo niet, welke oplossing is voorzien?

    Antwoord:
    Dit is een keuze die nog gemaakt moet worden. De voorziening biedt de mogelijkheid, waarbij 1) de rijksambtenaar of bewindspersoon expliciet toestemming dient te geven dat iemand van buiten de Rijksoverheid de conversatie initieert. Pas na deze bevestiging kan de communicatie plaatsvinden en wordt de chatconversatie vastgelegd (extra beveiliging). Of 2) iemand van buiten de Rijksoverheid initieert de conversatie en deze wordt direct vastgelegd.

13. Zijn er (andere) organisatorische, juridische of technische knelpunten te verwachten?

    Antwoord:
    Nee, voor genoemde knelpunten worden mitigerende maatregelen genomen en er wordt een risicoanalyse uitgevoerd.

14. Wanneer een bewindspersoon of (top)ambtenaar de chatvoorziening op diens telefoon krijgt, kunnen daarmee ook eerdere chatberichten worden veiliggesteld? Oftewel, kunnen bij de keuze voor Signal de berichten die zijn gewisseld vóór de komst van de chatvoorziening eenvoudig worden veiliggesteld?

    Antwoord:
    Nee, de chatapp kan alleen de vanuit de chatapp geïnitieerde chatconversaties veiligstellen. Eerdere chatberichten worden, bij ingebruikname van de voorziening, in overeenstemming met de huidige handmatige dienstverlening veiliggesteld.

15. Zullen alle ambtenaren van de ministeries de chatvoorziening op hun telefoon krijgen, of alleen bewindspersonen en de ambtelijke top?

Antwoord:
Alleen de sleutelfunctionarissen (bewindspersonen en ambtelijke top) krijgen de Rijksbrede chatapp op de smartphone beschikbaar. Dit aangezien er per gebruiker een licentie moet worden afgenomen. Parallel aan deze voorziening wil de Rijksoverheid op middellange termijn ook een eigen autonome, soevereine overheidsapp realiseren voor alle rijksambtenaren, waarbij ook functionele eisen en de geleerde lessen uit deze voorziening in worden meegenomen.

16. Welke andere organisaties binnen de Rijksoverheid kunnen de chatvoorziening gaan gebruiken op hun mobiele telefoons?

    Antwoord:
    De chatvoorziening betreft een Rijksbrede voorziening en alle organisaties die nu ook Rijksbrede voorzieningen gebruiken, kunnen deze Rijksbrede chatapp gebruiken, als zij voldoen aan de aansluitvoorwaarden.

17. Komen er ook licenties en/of documentatie beschikbaar voor gemeenten, provincies en waterschappen?

    Antwoord:
    Er komen geen licenties beschikbaar voor gemeenten, provincies en waterschappen. Dit valt buiten de scope van de aanbesteding. De verstrekte opdracht is alleen voor de sleutelfunctionarissen van de Rijksoverheid.

    Kennisdeling door het delen van documentatie is wel mogelijk.

18. Wie is de beoogde leverancier van de chatvoorziening (software en data-opslag)? Gaat het om een of meer dienstverleners binnen de Rijksoverheid zelf, om een of meer private bedrijven, of een combinatie van beiden?

    Antwoord:
    Aanbieder: Rijksorganisatie voor Informatiehuishouding (RvIHH)
    Software: er wordt gebruikt gemaakt van een standaard marktoplossing, aangeboden door een Nederlandse partner van de marktoplossing.
    Beheer: SSC-ICT
    Cloud: een door het Rijk (SSC-ICT) beheerde landing zone ingericht volgens Rijksoverheid veiligheidsmaatregelen voor tijdelijke bewaren van de berichten.
    Datacenter: ODCR voor het definitief veiligstellen van de chatberichten.

19. Als er private bedrijven betrokken zijn, hebben deze dan toegang tot de metadata en de inhoud van de chatberichten en zijn hier afspraken over?

    Antwoord:
    Private bedrijven kunnen niet bij (gebruikers) data komen.

Overgangssituatie
In de adviesaanvraag heeft BZK beschreven dat de introductie van AI-functionaliteit binnen WhatsApp tot zorgen leidt over de beveiliging van overheidsinformatie. Om die reden overwegen de ministeries om voor interne communicatie alleen nog Signal te gebruiken totdat de chatvoorziening gereed is.

Hierover hebben we de volgende aanvullende vragen:

20. Heeft BZK vertrouwen dat de inhoud van WhatsApp berichten end-to-end versleuteld is en niet door Meta wordt ingezien en gebruikt? Is in die taxatie verandering gekomen door de invoering van de AI-functionaliteit? Voor zover wij weten kan immers de AI-bot alleen eventuele communicatie tussen de accounthouder en de AI-bot lezen en niet de inhoud van overige chatconversaties.

    Antwoord:
    De inhoud van WhatsAppberichten is end-to-end versleuteld. Alleen wanneer je een opdracht aan de Meta AI geeft met het commando "@Meta AI" wordt deze opdracht onversleuteld door WhatsApp verwerkt. Voor metadata is dit anders, deze is zichtbaar voor Meta en wordt ook door Meta voor (afgeleide) commerciële doeleinden aangewend.

    Het uitgangspunt dat de AI-bot communicatie tussen de accounthouder en de AI-bot kan lezen is problematisch, aangezien het zakelijk chatgesprek hierdoor niet meer vertrouwelijk is. De versleuteling van de desbetreffende chatberichten wordt hiermee doorbroken, wat onwenselijk is voor zakelijke informatie.

21. Hoe taxeert u risico's op de verzameling en eventuele verwerking van metadata (o.a. met wie, wanneer, hoe lang en hoe vaak wordt gecommuniceerd) door WhatsApp en andere commerciële berichtendiensten? En is hierin onlangs nog verandering gekomen?

    Antwoord:
    Voor zakelijk gebruik van chatapps is het noodzakelijk dat het 'lekken' van overheidsinformatie zoveel mogelijk wordt tegengegaan. WhatsApp is een consumentenproduct dat veel en soms ook gevoelige metadata verzamelt met als doel het kunnen aanbieden van gepersonaliseerde advertenties.

    De werkgever kan de medewerker niet verplichten om de consumentenversie van WhatsApp te gebruiken en daarmee de privacy-voorwaarden van Meta te accepteren, omdat deze een zodanig grote inbreuk op de privacy van medewerkers betekent dat deze toestemming niet door een werkgever af te dwingen is.

    Signal verwerkt een minimale hoeveelheid metadata en gebruikt deze alleen voor de instandhouding van de dienst. Hierdoor heeft het CIO-beraad besloten om over te willen stappen op het gebruik van Signal voor communicatie tussen rijksambtenaren onderling totdat een meer autonome, soevereine chatapp voor de (rijks)overheid beschikbaar is.

Zie ook de tabel in antwoord op vraag 29.

22. Wanneer de AI-functionaliteit van WhatsApp uitstaat, is het niet mogelijk van de betreffende chatconversatie een export te maken. Het is echter altijd mogelijk om deze desnoods tijdelijk weer aan te zetten zodat de berichten wel uitgelezen kunnen worden en overgezet in een eigen DMS of andere beheerde omgeving. Kunt u aangeven hoeveel extra tijd dit kost vergeleken met de huidige situatie?

    Antwoord:
    Dit is mede afhankelijk van de hoeveelheid chatconversaties die de betreffende bewindspersoon of ambtenaar op de smartphone heeft. Het gebruik loopt uiteen van enkele tientallen tot honderden chatgesprekken. Hier zijn geen kwantitatieve gegevens van beschikbaar bij CIO Rijk.

23. Bestaan er gedragsregels over het gebruik van AI door bewindslieden en ambtenaren? In hoeverre is overwogen specifieke instructies op te stellen in verband met de introductie van de AI-functionaliteit van Whatsapp?

    Antwoord:
    Gedragsregeling voor de digitale en fysieke werkomgeving:
    Gebruik bij AI geen persoonsgegevens of vertrouwelijke informatie.

    Overheidsbrede handreiking voor de verantwoorde inzet van generatieve AI: Hoofdstuk 5.2, 7.2 en 9.1 bevat generieke informatie voor rijksambtenaren over privacy rondom generatieve AI

    Er is overwogen om specifieke instructies op te stellen in verband met de introductie van de AI-functionaliteit van Whatsapp. Het CIO beraad heeft echter gekozen voor een Rijksbrede overstap naar Signal.

24. Is bekend in hoeverre Signal nu al door bewindspersonen en topambtenaren wordt gebruikt?

    Antwoord:
    Bewindspersonen maken primair gebruik van WhatsApp. Topambtenaren maken gebruik van WhatsApp en Signal. Per ministerie is het gebruik afhankelijk van het departementale privacy- en informatiebeveiligingsbeleid. CIO Rijk heeft geen actueel overzicht van in hoeverre welke (delen van) ministeries gebruik maken van Signal.

25. Is de bedoeling dat alle rijksambtenaren voor communicatie onderling per 1 januari 2026 al overstappen naar Signal? Zo ja, wat zijn hiervoor de redenen?

    Antwoord:
    Nee, Rijksambtenaren stappen over op een nader te bepalen moment. Allereerst worden in het SGO nog de consequenties van dit besluit op de

uitvoering van de Wet Open Overheid op het gebied van chatberichten geagendeerd en besproken.

26. Zou bij een overstap naar Signal, communicatie met de buitenwereld via WhatsApp en andere berichtendiensten mogelijk blijven?

    Antwoord:
    Ja, dit blijft mogelijk. Het besluit om Signal te gaan gebruiken is primair bedoeld voor interne communicatie binnen de Rijksoverheid. Voor externe communicatie of communicatie met bewindspersonen wordt gebruik gemaakt van WhatsApp.

Overige vragen

27. Hoeveel invloed kan de Nederlandse overheid uitoefenen om WhatsApp de exporteer- en AI-functionaliteit los te laten koppelen?

    Antwoord:
    Beperkt, het betreft een consumentenproduct dat de Rijksoverheid niet als dienst afneemt maar onder eigen verantwoordelijkheid en risico heeft ingezet.

28. Hoeveel invloed kan de Nederlandse overheid uitoefenen om Signal exporteren mogelijk te laten maken?

    Antwoord:
    Beperkt, het betreft een consumentenproduct dat de Rijksoverheid niet als dienst afneemt maar onder eigen verantwoordelijkheid en risico heeft ingezet. Signal heeft aangekondigd een export functionaliteit te gaan ontwikkelen voor de desktop client waarmee chatconversaties geëxporteerd kunnen worden.

29. Zijn er mogelijkheden voor de Amerikaanse overheid om bij berichten van WhatsApp of Signal te komen? In hoeverre kan de Nederlandse overheid of de EU hierop nog invloed uitoefenen?

    Antwoord:
    In principe kan de Amerikaanse overheid niet bij de inhoud van berichten van zowel WhatsApp of Signal door de sterke en-to-end encryptie in het geval van een gerechtelijk bevel op basis van CLOUD Act of FISA. De private key ligt in beide gevallen bij de gebruiker op het apparaat, niet bij de service. Metadata is echter niet versleuteld en is dus wel op te vragen, en in het geval van WhatsApp is er best wel wat metadata op te vragen in vergelijking met Signal.

Type metadata	*WhatsApp (Meta)*	*Signal*
Wie met wie communiceert	*Ja*	*Nee*
Tijdstippen en frequentie berichten	*Ja*	*Nee*
Duur oproepen	*Ja*	*Nee*
IP-adressen	*Ja*	*Nee (of zeer beperkt)*
Contactenlijst / adresboek	*Ja (groot deel)*	*Nee*
Groepsleden	*Ja (in sommige gevallen)*	*Nee*
Registratiedatum	*Ja*	*Ja*
Laatste connectie	*Ja*	*Ja*

Invloed van NL of de EU is heel beperkt aangezien het Amerikaanse wetgeving is op Amerikaanse entiteiten.

30. Heeft de Digital Markets Act (DMA) invloed op de archiveerbaarheid, privacy, informatiebeveiliging en data-soevereiniteit van berichtendiensten?

Antwoord:
Ja, de DMA heeft invloed op de privacybescherming die berichtendiensten moeten toepassen. Het Europees Comité voor gegevensbescherming (EDPB) en de Europese Commissie zijn onlangs een gezamenlijke openbare raadpleging gestart over de eerste versie van de richtsnoeren 'Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation' die bedrijven houvast bieden bij het uitvoeren van hun verplichtingen onder de DMA zonder in strijd te komen met de AVG.
Deze richtsnoeren kunnen van invloed zijn op de functionele eisen voor archivering, privacy, informatiebeveiliging en data-soevereiniteit van berichtendiensten.